Säker och kostnadseffektiv it-drift

– rättsliga förutsättningar för utkontraktering

Delbetänkande av It-driftsutredningen

Stockholm 2021

STATENS OFFENTLIGA UTREDNINGAR

SOU 2021:1

SOU och Ds finns på regeringen.se under Rättsliga dokument.

Svara på remiss – hur och varför
Statsrådsberedningen, SB PM 2003:2 (reviderad 2009-05-02).
Information för dem som ska svara på remiss finns tillgänglig på regeringen.se/remisser.

Layout: Kommittéservice, Regeringskansliet
Omslag: Elanders Sverige AB
Tryck och remisshantering: Elanders Sverige AB, Stockholm 2021

ISBN 978-91-525-0001-9
ISSN 0375-250X

Till statsrådet Anders Ygeman

Regeringen beslutade vid regeringssammanträde den 26 september 2019 att uppdra åt en särskild utredare att kartlägga och analysera statliga myndigheters behov av säker och kostnadseffektiv it-drift samt hur dessa behov tillgodoses. Utredaren ska vidare analysera säkerhetsmässiga och rättsliga förutsättningar för samordnad statlig it-drift och lämna förslag på mer varaktiga former för sådan it-drift, om det bedöms lämpligt ur ett säkerhetsperspektiv, och de författningsförslag som detta kräver. Utredaren ska också analysera de rättsliga förutsättningarna för statliga myndigheter, kommuner och landsting att med bibehållen säkerhet utkontraktera it-drift till privata leverantörer och vid behov lämna författningsförslag (dir. 2019:64). Tilläggsdirektiv beslutades av regeringen den 2 juli 2020 (dir. 2020:73).

Som särskild utredare förordnades den 20 november 2019 generaldirektören Annelie Roswall Ljunggren.

Som huvudsekreterare anställdes den 17 februari 2020 enhetschefen Tina J Nilsson. Som utredningssekreterare anställdes den 3 februari 2020 departementssekreteraren Alexander Wall, den 1 april 2020 rådmannen Nils Sjöblom och den 10 augusti 2020 verksjuristen Eva Maria Broberg Lennartsson. Som utredningssekreterare anställdes under perioden den 2 december 2019 till den 30 april 2020 verksamhetsutvecklaren Sofia Allansson. Som utredningssekreterare anställdes under perioden den 3 februari 2020 till den 31 mars 2020 departementssekreteraren Ingela Alverfors.

Som experter att biträda utredningen förordnades den 3 februari 2020 kanslirådet Maria Fahlén, kanslirådet Nils Fjelkegård, ämnesrådet Sara Jendi Linder, departementssekreteraren Emelie Juter, departementssekreteraren Helen Kasström, rättssakkunnige Linnea Munkhammar, kanslirådet Fredrik Sandberg och departementssekreteraren Daniel Zerea. Den 1 april 2020 förordnades departementssekreteraren Ingela Alverfors som expert i utredningen. Emelie Juter entledigades från sitt upp-

drag den 14 april 2020 och samma dag förordnades departementssekreteraren Charlotte Koutras som expert i utredningen. Sara Jendi Linder entledigades från sitt uppdrag den 9 juni 2020 och samma dag förordnades kanslirådet Karina Aldén som expert i utredningen.

Den 13 mars 2020 fastställdes att följande personer skulle ingå i den referensgrupp som Infrastrukturdepartementet bjudit in till att biträda utredningen: Magnus Bergström, Datainspektionen; Anders Parmér, Fortifikationsverket; Maria Danielsson, Försäkringskassan; Anna Granström, Lantmäteriet; Nichlas Blomqvist, Länsstyrelsen Västra Götaland; Jan Zetterdahl, Myndigheten för digital förvaltning; Jonas Paulson, Myndigheten för samhällsskydd och beredskap; Peder Sjölander, Skatteverket; Marie Holmberg, Statens servicecenter; Victoria Ekstedt, Säkerhetspolisen; Monica Svingen, Trafikverket; Ann-Marie Eklund Löwinder, Internetstiftelsen; Pär Nygårds, IT&Telekomföretagen samt Lotta Nordström, Sveriges Kommuner och Regioner. Jan Zetterdahl, Myndigheten för digital förvaltning, ersattes den 1 september 2020 av Annika Bränström från samma myndighet. Maria Danielsson, Försäkringskassan, har under perioden den 23 september 2020 till den 1 februari 2021 ersatts av Ann-Louis Söderman från samma myndighet.

Utredningen redogör för uppdraget i vi-form, även om det inte funnits fullständig samsyn i alla delar.

Utredningen, som har antagit namnet It-driftsutredningen (I 2019:03), överlämnar härmed delbetänkandet *Säker och kostnadseffektiv it-drift – rättsliga förutsättningar för utkontraktering* (SOU 2021:1).

Stockholm i december 2020

Annelie Roswall Ljunggren

/Tina J Nilsson
Eva Maria Broberg Lennartsson
Nils Sjöblom
Alexander Wall

Innehåll

Bilagor

Vissa förkortningar

EU-rättsakter

dataskyddsdirektivet	Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF
dataskyddsförordningen	Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG
NIS-direktivet	Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen

Övriga förkortningar

AD	Arbetsdomstolen
US CLOUD Act	Clarifying Lawful Overseas Use of Data Act
dir.	direktiv
Digg	Myndigheten för digital förvaltning
Ds	Departementsserien
EDPB	Europeiska dataskyddsstyrelsen
eSamverkansprogrammet	eSam
ESV	Ekonomistyrningsverket
EU	Europeiska unionen
Europadomstolen	Europeiska domstolen för de mänskliga rättigheterna
Europakonventionen	Europeiska konventionen den 4 november 1950 angående skydd för de mänskliga rättigheterna och de grundläggande friheterna
FFS	Försvarsmaktens föreskrifter
FL	förvaltningslagen (2017:900)
HFD	Högsta förvaltningsdomstolen
HD	Högsta domstolen
IaaS	Infrastructure as a Service
JO	Riksdagens ombudsmän
LOU	lagen (2016:1145) om offentlig upphandling
MSB	Myndigheten för samhällsskydd och beredskap
MSBFS	Myndigheten för samhällsskydd och beredskaps föreskrifter
NJA	Nytt Juridiskt Arkiv
OECD	Organisationen för ekonomiskt samarbete och utveckling
OSL	offentlighets- och sekretesslagen (2009:400)
PaaS	Platform as a Service

PMFS	Säkerhetspolisens föreskrifter
Prop.	regeringens proposition
RÅ	Regeringsrättens årsbok
SaaS	Software as a Service
SCB	Statistiska centralbyrån
SOU	Statens offentliga utredningar
SSC	Statens servicecenter
SvKFS	Affärsverket svenska kraftnäts föreskrifter
TF	tryckfrihetsförordningen
TFS	Transportstyrelsens föreskrifter
Tystnadspliktslagen	lagen (2020:914) om tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter

Sammanfattning

Inledning

En säker och kostnadseffektiv it-drift är en förutsättning för den offentliga förvaltningens digitalisering. Statliga myndigheter, kommuner och regioner ansvarar för att verksamhetens it-driftslösningar stödjer en effektiv verksamhetsutveckling och uppfyller krav på säkerhet (säkerhetsskydd, sekretess och dataskydd) och kostnadseffektivitet. It-drift kan bedrivas i egen regi, genom utkontraktering till tjänsteleverantör eller genom samordnad it-drift. Vilken it-driftslösning som är den mest lämpade beror på verksamhetens uppdrag och vilka uppgifter som hanteras i verksamheten.

Utkontraktering av it-drift och användning av molntjänster är ett vanligt sätt för statliga myndigheter, kommuner och regioner att hantera sin it-drift. Det råder dock en viss osäkerhet bland dessa aktörer när det gäller de rättsliga förutsättningarna för utkontraktering av it-drift till privata tjänsteleverantörer. Osäkerheten gäller främst tolkningen av när en uppgift ska anses röjd enligt sekretesslagstiftningen och om det utifrån ett säkerhetsperspektiv är lämpligt att utkontraktera it-drift. Detta medför att en del aktörer avvaktar med beslut om it-drift, vilket kan få negativa konsekvenser för verksamhetens utveckling, säkerhet och kostnad.

Vårt uppdrag och innehållet i delbetänkandet

Syftet med utredningen är enligt våra direktiv att ”skapa bättre förutsättningar för den offentliga förvaltningen att få tillgång till säker och kostnadseffektiv it-drift genom antingen samordnad statlig it-drift eller genom tydligare rättsliga förutsättningar för att kunna anlita privata leverantörer av it-drift”.

I detta delbetänkande fokuserar vi på förutsättningarna för statliga myndigheter, kommuner och regioner att utkontraktera it-drift. Vi redovisar en rättslig analys av förutsättningarna för utkontraktering av it-drift till privata tjänsteleverantörer och lämnar två författningsförslag: ett förslag till sekretessbrytande bestämmelse i OSL om utkontraktering av it-drift och ett förslag om inskränkt meddelarfrihet. I delbetänkandet redovisar vi också en kartläggning av statliga myndigheters it-drift och en omvärldsanalys med erfarenheter från andra länder.

I vårt slutbetänkande som ska redovisas senast den 15 oktober 2021 kommer vi att fokusera på samordnad statlig it-drift. Vi kommer att analysera svenska erfarenheter av samordnad statlig it-drift och de säkerhetsmässiga och rättsliga förutsättningarna för samordnad it-drift. Vi redovisar också våra förslag om samordnad, säker och kostnadseffektiv statlig it-drift.

Vår kartläggning av statliga myndigheters it-drift

Vår kartläggning bygger på en enkät till 200 statliga myndigheter, fallstudier av fem myndigheter och en workshop med företrädare för 16 myndigheter. Vi har analyserat myndigheternas informationshantering och säkerhet, hur deras it-drift och kostnader för it-drift ser ut i dag, deras framtida behov av it-drift och vilka eventuella hinder för säker och kostnadseffektiv it-drift som finns.

Både små och stora myndigheter bedriver samhällsviktig verksamhet och hanterar uppgifter som ställer höga krav på säkra it-driftslösningar. Kartläggningen visar att nästan 90 procent av de 158 myndigheter som besvarat enkäten hanterar någon form av skyddsvärd information i sin verksamhet. Vanligast är att myndigheterna hanterar olika typer av sekretessreglerade uppgifter och känsliga personuppgifter. Hälften av myndigheterna arbetar systematiskt med informationssäkerhet i hela eller delar av verksamheten, medan hälften endast har påbörjat eller ska påbörja sitt informationssäkerhetsarbete.

De största hindren för säker it-drift är bristande informationsklassificering och avsaknad av kompetens inom it och säkerhet men också beställarkompetens. Kompetensbrist ses som en riskfaktor för säker it-drift både bland små och stora myndigheter. De största

hindren för kostnadseffektiv it-drift är höga krav på säkerhet, olika typer av inlåsningseffekter men även kompetensbrist.

Vår enkät visar att myndigheternas it-drift både skiljer sig åt och har stora likheter. Många myndigheter har utkontrakterat it-drift på något sätt, t.ex. genom att använda molntjänster från tjänsteleverantörer. Bland myndigheterna uppger 33, 32 och 95 procent att de använder någon form av IaaS-, PaaS- respektive SaaS-tjänster. Kartläggningen visar även att myndigheterna har behov av it-drift i egen regi och att det i dag finns minst 220 datacenter i den svenska statsförvaltningen. Dessa datacenter är dock av varierande karaktär, från större serverhallar till mindre utrymmen i myndigheternas lokaler. Större myndigheter har i regel högre kostnader för it-drift. Dock finns ett särskilt tydligt samband mellan de som har höga it-driftskostnader och de som bedriver samhällsviktig verksamhet eller som omfattas av förordningen om intern styrning och kontroll. Många myndigheter har samordnat sin it-drift med andra myndigheter. Denna samordning har i flera fall skett på initiativ av myndigheterna själva och omfattar allt från enklare applikationsdrift till att en myndighet tillhandahåller all it-verksamhet åt en annan myndighet som ett helhetsåtagande.

När det gäller framtida behov ser många myndigheter att de fortsatt har behov av att kunna utkontraktera it-drift och använda molntjänster samt att bedriva viss it-drift i egen regi. Många myndigheter pekar på behovet av att de rättsliga förutsättningarna för utkontraktering tydliggörs. Många myndigheter (57 procent) är även intresserade av en samordnad statlig it-drift. Uppfattningarna varierar något om vilka tjänster som bör ingå i ett samordnat åtagande, men många framhåller att fokus bör ligga på standardiserade tjänster.

Erfarenheter från andra länder

I Danmark, Finland och Nederländerna har inriktningen för den digitala förvaltningen inneburit att it-driftsrelaterade resurser och processer koncentrerats och konsoliderats till ett fåtal organisationer och servicecenter. Denna inriktning skiljer sig något mot utvecklingen i Storbritannien, och sedermera Norge, där marknadsplatser för molntjänster etablerats i syfte att göra det lättare för offentliga verksamheter att upphandla it-tjänster. Bakomliggande motiv till

samtliga länders strategier har dock varit effektivisering och kostnadsbesparingar. I Storbritannien anfördes även möjligheten att främja brittiska små- och medelstora it-tjänsteleverantörer som argument. Flera av länderna framhåller att genomförda reformer lett till effektivisering, men framför allt förbättrade möjligheter till digital utveckling. Dock är det svårt att veta exakt hur effektiva satsningarna har varit då länderna inte genomfört jämförbara utvärderingar både före och efter reformerna.

Samtliga länder i omvärldsanalysen lyfter en liknande problematik med osäkerhet avseende de rättsliga förutsättningarna för utkontraktering av it-verksamhet. Ett ökat fokus på informations- och cybersäkerhet har lett till att länderna upprättat nationella cybersäkerhetsmyndigheter och kompetenscentra. Det är möjligt att båda ansatser med servicecenter och marknadsplatser för molntjänster lett till en koncentration av kompetens avseende bl.a. it-säkerhet och att upphandling gett förutsättningar för kravställning som bidragit till bättre informationssäkerhet.

Överföring av personuppgifter till tredjeland enligt dataskyddsförordningen

Det är bara tillåtet att överföra personuppgifter till en mottagare i ett land utanför EU eller EES om det kan ske på någon av de grunder som anges i kapitel V i dataskyddsförordningen. Vi bedömer att det utgör en överföring av personuppgifter till tredjeland när en personuppgiftsansvarig eller ett personuppgiftsbiträde behandlar personuppgifter genom användning av utrustning som finns i tredjeland. Det saknar betydelse hur lång eller kort tid som utrustningen används, och om uppgifterna är krypterade eller pseudonymiserade – det är ändå fråga om personuppgifter och en överföring av sådana uppgifter.

Standardavtalsklausuler är en lämplig skyddsåtgärd som kan läggas till grund för överföring av personuppgifter till tredjeland om det i mottagarens land finns ett grundläggande rättighetsskydd och en möjlighet att göra detta skydd gällande inför domstol eller annan oberoende instans. EU-domstolen har ogiltigförklarat ett beslut som kommissionen fattat om att det finns en adekvat skyddsnivå för personuppgifter i USA, mot bakgrund att det grundläggande rättsskyddet i USA inte ger en sådan nivå av skydd som krävs enligt dataskydds-

förordningen. Vår bedömning är att domstolens konstateranden avseende rättsläget i USA vad gäller inskränkningar av grundläggande rättigheter och tillgången till rättsmedel och oberoende prövning äger giltighet även i förhållande till övriga grunder för överföring av personuppgifter till USA enligt dataskyddsförordningen, eftersom kravet på skyddsnivå är densamma oavsett vilken grund som tillämpas.

Utkontraktering och röjande

Vi bedömer att en myndighet som utkontrakterar it-drift har lämnat ut de uppgifter som omfattas av utkontrakteringen till tjänsteleverantören. Detta gäller oavsett om omständigheterna när uppgifterna tillgängliggjordes tjänsteleverantören var sådana att man – t.ex. pga. kryptering eller annan teknisk säkerhetsåtgärd – inte måste ha räknat med att tjänsteleverantören eller någon annan utomstående skulle komma att ta del av uppgifterna. Uppgifterna är röjda enligt offentlighets- och sekretesslagen (2009:400) eftersom ett utlämnande är en form av röjande.

Förslag till en sekretessbrytande bestämmelse

Vi föreslår att det i 10 kap. 2 a § OSL införs en sekretessbrytande bestämmelse som tar sikte på fall då uppgifter lämnas ut till företag eller en annan enskild (tjänsteleverantör) eller till en annan myndighet som har i uppdrag att utföra endast teknisk bearbetning eller teknisk lagring av de uppgifter som lämnas ut för den utlämnande myndighetens räkning.

Ett utlämnande ska – enligt den föreslagna bestämmelsen – inte ske om övervägande skäl talar för att det intresse som sekretessen ska skydda har företräde framför intresset av utkontraktering.

En inskränkt meddelarfrihet

Vi föreslår att meddelarfriheten enligt tryckfrihetsförordningen och yttrandefrihetsgrundlagen ska inskränkas för den krets av personer som träffas av tystnadspliktslagen.

Summary

Introduction

Secure and cost-effective IT operations are essential to the digitalisation of public administration. Government agencies, municipalities and regions are responsible for ensuring that the IT operations for their activities support effective development of these activities and meet requirements concerning security (protective security, secrecy and data protection) as well as cost-effectiveness. IT operations can be provided in-house, by outsourcing to a service provider or through shared IT operations. What type of IT operations are most appropriate depends on the kind of activities and what type of data is handled in those activities.

The outsourcing of IT operations and the use of cloud services is a common way for government agencies, municipalities and regions to handle their IT operations. However, there is some uncertainty among public actors regarding the legal conditions for outsourcing IT operations to service suppliers. This uncertainty mainly concerns the interpretation of when information is considered to have been disclosed under secrecy legislation and whether it is appropriate, from a security perspective, to outsource IT operations. As a result, some public actors are waiting to make decisions about IT operations, and this may have negative consequences for the development, security and cost of their activities.

Our remit and the content of this interim report

According to our terms of reference, the purpose of this inquiry is to "create better conditions for access by public administration to secure and cost-effective IT operations either through coordinated

central government IT operations or through clearer legal conditions for being able to engage private suppliers of IT operations".

In this interim report we focus on the conditions for the outsourcing of IT operations by government agencies, municipalities and regions. We present a legal analysis of the conditions for the outsourcing of IT operations to service providers and present proposals for two legislative amendments: a proposal for a secrecy-override provision in the Public Access to Information and Secrecy Act on the outsourcing of IT operations and a proposal for restricted freedom to communicate. In this interim report we also present a survey of the IT operations of government agencies and a comparative analysis of experience from other countries.

In our final report, to be presented by 15 October 2021, we will focus on coordinated central government IT operations. We will analyse the Swedish experience of coordinated central government IT operations and the security and legal conditions for coordinated IT operations. We will also present our proposals regarding coordinated, secure and cost-effective central government IT operations.

Our survey of government agencies' IT operations

Our survey is based on a questionnaire to 200 government agencies, case studies of five agencies and a workshop attended by representatives of 16 agencies. We have analysed the agencies' information management and security; what their IT operations and costs for IT operations are like today; their future needs of IT operations; and what potential obstacles may be to secure and cost-effective IT operations.

Both small and large agencies conduct critical activities and manage tasks that require a high standard of IT operations. Our survey shows that almost 90 percent of the 158 agencies that replied to the questionnaire handle some form of information worthy of protection in their activities. The most common situation is the handling of various types of information subject to secrecy and sensitive personal data. Half of the agencies are working systematically on information security in all or parts of their activities, while half have only started or are going to start their information security work.

The greatest obstacles to secure IT operations are deficient information classification and a lack of expertise in IT and security, as well as of procurement expertise. Lack of expertise is seen as a risk factor for secure IT operations among both small and large agencies. The greatest obstacles to cost-effective IT operations are high security requirements and various types of lock-in effects, as well as shortages of expertise.

Our survey shows that agencies' IT operations both differ yet have great similarities. Many agencies have outsourced IT operations in some way, e.g. by using cloud service providers. Among the agencies, 33, 32 and 95 percent respectively say that they use some form of Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). Our survey also shows that agencies need in-house IT operations and that, at present, there are at least 220 data centres in Sweden's central government administration. However, the nature of these data centres varies from more advanced data centres to small server rooms in the agencies' premises. In general, large agencies have higher costs for IT operations. However, there is a particularly clear correlation between those that have high IT operating costs and those that provide critical services or must apply the Internal Control Ordinance. Many agencies have coordinated their IT operations with other agencies. This coordination has often come about on the initiative of the agencies themselves and covers everything from simple application hosting to one agency providing most IT services for another agency comparable to an external IT department.

When it comes to future needs, many agencies see that they have a continued need to be able to outsource IT operations and use cloud services as well as to conduct some in-house IT operations. Many agencies point to the need to clarify the legal conditions for outsource. Many agencies (57 percent) are also interested in coordinated central government IT operations. Views vary to some extent about what services should be included in a coordinated central government undertaking, but many stress that the focus should be on standardised services.

Experience from other countries

In Denmark, Finland and the Netherlands the focus of digital management has meant that resources and processes related to IT operations have been concentrated and consolidated in a few organisations and service centres. This approach differs to some extent from the situation in the UK, and subsequently in Norway, where market places for cloud services have been established to make it easier for public actors to procure IT services. However, the motive underlying the strategies of all these countries has been greater effectiveness and cost savings. In the UK the possibility of promoting national small and medium-sized IT service providers was also put forward as an argument. Several of the countries stress that the reforms implemented have led to greater effectiveness, but especially to better possibilities for digital development. However, it is difficult to know exactly how effective their initiatives have been since the countries have not conducted comparable evaluations before and after their reforms.

All the countries in the analysis highlight similar problems with a perceived uncertainty regarding the legal conditions for outsourcing IT operations. A greater focus on information and cyber security has led to the countries setting up national cyber security agencies and centres of expertise. It is possible that service centre approaches and approaches using market places for cloud services have both led to a concentration of expertise in areas including IT security and that procurement has made it possible to specify requirements that have contributed to better information security.

Transfer of personal data to third countries under the Data Protection Regulation

The transfer of personal data to a recipient in a country outside the EU and EEA is only permitted if it can take place on one of the grounds specified in Chapter V of the Data Protection Regulation. We make the assessment that there is a transfer of personal data to a third country when a controller or processor processes personal data by using equipment located in a third country. How long or short a period of time the equipment is used for is of no importance, nor is whether the data is encrypted or pseudonymised – it still involves personal data and a transfer of such data.

Standard contractual clauses are a suitable safeguard that can form the basis for the transfer of personal data to a third country if the country of the recipient has a level of protection of fundamental rights essentially equivalent to that guaranteed in the EU legal order and a possibility of asserting this protection before a court of another independent body.

The Court of Justice of the European Union has declared a decision made by the Commission that there is an adequate level of protection for personal data in the US invalid in the light of the fact that the protection of fundamental rights in the US does not provide the level of protection that is required under the Data Protection Regulation. Our assessment is that the Court's observations regarding the legal situation in the US concerning restrictions of fundamental rights and access to legal remedies is also valid in relation to the other grounds for transfer of personal data to the US under the Data Protection Regulation, since the same level of protection is required irrespective which ground is applied.

Outsourcing and disclosure

It is our assessment that when an agency outsource IT operations it implies that the information subject to secrecy that is subject to the outsourcing is disclosed in the meaning of the Public Access to Information and Secrecy Act to the service provider, irrespective of whether the information is encrypted or subject to other technical measures.

Proposal of a secrecy-override provision

We propose adding a secrecy-override provision to Chapter 10, Section 2 a of the Public Access to Information and Secrecy Act that is aimed at cases where information is released to a company or another private party (service supplier) or to another agency that is commissioned to carry out solely technical processing or storage of the information released on behalf of the releasing agency.

Under the proposed provision, the information shall not be released if overriding reasons indicate that the interest to be protected by the secrecy takes precedence over the interest of outsourcing.

Restriction of the freedom to communicate

We propose that the freedom to communicate under the Freedom of the Press Act and the Fundamental Law on Freedom of Expression be restricted for the group of persons covered by the Act on the obligation to observe secrecy in the outsourcing of technical processing or storage of data (2020:914).

1 Författningsförslag

1.1 Förslag till lag om ändring i offentlighets- och sekretesslagen (2009:400)

Härigenom föreskrivs i fråga om offentlighets- och sekretesslagen (2009:400)

dels att det ska införas en ny paragraf, 10 kap. 2 a §, och en ny rubrik före 10 kap. 2 a § av följande lydelse

dels att 44 kap. 5 § ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	10 kap.
	Utkontraktering av teknisk bearbetning eller lagring av uppgifter
	2 a §
	Sekretess hindrar inte att en uppgift lämnas ut till ett företag eller en annan enskild eller till en annan myndighet som har i uppdrag att utföra endast teknisk bearbetning eller teknisk lagring av de uppgifter som lämnas ut för den utlämnande myndighetens räkning.
	En uppgift ska inte lämnas ut om det intresse som sekretessen ska skydda har företräde framför intresset av att uppgiften lämnas ut.

44 kap.

5 §

Rätten enligt 1 kap. 1 och 7 §§ tryckfrihetsförordningen och 1 kap. 1 och 10 §§ yttrandefrihetsgrundlagen att meddela och offentliggöra uppgifter inskränks av den tystnadsplikt som följer

1. av beslut som har meddelats med stöd av 7 § lagen (1999:988) om förhör m.m. hos kommissionen för granskning av de svenska säkerhetstjänsternas författningsskyddande verksamhet,

2. av 7 kap. 1 § 1 lagen (2006:544) om kommuners och regioners åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap,

3. av 4 kap. 16 § försäkringsrörelselagen (2010:2043),

4. av 5 kap. 15 § lagen (1998:293) om utländska försäkringsgivares och tjänstepensionsinstituts verksamhet i Sverige, *och*

5. av 32 § lagen (2020:62) om hemlig dataavläsning.

4. av 5 kap. 15 § lagen (1998:293) om utländska försäkringsgivares och tjänstepensionsinstituts verksamhet i Sverige,

5. av 32 § lagen (2020:62) om hemlig dataavläsning, *och*

6. av 4 § lagen (2020:914) om tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter.

Denna lag träder i kraft den 1 januari 2022.

2 Utredningens uppdrag och arbete

2.1 Utredningens uppdrag

Regeringen beslutade den 26 september 2019 att ge en särskild utredare i uppdrag att kartlägga och analysera statliga myndigheters behov av säker och kostnadseffektiv it-drift samt hur dessa behov tillgodoses (bilaga 1). Utredaren ska också analysera säkerhetsmässiga och rättsliga förutsättningar för samordnad statlig it-drift och lämna förslag på mer varaktiga former för sådan it-drift, om det bedöms lämpligt ur ett säkerhetsperspektiv, och de författningsförslag som detta kräver. Utredaren ska vidare analysera de rättsliga förutsättningarna för statliga myndigheter, kommuner och regioner att med bibehållen säkerhet utkontraktera it-drift till privata leverantörer och vid behov lämna författningsförslag.

Syftet med utredningen är att skapa bättre förutsättningar för den offentliga förvaltningen att få tillgång till säker och kostnadseffektiv it-drift genom antingen samordnad statlig it-drift eller tydligare rättsliga förutsättningar för att kunna anlita privata leverantörer av it-drift.

Enligt direktiven ingår följande delar i uppdraget:

- Kartläggning och analys av statliga myndigheters behov av it-drift
- Omvärldsanalys för att kartlägga och analysera relevanta modeller för myndigheters it-drift nationellt och internationellt
- Analys av de rättsliga förutsättningarna för utkontraktering av it-drift till privata leverantörer
- Utvärdering av Försäkringskassans regeringsuppdrag om samordnad och säker statlig it-drift

– Analys av säkerhetsmässiga och rättsliga förutsättningar för samordnad statlig it-drift
– Förslag på varaktiga former för samordnad statlig it-drift
– Konsekvensanalys.

Genom tilläggsdirektiv den 2 juli 2020 (bilaga 2) förlängdes utredningstiden. Uppdragen att kartlägga och analysera statliga myndigheters it-drift och de rättsliga förutsättningarna för utkontraktering, inklusive eventuella författningsförslag, ska redovisas senast den 15 januari 2021. Uppdraget att föreslå mer varaktiga former för samordnad statlig it-drift ska redovisas senast den 15 oktober 2021.

2.2 Centrala begrepp

I detta betänkande förekommer ett antal begrepp som är centrala i utredningen. Det handlar om begreppen *säker*, *kostnadseffektiv*, *it-drift* och *utkontraktering*. Begreppen har inga generellt fastlagda definitioner utan de beskrivs vanligen utifrån det sammanhang de används i. Vi har därför behövt definiera hur begreppen ska användas i uppdraget. Begreppen säker och kostnadseffektiv it-drift behöver dessutom ställas i relation till och balanseras gentemot varandra.

2.2.1 Säker

I utredningsdirektiven relateras begreppet *säker* till de krav som ställs för säkerhetsskydd, informationssäkerhet samt sekretess och skydd för den personliga integriteten.

Begreppet säkerhet avser i säkerhetsskyddslagen (2018:585) verksamheter och hantering av uppgifter som rör Sveriges säkerhet. I lagen specificeras vilka verksamheter som omfattas av lagen och vad som avses med begreppet säkerhetsskydd och säkerhetsskyddsklassificerade uppgifter. Både offentliga och privata aktörer ska utifrån säkerhetsskyddslagen bedöma om de bedriver verksamhet som är av betydelse för Sveriges säkerhet och om de hanterar säkerhetsskyddsklassificerade uppgifter samt vidta åtgärder med anledning av detta.

Informationssäkerhet innebär att information, oavsett vilken den är, får det skydd som behövs avseende konfidentialitet, riktighet och tillgänglighet. Det gäller såväl hos enskilda som hos organisationer, både i näringslivet och i offentlig verksamhet. Informationssäkerhet omfattar därför hela samhället. Ett systematiskt och riskbaserat informationssäkerhetsarbete syftar till att skapa förutsättningar för att över tid upprätthålla informationssäkerhet som svarar mot identifierade behov. Reglering som ställer krav på organisationer att bedriva ett systematiskt och riskbaserat arbete finns främst i förordning (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap samt lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.

Dataskydd är ett begrepp som används för att ange skyddet för den personliga integriteten i de regelverk som ska tillämpas vid behandling av personuppgifter. Med säker avses här att aktörer som behandlar personuppgifter måste säkerställa en lämplig nivå av informationssäkerhet vid behandlingen. Dataskyddsregelverket är dock inte begränsat till ett krav på säkerhet, utan behandlingen av personuppgifter måste ske i enlighet med dataskyddsregelverket i sin helhet.

Begreppet säker i relation till it-drift kan avse olika nivåer i samhället – från säkerhet för enskilda personer, verksamheter eller sektorer, till säkerhet för riket som helhet. Beroende på verksamhet och vilka uppgifter som hanteras i verksamheten ställs olika krav på säkerhet. Varje aktör ansvarar för att klargöra vilka krav på säkerhet deras verksamhet och uppgifter omfattas av. Samtidigt måste definitionen av säker omfatta även ett bredare samhällsperspektiv, dvs. hela den offentliga förvaltningen. Utifrån detta resonemang behöver begreppet säker definieras både på aktörs- och samhällsnivå. På samhällsnivå bör begreppet relateras till olika hotbilder i samhället.

Med *säker* på *aktörsnivå* avses att en offentlig aktörs it-drift lever upp till för verksamheten rättsliga och säkerhetsmässiga krav, exempelvis krav på säkerhetsskydd och informationssäkerhet samt sekretess och skydd för den personliga integriteten. I begreppet ingår även förmåga att kontinuerligt bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete som omhändertar förändrade krav och risker. Detta innebär att säkerhet för en aktör ska bedömas utifrån de olika förutsättningar i samhället under vilka aktören ska verka enligt sitt uppdrag. Säkerhet kan därför inte endast bedömas utifrån

informationsklass eller tillgänglighet i normalläget utan även vid samhällskriser eller höjd beredskap.

Med *säker på samhällsnivå* avses att it-driften i den offentliga förvaltningen som helhet är organiserad på ett sådant sätt att den kan stå emot olika störningar och hotnivåer i samhället. I detta sammanhang är begreppet robusthet nära kopplat till säker, dvs. en förmåga att stå emot störningar till följd av såväl yttre som inre påverkan. Det handlar här inte bara om tillgänglighetsaspekten utan exempelvis även störningar orsakade av att information blir obehörigt förändrad och inte kan användas på avsett sätt. En robust och säker it-driftslösning på samhällsnivå tar hänsyn till olika typer av risker, exempelvis vad gäller koncentration av data eller störningar i andra infrastrukturer såsom elektroniska kommunikationer som tillgången till it-driftslösningen är beroende av. Den tar också hänsyn till olika former av naturhändelser, skadegörelse och inbrott samt beroende på skyddsvärdet även antagonistiska angrepp och förhållanden som råder under höjd beredskap och krig. Detta blir särskilt relevant när det gäller lösningar för en samordnad statlig it-drift. Om säkerheten hos enskilda aktörer är låg kan en samordnad lösning bidra till att höja säkerheten både för den enskilda aktören och för en större del av samhället som helhet. Det har även betydelse ur ett totalförsvarsperspektiv.

2.2.2 Kostnadseffektiv

Enligt budgetlagen (2011:203) ska hög effektivitet eftersträvas i statens verksamhet och god hushållning iakttas. Av myndighetsförordningen (2007:515) framgår att myndigheter ska hushålla väl med statens medel. Kommuner och regioner ska enligt kommunallagen (2017:725) ha en god ekonomisk hushållning i sin verksamhet.

Kostnadseffektivitet avser förhållandet mellan de resurser som används och hur väl ett mål eller förväntat resultat uppnås. Offentliga aktörer ska inte använda mer resurser än vad som är nödvändigt för att uppnå de krav som ställs på verksamheten.

När det gäller it-drift kan kostnadseffektiviteten påverkas av flera faktorer, som t.ex. dimensioneringen av it-drift, val av it-driftslösning (egen regi, utkontraktering eller samordnad it-drift), utbudet av tjänster och leverantörer, tjänsternas utformning (exempelvis skal-

barhet) och avtalsrelaterade frågor. Leverantörsberoenden och andra inlåsningseffekter kan påverka kostnadseffektiviteten negativt. Långsiktiga avtal med en leverantör som har stora kunskaper om verksamheten kan å andra sidan vara en kostnadseffektiv lösning.

Utifrån utredningens uppdrag om säker och kostnadseffektiv it-drift måste kostnadseffektivitet också ställas i relation till säkerhet. Behovet av säkerhet varierar mellan aktörer, verksamheter, inom verksamheter och beroende på vilka uppgifter som hanteras. Varje aktör måste utifrån de krav som ställs på verksamheten göra en riskanalys och utifrån den avgöra vilken säkerhet som krävs och hitta kostnadseffektiva lösningar för it-driften. En alltför hög säkerhetsnivå i förhållande till de krav som ställs kan ge för höga kostnader. Å andra sidan kan en för låg säkerhet, utöver rent säkerhetsmässiga konsekvenser, ge ökade kostnader i form av minskat förtroende för verksamheten och de tjänster som erbjuds.

För att hitta rätt balans mellan säkerhet och kostnad kan begreppet *ändamålsenlig* användas. En ändamålsenlig lösning för it-drift innebär att den uppfyller de krav på funktion och säkerhet som ställs i olika delar av verksamheten till lägsta möjliga kostnad.

Precis som med begreppet säker bör kostnadseffektivitet analyseras både på aktörsnivå och på samhällsnivå. En it-driftslösning som är kostnadseffektiv för en enskild aktör behöver inte vara det för en annan. På samhällsnivå kan en gemensam it-driftslösning vara kostnadseffektiv och ändamålsenlig om den anpassas till gemensamma behov och krav på säkerhet.

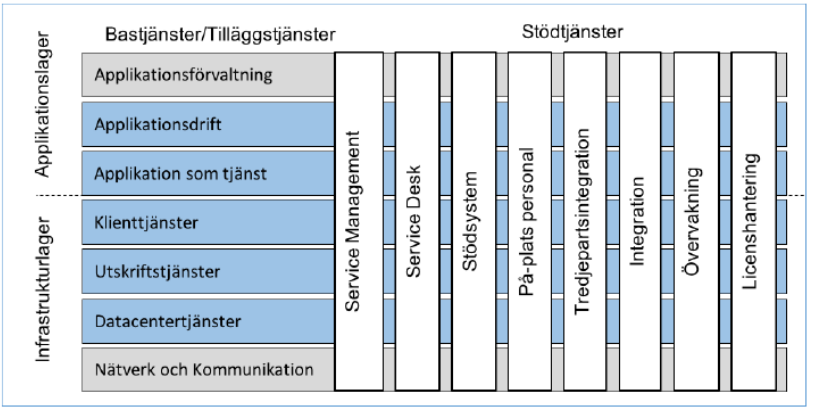
2.2.3 It-drift

It-drift är ett begrepp vars innebörd förändras i och med utvecklingen av utbud och efterfrågan av nya it-tjänster på marknaden. Enligt utredningsdirektiven har it-drift ingen ”tydlig avgränsning utan omfattar både fysisk hårdvara som servrar och datorer, och mjukvara som datorprogram och operativsystem”. I Kammarkollegiets vägledning för avrop på ramavtalet för ”IT Drift” används begreppet för

> […] både ’traditionell’ serverdrift som produceras av leverantören (eller hos underleverantör) och tredjepartstjänster (t.ex. molntjänster) som produceras av tredjepartsleverantör; exempelvis avseende applikationer, datorkapacitet, klienthanteringstjänster, datalagring och säkerhetskopiering.

It-drift beskrivs bestå av ett antal tjänster som antingen bygger på varandra eller kompletterar varandra (Figur 2.1).

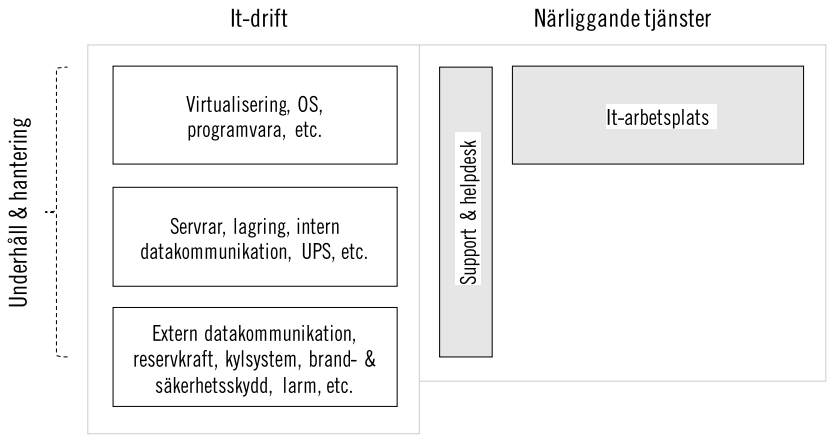
Figur 2.1 Kammarkollegiets modell för it-drift



Källa: Statens inköpscentral, Vägledning för avrop från IT Drift.

I betänkandet har vi valt att beskriva it-drift som en aktivitet snarare än en tjänst, närmare bestämt aktiviteten att underhålla och hantera hårdvara och mjukvara (Figur 2.2). Detta hindrar dock inte att denna aktivitet kan paketeras som en tjänst, vilken den ofta gör. Beskrivningen underhåll och hantering av hård- och mjukvara har potential att omfatta det mesta en it-avdelning gör. Det som är specifikt för it-drift är dock att denna aktivitet syftar till att skapa förutsättningar för att utveckla eller förvalta de system och applikationer en verksamhet använder, dvs. de tidiga aktiviteter i en värdekedja som leder fram till slutanvändaren. Uttryckt på ett annat sätt bör t.ex. inte systemutveckling betraktas som it-drift med detta synsätt, men däremot underhåll och hantering av de fysiska eller virtuella serverar som utvecklade system körs på. Det bör understrykas att det i praktiken kan vara svårt att skilja it-drift från t.ex. it-förvaltning. Nya metoder och arbetssätt inom systemutveckling har dessutom gjort att rollerna för utvecklare, förvaltare och it-driftstekniker överlappar varandra i allt större utsträckning. Mot bakgrund av denna problematik har vi valt en allmänt hållen beskrivning, med ansatsen att försöka avgränsa oss i sammanhang där det är möjligt, snarare än att slå fast en snäv definition som riskerar att bli svår att tillämpa.

Figur 2.2 It-drift och närliggande tjänster



Källa: Egen illustration.

I Kammarkollegiets definition av it-drift är tjänstebegreppet centralt. Tjänst beskriver här ”de leveranser som utförs för att uppfylla ställda krav eller avtalad specifikation, enligt en fördefinierad leveransprocess”. För vissa typer av it-tjänster är det vanligt att tala om tjänstenivåavtal (eng. Service Level Agreement) som reglerar skyldigheter och rättigheter mellan en beställare och en utförare. I betänkandet använder vi begreppet tjänst för att beskriva vad som levereras inom ramen för en affärsmässig transaktion mellan en upphandlande myndighet och en privat tjänsteleverantör, en överenskommelse mellan myndigheter eller internt inom en verksamhet. Konsekvensen av detta synsätt är att it-drift är en aktivitet som kan tillhandahållas som en tjänst i samband med utkontraktering till tjänsteleverantör, men även genom samordning inom staten eller t.o.m. inom en verksamhet. Det bör dock poängteras att det inte är naturligt för alla verksamheter att beskriva it-drift som en tjänst, eftersom aktiviteten och transaktionen inte alltid är formaliserad.

Utöver it-drift har vi valt att definiera hantering och underhåll av it-arbetsplats och support som närliggande tjänster. Support och helpdesk avser i detta sammanhang sådana servicefunktioner som finns till för slutanvändare, dvs. medarbetare i myndigheternas kärnverksamheter. Teknisk support är även en naturlig del av det underhåll och den hantering av hårdvara och mjukvara som utgör it-drift, men riktar sig då främst till it-avdelningar.

En annan närliggande tjänst är samlokalisering av servrar och annan it-utrustning, vilket också kallas co-location. Med samlokalisering avses vanligtvis att en myndighet eller ett företag hyr ett utrymme i ett annat företags datacenter där myndigheten eller företaget kan ställa servrar och annan it-utrustning.

2.2.4 Molntjänster

It-drift är en nödvändig del i att tillhandahålla molntjänster och i vissa fall används molntjänster och it-driftstjänster synonymt. Molntjänst används för att beskriva en viss typ av it-tjänst som går ut på att leverera datorresurser organiserade i ett datormoln. Datormoln kommer från engelskans ”Cloud Computing” och finns numera definierat i en rad standarder och specifikationer. Begreppet finns även definierat i 2 § 7 p. i lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster, där det framgår att en molntjänst är

> är en tjänst som möjliggör tillgång till en skalbar och elastisk pool av delbara dataresurser.

Skalbar avser här dataresurser som leverantören av molntjänster fördelar på ett flexibelt sätt, oberoende av resursernas geografiska läge, för att hantera fluktuationer i efterfrågan. En elastisk pool av dataresurser används vidare för att beskriva dataresurser som avsätts och utnyttjas beroende på efterfrågan för att tillgängliga resurser snabbt ska kunna utökas och minskas i takt med arbetsbördan.

Swedish Standards Institute (SIS) har antagit en svensk standard (ISO/IEC 17788:2014, IDT) som fastslår att en molnbaserad datortjänst är ett

> koncept som möjliggör nätverksåtkomst till en skalbar och elastisk pool av delade fysiska eller virtuella resurser som via självbetjäning levereras och administreras på begäran.

Det amerikanska standardiseringsorganet National Institute for Standards and Technology (NIST) publicerade redan 2011 en definition (SP 800-145) av datormoln som fått stor spridning. Enligt NIST:s definition är ett datormoln en

> model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks,

servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

I NIST:s definition beskrivs datormoln ha fem egenskaper, nämligen att

- en användare genom självservice bestämma kapacitet utifrån behov utan att involvera en mänsklig operatör,
- tillgång till datormolnet sker via nätverk och genom standardenheter såsom datorer, mobiltelefoner och surfplattor,
- användaren delar datormolnets resurser med andra användare,
- de resurser och den kapacitet som användaren har tillgång till kan skalas upp och ned elastiskt, och
- resursutnyttjande kan mätas (bl.a. för att avgöra hur kunder ska debiteras om datormolnet tillhandahålls som tjänst).

Definitionen innehåller även följande tre leveransmodeller (även kallade molntjänstkategorier i delbetänkandet).

- *Software as a Service* (SaaS), som ger användaren möjlighet att använda de applikationer som finns i datormolnet. Applikationerna är tillgängliga genom olika klienter, antingen tunna klienter såsom webbläsare eller programgränssnitt. Användaren hanterar och kontrollerar inte underliggande molninfrastruktur inklusive nätverk, servrar, operativsystem, lagring eller applikationsmiljö med undantag för applikationens användarinställningar.
- *Platform as a Service* (PaaS), som ger användaren möjlighet att implementera applikationer denne själv utvecklat eller anskaffat som kräver stöd från programmeringsspråk, bibliotek, tjänster eller verktyg som tillhandahålls genom datormolnet. Användaren hanterar eller kontrollerar inte underliggande molninfrastruktur inklusive nätverk, servrar, operativsystem, lagring, men har kontroll över implementerade applikationer och möjligen konfigurationen av deras miljö.
- *Infrastructure as a Service* (IaaS), som ger användaren tillgång till beräkningskapacitet, lagring, nätverk och andra fundamentala datorresurser med vilka användaren kan implementera och exe-

kvera godtycklig mjukvara, vilket inkluderar operativsystem och applikationer. Användaren hanterar eller kontrollerar inte underliggande molninfrastruktur men har kontroll över operativsystem, lagring, implementerade applikationer och möjligen begränsad kontroll över vissa nätverkskomponenter.

Exempel på populära SaaS, PaaS och IaaS är Gmail, Google App Engine respektive Amazon EC2.

NIST etablerar i sin definition fyra leveransmodeller som beskriver förhållandet mellan användaren, andra användare (vanligen benämnda som kunder för kommersiella molntjänster) och tillhandahållaren av datormolnet (leverantören).

– *Privat moln*, där tillgång till datormolnets resurser är begränsat till en organisation. Datormolnet kan dock ägas, administreras av en extern leverantör. Det kan rent fysiskt vara placerat i organisationens lokaler eller externt.
– *Partnermoln*, där tillgång till datormolnets resurser är begränsat till specifika organisationer och användare. Datormolnet kan ägas och administreras av någon eller flera av dessa organisationer eller en extern part. Det kan rent fysiskt vara placerat i organisationens lokaler eller externt.
– *Publikt moln*, där datormolnet är generellt tillgängligt för allmänheten, t.ex. för betalande kunder. Datormolnet kan t.ex. ägas och administreras av ett företag, ett lärosäte, en myndighet eller samägas på något sätt. Det är rent fysiskt placerat hos den organisation som tillhandahåller det.
– *Hybridmoln*, där datormolnet är sammanvävt av infrastruktur från andra leveransmodeller såsom privat, partner eller publikt moln.

2.2.5 Utkontraktering

Begreppet utkontraktering har ingen legaldefinition. I utredningsdirektiven anges att ”[m]ed utkontraktering av it-drift avses […] att en myndighet genom offentlig upphandling eller på något annat sätt uppdrar åt en privat leverantör att hantera hela eller delar av myndighetens it-drift”. Utkontraktering innebär med denna utgångspunkt att en statlig myndighet, kommun eller region lägger ut en del av den

egna verksamheten på entreprenad. Närmare bestämt handlar det om att en tjänst, process eller verksamhet som annars skulle ha utförts av den statliga myndigheten, kommunen eller regionen själv läggs ut på en privat tjänsteleverantör.

I betänkandet *Kompletteringar till den nya säkerhetsskyddslagen* (SOU 2018:82) beskrivs utkontraktering som när en verksamhetsutövare lägger ut drift, underhåll eller skötsel av en viss del av sin verksamhet till en utomstående leverantör. Det kan t.ex. handla om att man lägger ut underhållet av ett system eller utveckling av någon produkt på en extern leverantör. Oavsett vilken definition som används, torde det leda till i allt väsentligt samma resultat. Det centrala är att det handlar om en del av den egna verksamheten. Vidare beskrivs att det är centralt att det handlar om någon form av tjänst eller verksamhet och inte om ett köp av varor. Det rör sig således om utkontraktering när en verksamhetsutövare lägger ut hela eller delar av sin it-drift på en extern aktör. Däremot är det inte utkontraktering att upphandla teknisk utrustning som behövs för den egna it-driften.

I vårt betänkande utgår vi från att hyra av lokaler inte är att beteckna som utkontraktering. Mot denna bakgrund betraktar vi inte hyra av ett utrymme där en verksamhetsutövare ställer sin it-utrustning (samlokalisering eller co-location) som utkontraktering. Det finns nämligen enligt vår mening ingen principiell skillnad mellan att specifikt hyra utrymme för sin it-utrustning, eller att generellt hyra lokaler för sin verksamhet, där verksamhetsutövaren även har sin it-utrustning.

Nyttjande av sådana elektroniska kommunikationstjänster som regleras i lagen (2003:389) om elektronisk kommunikation innebär enligt vår definition inte heller utkontraktering, eftersom det inte är fråga om en tjänst, process eller verksamhet som annars skulle ha utförts av myndigheten själv.

2.3 Vårt arbete

Vårt uppdrag är omfattande och komplext. Det ställer krav på svåra avvägningar mellan olika intressen och värden, inte minst i relationen mellan säkerhet och kostnad. I omvärlden händer mycket på området som vi behövt ta ställning till och som har påverkan på vårt

arbete. Till detta kommer de höga förväntningar från såväl offentliga och privata aktörer på vad vi ska åstadkomma, exempelvis vad gäller frågor om utkontraktering.

Öppenhet och dialog är viktiga utgångspunkter i vårt arbete. Vi har inhämtat information och haft dialog med statliga myndigheter, kommuner och regioner samt med it-branschen. Detta för att få en förståelse för hur frågor om it-drift hanteras hos olika aktörer i dag men också deras tankar om behov och lösningar framåt.

Nedan presenterar vi hur vi valt att redovisa de olika delarna i uppdraget samt hur vi lagt upp och genomfört vårt arbete.

2.3.1 Redovisning av uppdraget

Av utredningsdirektiven framgår att uppdragen att kartlägga och analysera statliga myndigheters it-drift och de rättsliga förutsättningarna för utkontraktering, inklusive eventuella författningsförslag, ska redovisas senast den 15 januari 2021. Uppdraget att föreslå mer varaktiga former för samordnad statlig it-drift ska redovisas senast den 15 oktober 2021.

Vi har utifrån detta lagt fast vilka delar som ska ingå i delbetänkandet respektive slutbetänkandet.

Delbetänkandet

I detta delbetänkande redovisar vi kartläggningen av statliga myndigheters it-drift, omvärldsanalysen samt analysen av de rättsliga förutsättningarna för utkontraktering av it-drift till privata tjänsteleverantörer. Vi lämnar också författningsförslag som rör utkontraktering av it-drift till både privata tjänsteleverantörer och myndigheter emellan. Därutöver redovisar vi en konsekvensanalys av förslagen.

Enligt direktiven ingår att beskriva nationella exempel på samordnad it-drift som en del i omvärldsanalysen. Vi har valt att i stället redovisa denna del i slutbetänkandet.

Slutbetänkande

I slutbetänkandet fokuserar vi på samordnad statlig it-drift. Vi redovisar utvärderingen av Försäkringskassans uppdrag om samordnad it-drift. Vi beskriver även andra exempel på samordnad it-drift mellan myndigheter i Sverige. Analysen av de säkerhetsmässiga och rättsliga förutsättningarna för samordnad statlig it-drift redovisas också. Avslutningsvis redovisar vi våra förslag om samordnad, säker och kostnadseffektiv statlig it-drift samt en konsekvensanalys.

2.3.2 Avgränsningar

Begreppet säker it-drift kan behöva utvecklas i relation till olika hotnivåer i samhället. Vi bedömer att detta kommer vara särskilt relevant för förslagen om samordnad statlig it-drift som presenteras i vårt slutbetänkande. Frågan om hotnivåer har därför avgränsats bort i delbetänkandet.

Den tolkning av röjandebegreppet som vi gör i vår rättsliga analys avser endast utkontraktering av it-drift till privata tjänsteleverantörer. En bredare ansats än så ligger utanför vårt uppdrag och skulle dessutom kräva utredningsresurser som inte står till vårt förfogande. Vi tar således inte ställning till hur röjandebegreppet i offentlighets- och sekretesslagen (2009:400) (OSL) ska tolkas i andra situationer än vid utkontraktering av it-drift till privata tjänsteleverantörer.

Förbudet att röja eller utnyttja en uppgift enligt OSL gäller inte endast för myndigheter utan även för en person som fått kännedom om uppgiften genom att för det allmännas räkning delta i en myndighets verksamhet genom t.ex. uppdrag hos myndigheten. Vad som avses här är uppdrag som getts direkt till en fysisk person. I allmänhet bör uppdragstagaren vara så knuten till myndigheten att han eller hon kan sägas delta i myndighetens egentliga verksamhet, dvs. som regel myndighetens uppgifter enligt instruktion eller motsvarande reglering. I betänkandet behandlas inte den situationen att en myndighet utkontrakterar it-drift åt en tjänsteleverantör vars personal är bunden av OSL.

Vi lämnar två författningsförslag i detta delbetänkande. Det ena förslaget avser införande av en sekretessbrytande bestämmelse i OSL om utkontraktering av teknisk bearbetning och teknisk lagring av uppgifter. Det andra förslaget avser en inskränkt meddelarfrihet för

den krets av personer som träffas av lagen (2020:914) om tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter (tystnadspliktslagen). För att säkerställa utkontraktering med bibehållen säkerhet bedömer vi att den sekretessbrytande bestämmelsen med intresseavvägning bör kompletteras med central vägledning och stöd till statliga myndigheter, kommuner och regioner. Vi avser att återkomma med förslag om detta tillsammans med andra förslag i vårt slutbetänkande.

2.3.3 Metod och arbetssätt

Här redovisar vi i korthet metoder och arbetssätt för de analyser som presenteras i delbetänkandet.

Kartläggningen av statliga myndigheters it-drift har genomförts genom en enkät till 200 statliga myndigheter, fallstudier av fem myndigheter samt en digital workshop med 16 myndigheter. I kartläggningen har frågor ställts om verksamhet, uppgiftshantering och informationssäkerhet, it-drift och kostnader i dag, hinder för it-drift samt behoven framåt. Viktiga parametrar för analysen är myndigheternas storlek, verksamhet och uppgiftshantering samt vilka krav som utifrån detta ställs på it-driften.

Omvärldsanalysen har genomförts genom dokumentstudier och genom intervjuer med företrädare för myndigheter i respektive utvalt land. Länderna har valts ut med beaktande av att de har en jämförbar förvaltningstradition eller en väsentligen annorlunda ansats när det gäller it-driftsförsörjningen (Storbritannien).

I *den rättsliga analysen om förutsättningar för utkontraktering av it-drift* har vi använt oss av en sedvanlig juridisk metod. Det innebär att vi sökt svaren på de frågor som vi ställts inför genom att analysera lagtext, lagmotiv, rättspraxis och litteratur.

2.3.4 Möten, dialoger och samverkan

Vi har haft kontakt med ett stort antal aktörer i arbetet. På grund av covid-19 har de flesta möten hållits digitalt.

Expertgruppen, där företrädare för Regeringskansliet ingår, har haft fyra möten under år 2020. Även referensgruppen, med företrädare för elva statliga myndigheter, Sveriges kommuner och regioner (SKR), It- och Telekomföretagen samt Internetstiftelsen, har haft fyra möten. På mötena har sekretariatet presenterat upplägg för arbetet, redovisat resultat och delresultat i de olika analyserna samt lyft principfrågor och förslag för diskussion. Sekretariatet har utöver det stämt av mer specifika frågor med enskilda experter och företrädare i referensgruppen. Löpande avstämningar har också hållits med Infrastrukturdepartementet.

Enligt direktiven ska uppdraget utföras i nära dialog med Försäkringskassan och Myndigheten för digital förvaltning. Vi ska samråda med Myndigheten för samhällsskydd och beredskap, Försvarsmakten/MUST, Försvarets radioanstalt och Säkerhetspolisen, Fortifikationsverket och Datainspektionen. Vi har under våren 2020 haft formell dialog med respektive myndighet angående uppdraget. Vi har därutöver haft flera möten med Försäkringskassan där former för samverkan och upplägg samt kravställning för utvärderingen av Försäkringskassans uppdrag om samordnad it-drift har diskuterats. Sekretariatet har också deltagit vid ett möte om Försäkringskassans samordnade it-drift som myndigheten anordnat för sina kundmyndigheter. Utöver dessa aktörer har vi också haft möten med Skatteverket, Post- och telestyrelsen samt Lantmäteriet. Vi har också deltagit vid möten som anordnats av eSamverkansprogrammet.

Som stöd i arbetet har vi bildat två arbetsgrupper – en juridisk och en inom säkerhet – bestående av jurister respektive specialister inom informationssäkerhet och säkerhetsskydd som arbetar vid statliga myndigheter. I den juridiska arbetsgruppen har även företrädare för SKR ingått. Arbetsgrupperna har kvalitetssäkrat underlag och skrivningar samt bidragit med synpunkter i principiella frågor.

Vi ska enligt direktiven också, i relevanta delar i uppdraget, inhämta synpunkter från privata it-driftsleverantörer, it-branschen och SKR. Vi har deltagit i flera möten som anordnats av SKR, exempelvis med SKR:s beredning för digitalisering och i livesändning för kommuner och regioner. I augusti 2020 medverkade vi på

Offentliga rummet och ett seminarium om it-drift och molntjänster som anordnades av SKR. SKR har också inkommit med skriftliga synpunkter. Utöver det har vi haft möten med enskilda kommun- och regiongrupperingar. Under våren 2020 har vi haft möten med It- och telekomföretagen och deras Dataråd. Vi har haft ett möte med American Chamber of Commerce under ledning av Utrikesdepartementet där företrädare för it-branschen deltog. Det har inkommit ett stort antal förfrågningar från enskilda företag om separata möten. För att värna likvärdigheten och ge alla företag samma möjlighet att komma i kontakt med oss anordnade vi ett webinarium för it- och telekombranschen den 15 oktober 2020. Under webinariet presenterade vi vårt arbete och branschen fick ställa frågor till oss. Vi fick också synpunkter från branschen på ett antal frågor. Utöver det har enskilda företag haft möjlighet att komma med skriftliga synpunkter.

Vi har därutöver haft kontakt med Utredningen om samordning av statliga utbetalningar från välfärdsystemen (Fi 2018:05) och Utredningen om ökad och standardiserad användning av betrodda tjänster i den offentliga förvaltningen (I 2020:01).

Som stöd för planering och genomförande av workshopen med myndigheterna samt webinariet med it- och telekombranschen har vi anlitat Sherpa Management AB. Underlag till konsekvensutredningen har tagits fram av Governo AB på vårt uppdrag.

2.4 Delbetänkandets disposition

I kapitel 3 går vi igenom ett urval tidigare kartläggningar och utredningar som rör frågor om säker och kostnadseffektiv it-drift samt utkontraktering av it-drift i den offentliga förvaltningen.

I kapitel 4 presenteras kartläggningen av de statliga myndigheternas it-drift: hur it-driften hanteras i dag, kostnader för it-drift och vilka hinder som finns för säker och kostnadseffektiv it-drift samt hur myndigheternas behov av it-drift ser ut framåt.

I kapitel 5 presenteras omvärldsanalysen och hur it-driftsfrågor och samordnad it-drift hanteras i ett antal utvalda länder.

I kapitel 6–10 redovisar vi vår rättsliga analys av förutsättningarna för utkontraktering av it-drift till privata tjänsteleverantörer.

Kapitel 6 är främst av beskrivande karaktär och innehåller en genomgång av rättsliga krav på säkerhetsskydd och informationssäkerhet vid utkontraktering.

Kapitel 7 innehåller en beskrivning av dataskyddsregelverket och innefattar dels en genomgång av de bestämmelser som rör det avtalsmässiga och organisatoriska förhållandet mellan den personuppgiftsansvarige och personuppgiftsbiträdet, dels en analys av reglerna om tredjelandsöverföring.

I kapitel 8 analyserar vi röjandebegreppet i OSL.

Kapitel 9 innehåller en redogörelse för hur röjandebegreppet hanterats i tidigare utredningar m.m. liksom en redovisning av hur vi bedömer några av de frågor som förekommit i tidigare utredningar.

I kapitel 10 behandlar vi förslaget till en sekretessbrytande bestämmelse och de villkor som ska gälla för denna.

Kapitel 11 innehåller ett förslag till undantag från meddelarfriheten för den krets av personer som träffas av tystnadspliktslagen.

I kapitel 12 redovisas en konsekvensutredning av författningsförslagen.

I kapitel 13 presenterar utredningen förslag till inriktning för det fortsatta utredningsarbetet när det gäller samordnad statlig it-drift.

I kapitel 14 behandlas ikraftträdande.

Kapitel 15 innehåller författningskommentarer.

3 Tidigare kartläggningar och utredningar

I detta kapitel går vi igenom ett urval av kartläggningar och utredningar som rör frågor om säker och kostnadseffektiv it-drift i den offentliga förvaltningen.

Vi har framför allt valt att lyfta fram rapporter som analyserar frågor om hur it-driften inom den offentliga förvaltningen ser ut i dag, vilka hinder och utmaningar som finns vad gäller bl.a. säkerhet och kostnader kopplat till it-drift samt frågor om utkontraktering till privata tjänsteleverantörer. En del av rapporterna återkommer vi till i senare delar av delbetänkandet.

Rapporter som hanterar frågor om samordnad it-drift avser vi att återkomma till i vårt slutbetänkande.

3.1 Kartläggningar av it-drift, molntjänster och it-kostnader

Under de senaste fem åren har det genomförts ett antal kartläggningar av it-drift och molntjänster. Fokus har framför allt varit på molntjänster och vilka möjligheter och hinder som finns för användningen av molntjänster i offentlig verksamhet. En studie fokuserar särskilt på de risker som kan uppstå när offentliga aktörer använder sig av molntjänster.

Outsourcing av it-tjänster i kommuner

I en rapport från år 2014 analyserade Myndigheten för samhällsskydd och beredskap (MSB) hur kommunerna ”använder outsourcing, samverkan kring it-tjänster och molntjänster i sin verksamhet”. MSB

lät genomföra en enkätundersökning som visade att 80 procent av de drygt 120 kommuner som besvarade enkäten ägnar sig åt någon form av outsourcing (utkontraktering). I denna siffra ingick dock både användning av kommersiella tjänster och olika typer av kommunal samverkan. Det vanligaste var att kommunerna lade ut enskilda system och tjänster på en utomstående part.

Av rapporten framgår att skälen till att utkontraktera it-drift inte i första hand är ekonomiska utan att det i stället handlar om tillgänglighet och driftssäkerhet. Många kommuner ser utkontraktering och samverkan som ett sätt att förbättra kommunens kompetensbehov och säkerhet inom it-området. En utmaning som lyftes fram var att kommunernas komplexa uppdrag ställer stora krav på informationshanteringen, vilket i sin tur gör att kommunerna måste ha tillgång till en både hög och bred it-kompetens och en väl utvecklad informationssäkerhet. Samtidigt ställer den ofta pressade ekonomin krav på hög grad av effektivitet i stödfunktioner som it.

I enkäten ombads kommunerna att ange på en fem-gradig skala hur svårt de tycker att det är att genomföra en it-upphandling vad gäller aspekterna it, juridik och upphandling. Medelvärdet översteg i samtliga fall tre på skalan vilket enligt MSB visade att kommunerna uppfattar detta som en svår uppgift. Den juridiska aspekten i it-upphandling bedömdes som den allra svåraste. MSB konstaterade att det är viktigt med ett systematiskt informationssäkerhetsarbete, att kommunerna ansvarar för samhällsviktig verksamhet och att det därför bör ses som en prioriterad fråga att ge kommunerna ytterligare stöd i deras systematiska informationssäkerhetsarbete.

Informationssäkerhet – trender 2015

Försvarsmakten, Försvarets radioanstalt, MSB och Rikskriminalpolisen tog år 2015 fram en trendrapport som underlag för stöd i säkerhetsarbete i samhället. I rapporten konstaterade myndigheterna att allt flera system läggs ut på externa leverantörer och i molntjänster. Kostnadseffektivitet, kvalitet och driftsäkerhet är enligt rapporten drivkrafter bakom outsourcing (utkontraktering) samtidigt som det ställer höga krav på beställaren för att inte leda till oönskade risker. Utvecklingen med utkontraktering leder enligt myndigheterna ofrånkomligen till att allt mer information samlas hos ett fåtal aktörer.

och att konsekvenserna av såväl attacker som icke-antagonistiska driftavbrott blir mer svåröverskådliga. Både enkla och sofistikerade hot och risker bör därför enligt myndigheterna vägas in i de riskanalyser som genomförs innan verksamhet läggs ut till underleverantörer eller data läggs i molntjänster. Myndigheterna konstaterar att molntjänster gör att ansvar allt oftare är utspritt över flera organisationer, trots att säkerhet förutsätter tydlighet och gott samarbete. De skriver också att även om den upplevda säkerheten i en molnlösning kan vara hög så ersätter den inte den egna organisationens ansvar eller säkerhetsarbete.

Pensionsmyndighetens kartläggning av molntjänster i staten

År 2015 fick Pensionsmyndigheten i uppdrag av regeringen att analysera och värdera potentialen för användning av molntjänster i staten samt att redovisa risker och hinder med att använda molntjänster i statlig verksamhet. Uppdraget redovisades i rapporten *Molntjänster i staten – en ny generation av outsourcing*. Som en del i uppdraget genomförde Pensionsmyndigheten en enkätundersökning till 211 statliga myndigheter. I enkäten ställdes frågor om motiven bakom att använda molntjänster liksom vilken nytta molntjänster kan erbjuda. Frågor ställdes också om de största upplevda hindren för att använda molntjänster.

Pensionsmyndigheten konstaterade i rapporten att statliga myndigheter som använder molntjänster kan styra om sina resurser mot utveckling och innovation i andra delar av sina verksamheter, exempelvis utveckling av nya tjänster för medborgare och företag. Detta eftersom de kan dra nytta av att en molntjänstleverantör i kraft av sin stora skala och specialisering har mycket större möjligheter att arbeta strukturerat och långsiktigt med utveckling och innovation av tjänster. Pensionsmyndigheten konstaterade vidare att molntjänster kan vara fördelaktiga för de myndigheter som har kraftigt varierande behov av it-resurser, som exempel nämndes Pensionsmyndighetens utskick av orange kuvert, Skatteverkets hantering av deklarationer samt Valmyndighetens uppgifter vid allmänna val. Flexibiliteten i en molntjänst innebär enligt Pensionsmyndigheten att när behoven ökar kan organisationen öka sin dator- eller lagringskapacitet, för att sedan minska när efterfrågan är lägre. Detta innebär att myndigheten

aldrig behöver köpa kapacitet som inte utnyttjas och att besparingen kan användas till andra värdehöjande aktiviteter. Pensionsmyndigheten belyste samtidigt utmaningar med s.k. inlåsningseffekter som uppstår om en myndighet på ett eller annat sätt har ett beroende till en specifik leverantör. De kan bl.a. uppstå på grund av en viss leverantörs specifika produkter, tjänster eller teknologi. Men även kompetensmässiga och rättsliga skäl kan medföra att tjänsten varken kan eller får förvaltas av någon annan än den som levererar den för tillfället. Pensionsmyndigheten pekade på att de största upplevda hindren för statliga myndigheter att använda molntjänster var säkerhetsrelaterade frågor samt oklarheter kring de juridiska förutsättningarna för nyttjande av molntjänster. Att tillämpa gällande regelverk och balansera integritetsskydd och effektivitet upplevdes också som svårt av myndigheterna.

Statens servicecenters rapport om en gemensam statlig molntjänst för myndigheternas it-drift

Statens servicecenter (SSC) fick år 2016 i uppdrag av regeringen att analysera och föreslå vilka myndighetsfunktioner som kan vara lämpliga att bedriva samordnat inom staten och utanför storstadsområden. Som en del i uppdraget genomförde SSC en enkätundersökning till statliga myndigheter om hur myndigheterna hanterade sin it-drift (i egen regi eller genom utkontraktering) samt vilka kostnader de hade för sin it-drift. Enkäten besvarades av 166 myndigheter. Av dessa hanterade 111 myndigheter sin it-drift i egen regi, medan 56 myndigheter hade utkontrakterat sin it-drift.

SSC rekommenderade i sin redovisning av uppdraget att inrätta en statlig molntjänst som skulle erbjuda myndigheterna datorkraft och lagring. Inrättandet av en statlig molntjänst skulle enligt SSC ge årliga besparingar på 750 till 800 miljoner kronor och skapa nya arbetstillfällen motsvarande 200 årsarbetskrafter. Förslaget skulle enligt SSC också öka it-säkerheten för hela statsförvaltningen.

Post- och telestyrelsens rapport Förslag till en förvaltningsmodell för skyddade it-utrymmen

Regeringen uppdrog år 2017 åt Post- och telestyrelsen (PTS) att lämna förslag till en förvaltningsmodell för skyddade it-utrymmen för offentliga aktörer som bedriver säkerhetskänslig verksamhet. PTS genomförde uppdraget i samverkan med Försäkringskassan och Fortifikationsverket och redovisade i februari 2018 en modell med en prioriteringsfunktion, utrymmesförvaltare, anläggningsägare och en nyttjare. Förslaget innehöll inga författningsändringar och PTS framhöll att ytterligare utredningar behöver göras innan förslagen kan implementeras.

MSB:s studie om säkerhet vid molnlösningar

År 2018 genomförde Örebro universitet på uppdrag av MSB en kartläggning av säkerhet vid molnlösningar bland offentliga aktörer. Kartläggningen omfattade både statliga myndigheter och kommuner. Syftet var att kartlägga användningen av molnlösningar bland offentliga aktörer, identifiera samhällsrisker när offentliga aktörer använder molntjänster, analysera graden av centralisering av tillhandahållandet av molntjänster samt kartlägga utmaningar vid upphandling av molntjänster. I studien ingick också en internationell utblick av användningen av molntjänster inom EU och Norden.

I rapporten konstaterades att en övervägande del av de offentliga aktörerna använder upphandlade molntjänster i sin verksamhet och att mjukvara som tjänst (SaaS) är den vanligast förekommande molntjänsten. Ett fåtal molntjänster identifierades där det fanns en tydlig centralisering. Dessa molntjänster bedömdes dock inte ha betydelse för samhällskritisk infrastruktur eller samhällskritiska tjänster. Av rapporten framgick vidare att statliga myndigheter och kommuner ser kompetensutmaningar när det gäller regelverk, kontraktsfrågor och upphandlingsfrågor. Rapporten visade också att det inte finns någon systematik i hur kontrakt med molntjänstleverantörer följs upp. En minoritet av de som deltagit i studien genomförde revisioner, vilket enligt rapportförfattarna gör det svårt att veta vilka av de ställda kraven som uppfylls och på vilken nivå.

I rapporten presenterades prioriterade krav och rekommendationer för hur MSB i sitt informationssäkerhetsarbete ska kunna underlätta för offentliga aktörer att nyttja molntjänster. De högst prioriterade rekommendationerna handlade om att höja kunskapsnivån om molntjänster och vad användningen av en molntjänst innebär samt att utveckla stöd för statliga myndigheter och kommuner i att genomföra riskanalyser vid upphandling av molntjänster och i uppföljning av molntjänstavtal.

Kartläggningar av it-kostnader och it-mognad

Ekonomistyrningsverket (ESV) genomförde år 2014–2017 på uppdrag av regeringen analyser av statliga myndigheters it-kostnader, strategiska it-projekt och it-mognad. ESV tog tillsammans med de deltagande myndigheterna fram ett antal nyckeltal för it-kostnader, exempelvis utkontrakterad verksamhet/it-kostnad och kostnad för lagring. I analyserna ingick inte några specifika nyckeltal för it-drift. En uppskattning av de totala it-kostnaderna i staten gjordes. För mätningen av it-mognad fick myndigheterna göra en självskattning av bl.a. strategi för it-försörjning, it-kompetensförsörjningsplan, rutin för att göra kostnadsjämförelser med stöd av nyckeltal samt informationssäkerhet. ESV konstaterade bl.a. att det fanns ett behov av att stärka förmågan att beräkna it-kostnader och öka kostnadsmedvetenheten i statsförvaltningen men också att mäta myndigheternas it-mognad. Myndigheterna behövde enligt ESV också utveckla sin förmåga inom bl.a. informationssäkerhet, strategi för it-försörjning och it-kompetensförsörjning.

Sedan år 2019 har Myndigheten för digital förvaltning (Digg) ansvaret att följa upp de statliga myndigheternas digitala mognad och it-kostnader. År 2019 genomförde Digg en enkätundersökning som riktade sig till 175 statliga myndigheter vilket var ett bredare urval än ESV tidigare haft. Frågorna var dock i stora delar desamma som ESV tidigare ställt. Digg konstaterade att myndigheterna kommit olika långt i sin it-mognadsgrad. Små myndigheter är generellt mindre it-mogna än större myndigheter. Myndigheterna skattar sin mognadsnivå som högst för bl.a. informationssäkerhet och lägst när det gäller kostnadsjämförelser med andra aktörer.

3.2 Utredningar och rapporter som rör utkontraktering

Det har inte gjorts några utredningar specifikt av utkontraktering av it-drift till privata tjänsteleverantörer. Däremot har frågan om utkontraktering berörts i ett antal utredningar och rapporter, varav två av dem beskrivs närmare nedan.

E-delegationens förstudie om Effektiv it-drift inom staten

E-delegationen var en expertgrupp inom e-förvaltning som tillsattes av regeringen 2009 och upphörde 2015.

År 2012 genomförde E-delegationen en förstudie om effektiv it-drift inom staten. Syftet med förstudien var att identifiera och beskriva möjligheter till effektivisering av myndigheternas it-drift samt föreslå hur sådana lösningar kan utformas.

I förstudien konstaterades att det finns en betydande potential att effektivisera myndigheternas it-drift och att denna potential inte kommer att kunna nås genom fortsatt mål- och resultatstyrning. Mot denna bakgrund lämnade E-delegationen två förslag. Det ena förslaget handlade om att skapa en myndighetsgemensam aktör, i form av en statlig myndighet, som på regeringens uppdrag effektiviserar myndigheternas it-drift genom koncentration, konsolidering, harmonisering och konkurrensutsättning. Det andra förslaget var att regeringen skulle ålägga myndigheterna att konkurrensutsätta it-driften, dock med viss it-drift i egen regi. Detta förslag gick enligt E-delegationen lättare att genomföra men bedömdes ge mindre effektiviseringsvinster än att koncentrera it-driften inom statsförvaltningen. Nackdelarna med förslaget om obligatorisk konkurrensutsättning var enligt E-delegationen att det ställer krav på att myndigheterna har god branschkunskap, beställar- och upphandlarkompetens inom it samt att myndighetsvis outsourcing (utkontraktering) skapar en leverantörsstruktur som är svår att styra och kontrollera. De risker som E-delegationen lyfte fram med förslaget om obligatorisk konkurrensutsättning var att det bygger på ett fortsatt ”silotänk” där varje myndighet var och en för sig ansvarar för genomförandet samt att informationssäkerhetsarbetet skulle bli lidande.

Digitaliseringsrättsutredningen

År 2018 presenterade Digitaliseringsrättsutredningen sitt betänkande *Juridik som stöd för förvaltningens digitalisering* (SOU 2018:25). I utredningsuppdraget ingick att kartlägga och analysera i vilken utsträckning det förekommer lagstiftning som i onödan försvårar digital utveckling och samverkan inom den offentliga förvaltningen.

I betänkandet lyfter man bl.a. frågan om informationssäkerhet vid utkontraktering till privata leverantörer. Utredningen konstaterar att utkontraktering av it-drift och andra it-baserade funktioner har blivit allt mer centralt för en kostnadseffektiv och i övrigt väl fungerande digital förvaltning. Samtidigt ställer utkontraktering enligt utredningen höga krav på beställarkompetens och säkerhetsmedvetande hos en myndighet för att inte leda till oförutsedda risker. Utredningen hänvisar till en rapport från Riksrevisionen (RiR 2014:23) som pekar på att utkontraktering i kombination med otillräcklig beställarkompetens i det långa loppet kan leda till brister som är svåra att värdera kostnadsmässigt. Samtidigt pekade utredningen på att informationssäkerhetsfrågor fått en högre prioritet och att säkerhetsmedvetandet höjts bland offentliga aktörer. Utredningen pekade på att det finns ett behov av att klargöra de rättsliga förutsättningarna för utkontraktering av it-drift och andra it-baserade funktioner från myndigheter till privata leverantörer. Utredningen lämnade därför ett författningsförslag om tystnadsplikt vid utkontraktering av teknisk bearbetning och lagring. Detta förslag, som nu lett till lagstiftning, behandlas närmare i avsnitt 9.6.

4 Kartläggning av statliga myndigheters it-drift

Vi ska enligt direktiven kartlägga och analysera de statliga myndigheternas behov av säker och kostnadseffektiv it-drift, hur behoven är tillgodosedda och vilka kostnader myndigheterna har för it-driften. Vi ska också kartlägga och analysera i vilken utsträckning olika it-driftsformer – i egen regi, samordning respektive utkontraktering – kan svara mot statliga myndigheters behov av och krav på it-drift och vilka förutsättningar myndigheterna har för ändamålsenlig kravställning inom området. Vidare ska vi analysera vilka behov av it-drift och närliggande tjänster hos statliga myndigheter och olika verksamhetssektorer som utifrån behovsanalysen är mest prioriterade att tillgodose.

Kartläggningen ska omfatta ett representativt urval av statliga myndigheter. Kriterier att beakta i urvalet är bl.a. storlek, finansieringsform och verksamhetsområde.

4.1 Vår kartläggning

I kapitel 3 går vi igenom ett antal kartläggningar som gjorts under de senaste åren och som rör frågor om säker och kostnadseffektiv it-drift i den offentliga förvaltningen. Vi har med utgångspunkt i direktiven sett behov av att dels följa upp några av de frågeställningar som ingått i tidigare kartläggningar, dels bredda och fördjupa kunskapen om it-driften i dag och behoven framåt liksom säkerhetsaspekter och hinder kopplade till statliga myndigheters it-drift. Vår kartläggning bygger på en enkät till 200 statliga myndigheter, fallstudier av fem myndigheter och en workshop med företrädare för 16 myndigheter.

Enkät till 200 statliga myndigheter

Den första delen i kartläggningen omfattar en enkät till 200 statliga myndigheter. I urvalet ingår myndigheterna i den statliga redovisningsorganisationen, exklusive försvarsmyndigheter, myndigheter med en värdmyndighet och små myndigheter med särskilt låg omsättning. Syftet med enkäten är att få en representativ bild av myndigheternas informationshantering och säkerhet, hur deras it-drift och kostnader för it-drift ser ut i dag, deras framtida behov och vilka eventuella hinder för säker och kostnadseffektiv it-drift som finns (se Figur 4.1 nedan). Bakgrundsvariabler som myndighetsstorlek, finansieringsform och departementstillhörighet har ingått i analysen.

Enkäten genomfördes mellan den 16 mars 2020 och den 30 juni 2020. Som följd av de begränsningar som covid-19 har medfört har vi fått förlänga svarstiden för enkäten i två omgångar. Enkäten skickades ut till 200 myndigheter. De 21 länsstyrelserna samordnade sitt svar. Totalt förväntades därmed 180 myndigheter inkomma med svar. Totalt har 158 myndigheter besvarat hela eller delar av enkäten, fyra myndigheter har meddelat att de avstår och 18 myndigheter har inte svarat. Svarsfrekvensen uppgår därmed till 88 procent. En bortfallsanalys visar att de myndigheter som inte svarat omfattar såväl små som medelstora myndigheter och med olika typer av verksamhet och verksamhetsområden. Enkätens representativitet är därmed mycket god.

I enkäten används följande indelning för myndighetsstorlek.

Tabell 4.1 Kategorier för myndighetsstorlek

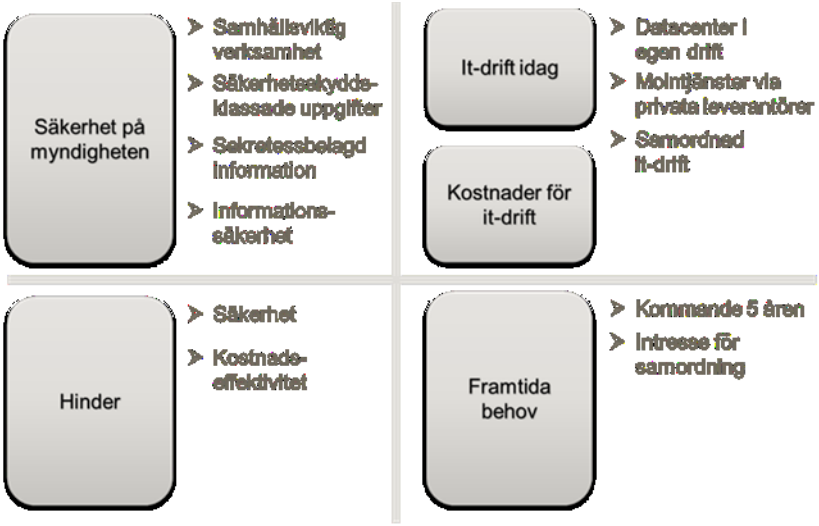
	Antal anställda	Antal myndigheter i enkäturvalet
Små myndigheter	–49	33
Medelsmå myndigheter	50–199	47
Medelstora myndigheter	200–499	34
Stora myndigheter	500–	66
Totalt antal		**180**

Kommentar: Svaren för de 21 länsstyrelserna har samordnats av en länsstyrelse, denna ligger i kategorin stor myndighet.

Kategorin stora myndigheter är bred. Inom kategorin 500–999 anställda finns 27 myndigheter, 16 myndigheter har 1 000–1 999 anställda. Inom spannet 2 000–4 999 anställda finns 9 myndigheter. Antalet myndigheter med fler än 5 000 anställda uppgår till 14.

I enkäten ingår ett antal frågeområden som sammantaget ska ge en bild av de statliga myndigheternas verksamhet, uppgifter och säkerhetsarbete, hur it-driften och it-kostnaderna ser ut i dag, vilka hinder myndigheterna ser för en säker och kostnadseffektiv it-drift och hur de ser på de framtida behoven av it-drift.

Figur 4.1 Frågeområden i enkät om säker och kostnadseffektiv it-drift



Fallstudier av fem typmyndigheter

Den andra delen i kartläggningen består av fallstudier av fem myndigheter för att fördjupa analysen utifrån enkäten. Myndigheterna har valts ut utifrån myndighetsstorlek och vilken roll it spelar i verksamheten. För att få en god representativitet och spridning har hänsyn också tagits till hur myndigheterna svarat på enkäten när det gäller t.ex. val av it-driftslösningar, erfarenhet och intresse av samordnad it-drift. Fallstudierna har inriktats på följande typ av myndigheter:

– Stor myndighet där it utgör en kritisk del av verksamheten.

– Mellanstor myndighet där it utgör en stödfunktion.
– Mindre myndighet där it utgör en kritisk del av verksamheten.
– Mindre myndighet där it utgör en stödfunktion.
– Universitet/högskola.

Fallstudierna har genomförts genom semistrukturerade intervjuer med företrädare för ledning, it, säkerhet, ekonomi och juridik samt andra relevanta funktioner eller verksamheter inom myndigheten. En intervjuguide har tagits fram som myndigheterna fått del av inför intervjuerna.

Workshop om myndigheternas behov av it-drift

Vi anordnade en digital workshop med 16 myndigheter i oktober 2020 för att fördjupa kunskapen och förståelsen för myndigheternas behov av it-drift i dag och framåt. På workshopen diskuterades också i vilken utsträckning olika lösningar för it-drift kan tillgodose myndigheternas behov och vilka behov som är mest prioriterade att tillgodose.

4.2 Verksamhet, uppgifter och informationssäkerhet

Olika verksamheter har olika behov av säker och kostnadseffektiv it-drift. För samhällskritisk verksamhet ställs högre krav på säkra it-driftslösningar än för verksamheter som inte är samhällskritiska. Icke samhällskritiska verksamheter kan dock hantera känsliga personuppgifter som i sig ställer krav på säkerhet. Myndigheternas verksamhet och vilka uppgifter de hanterar påverkar vilka krav som ställs på it-driften och i sin tur vilka behov av säker och kostnadseffektiv it-drift som finns i den statliga förvaltningen. Den första delen i enkäten hanterar denna typ av frågeställningar.

4.2.1 Samhällsviktig verksamhet

Samhällsviktig verksamhet är ett samlingsbegrepp som omfattar de verksamheter, anläggningar, noder, infrastrukturer och tjänster som är av avgörande betydelse för att upprätthålla viktiga samhällsfunktioner inom en samhällssektor. Med samhällsviktig verksamhet menas dels verksamhet som måste fungera för att inte dess bortfall ska leda till en samhällsstörning, dels verksamhet som måste finnas för att hantera en samhällsstörning när den väl inträffar.

Ett drygt 20-tal myndigheter har enligt förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap ett särskilt utpekat ansvar för att inom olika samverkansområden planera och vidta förberedelser för att skapa förmåga att hantera en kris, förebygga sårbarheter och motstå hot och risker. I detta ansvar ingår bl.a. att beakta behovet av säkerhet och kompatibilitet i de tekniska system som är nödvändiga för att myndigheterna ska kunna utföra sitt arbete. Samverkansområdena omfattar teknisk infrastruktur, transporter, farliga ämnen, ekonomisk säkerhet och skydd samt undsättning och vård.

Övriga myndigheter, som inte har ett särskilt sektors- eller bevakningsansvar ska själva bedöma om de bedriver samhällsviktig verksamhet eller inte. Som stöd för bedömningen har Myndigheten för samhällsskydd- och beredskap (MSB) tagit fram en vägledning för identifiering av samhällsviktig verksamhet (MSB1408).

Drygt en tredjedel av myndigheterna bedriver samhällsviktig verksamhet

I enkäten fick myndigheterna ange om de bedriver verksamhet som kan bedömas vara samhällsviktig. 55 av 158 svarande myndigheter (35 procent) bedömer att de bedriver samhällsviktig verksamhet, medan 100 myndigheter (63 procent) bedömer att de inte gör det. Tre myndigheter anger att de inte vet om de bedriver samhällsviktig verksamhet.

Det finns ett visst samband mellan samhällsviktig verksamhet och storlek på myndighet. Större myndigheter bedriver i högre utsträckning samhällsviktig verksamhet jämfört med mindre myndigheter, vilket framgår av tabell 4.2 nedan.

Tabell 4.2 Myndigheter som bedriver samhällsviktig verksamhet

Fördelning på myndighetsstorlek

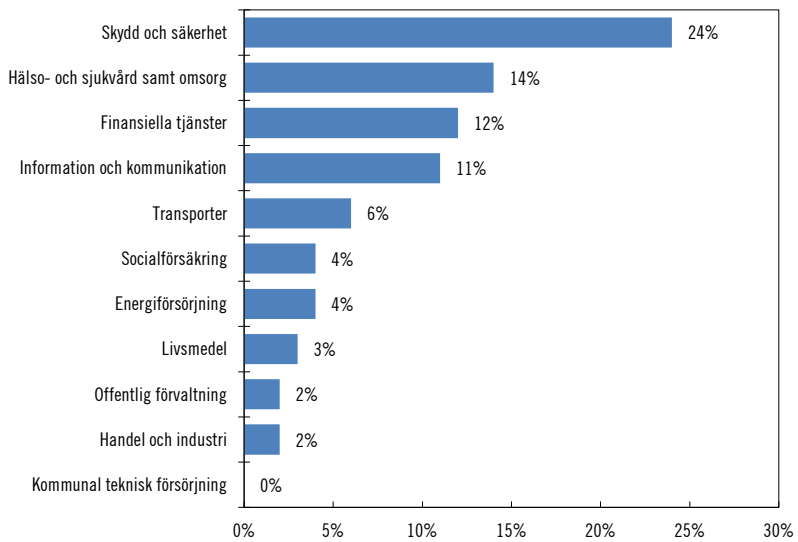
	Antal svar
Små myndigheter	6
Medelsmå myndigheter	6
Medelstora myndigheter	11
Stora myndigheter	32
Totalt antal svarande: 55	

Källa: Enkätundersökning.

De myndigheter som angett att de bedriver samhällsviktig verksamhet fick också ange inom vilken samhällssektor som den samhällsviktiga verksamheten ingår. Detta utifrån de sektorer som MSB pekar ut i sin vägledning; bl.a. energiförsörjning, finansiella tjänster, hälso- och sjukvård samt omsorg, information och kommunikation, livsmedel, skydd och säkerhet, socialförsäkringar och transporter. Myndigheterna kunde i sitt svar ange fler än en sektor. Av svaren framgår att myndigheternas samhällsviktiga verksamhet finns inom flera samhällssektorer, med viss övervikt på skydd och säkerhet, offentlig förvaltning, hälso- och sjukvård och finansiella tjänster.

Figur 4.2 Samhällsviktig verksamhet fördelad på sektor

Myndigheterna har fått ange flera sektorer



Källa: Enkätundersökning.

4.2.2 Vilka uppgifter hanterar myndigheterna?

De uppgifter som myndigheterna hanterar i sin verksamhet omfattas av en rad olika regleringar bl.a.: säkerhetsskyddslagstiftningen, offentlighets- och sekretesslagen (2009:400) (OSL) och dataskyddsförordningen. Myndigheter hanterar även andra typer av uppgifter som inte omfattas av särskilda lagkrav.

Myndigheterna har i enkäten fått svara på vilken typ av uppgifter de hanterar i sin verksamhet: säkerhetsskyddsklassificerade uppgifter enligt säkerhetsskyddslagen (2018:585), uppgifter som är sekretessreglerade enligt OSL och känsliga personuppgifter enligt dataskyddsförordningen. Några motsvarande frågor har inte ställts i de tidigare kartläggningarna om it-drift och molntjänster.

Merparten av myndigheterna hanterar någon form av skyddsvärd information

Sammanställningen av enkätsvaren om vilken typ av uppgifter myndigheterna hanterar visar att merparten (nästan 90 procent) av myndigheterna hanterar någon form av skyddsvärd information i sin verksamhet. Endast 14 av 158 myndigheter bedömer att de inte hanterar någon form av känsliga eller skyddsvärda uppgifter. Olika typer av sekretessreglerade uppgifter är vanligast förekommande liksom känsliga personuppgifter. En mindre andel av myndigheterna hanterar uppgifter som kräver den högsta formen av skydd, dvs. säkerhetsskyddsklassificerad information.

Säkerhetsskyddsklassificerade uppgifter

Med säkerhetsskyddsklassificerade uppgifter avses enligt säkerhetsskyddslagen uppgifter som rör säkerhetskänslig verksamhet och som därför omfattas av sekretess enligt OSL. Hantering av säkerhetsskyddsklassificerade uppgifter ställer särskilda säkerhetskrav på myndighetens it-drift.

Enligt enkätsvaren hanterar 61 av 152 svarande myndigheter (40 procent) säkerhetsskyddsklassificerade uppgifter medan 85 myndigheter (56 procent) inte gör det. Ett fåtal myndigheter vet inte om de hanterar säkerhetsskyddsklassificerade uppgifter. Större myndigheter hanterar i

högre grad säkerhetsskyddsklassificerade uppgifter jämfört med mindre myndigheter, vilket framgår av tabell 4.3 nedan.

Tabell 4.3 Myndigheter som hanterar säkerhetsskyddsklassificerad information

Fördelning på myndighetsstorlek

	Antal svar
Små myndigheter	5
Medelstora myndigheter	9
Medelstora myndigheter	13
Stora myndigheter	34
Totalt antal svarande: 61	

Källa: Enkätundersökning.

Myndigheternas säkerhetsskyddsklassificerade uppgifter fördelar sig på olika säkerhetsskyddsklasser. Olika säkerhetsklasser kräver olika skydd – ju högre skyddsklass desto högre krav på skydd. Begränsat hemlig är den lägsta skyddsklassen och kvalificerat hemlig den högsta.

Tabell 4.4 Myndigheternas säkerhetsskyddsklassificerade uppgifter fördelat på säkerhetsskyddsklasser

Antal svar per kategori

Säkerhetsklass	Antal svar
Kvalificerat hemlig	17
Hemlig	50
Konfidentiell	49
Begränsat hemlig	50
Vet ej	5
Totalt antal svarande: 61	

Källa: Enkätundersökning.

Majoriteten av myndigheterna hanterar säkerhetsskyddsklassificerad information som klassats som hemlig, konfidentiell eller begränsat hemlig. Ett fåtal myndigheter hanterar uppgifter i den högsta säkerhetsskyddsklassen. Några myndigheter anger att de inte vet vilka säkerhetsskyddsklasser uppgifterna ligger inom (alternativt att de inte vet om de har säkerhetsskyddsklassificerade uppgifter i verksamheten). Oavsett säkerhetsskyddsklass ställer förekomsten av säkerhetsskydds-

klassificerade uppgifter särskilda krav på säkerhet i myndigheternas it-driftslösningar.

Sekretessreglerade uppgifter

Myndigheterna fick i enkäten även ange om de hanterade uppgifter som är sekretessreglerade enligt OSL i sin kärnverksamhet. Att frågan avgränsades till just kärnverksamheten var för att kunna särskilja dem från uppgifter som hanteras i alla myndigheter, exempelvis uppgifter om upphandling och den egna personalen. Huruvida alla svarande myndigheter kunnat särskilja detta är oklart.

Av svaren framgår att drygt 80 procent (123) av myndigheterna hanterar någon form av sekretessreglerade uppgifter i sin kärnverksamhet. 29 myndigheter svarar att de inte gör det och fem myndigheter vet inte om de gör det.

De sekretessreglerade uppgifterna regleras med olika styrka, vilket framgår av tabell 4.5 nedan. 90 myndigheter har svarat att de hanterar uppgifter med absolut sekretess, vilket ställer särskilda krav på säkerhetslösningar i it-driften. 80 procent av myndigheterna hanterar sekretessreglerade uppgifter som omfattas av ett omvänt skaderekvisit, dvs. med en presumtion för sekretess.

Tabell 4.5 Myndigheternas sekretessreglerade uppgifter fördelat på sekretessgrad

Antal svar per kategori

Sekretessgrad	Antal svar
Uppgifter med rakt skaderekvisit (presumtion för offentlighet)	121
Uppgifter med omvänt skaderekvisit (presumtion för sekretess)	93
Uppgifter med absolut sekretess	90
Vet ej	5
Totalt antal svarande: 154	

Källa: Enkätundersökning.

Känsliga personuppgifter

En tredje typ av särskilt skyddsvärda uppgifter som kan hanteras i myndigheter är känsliga personuppgifter. Med känsliga personuppgifter avses sådana uppgifter som avses i artikel 9.1 i dataskydds-

förordningen (3 kap. 1 § lagen /2018:218/ med kompletterande bestämmelser till EU:s dataskyddsförordning). Uppgifter om etniskt ursprung, politiska åsikter och genetiska uppgifter och hälsouppgifter utgör exempel på känsliga personuppgifter.

Myndigheterna fick i enkäten ange om de hanterade känsliga personuppgifter i sin kärnverksamhet (samma avgränsning som för sekretessreglerade uppgifter). Av enkätsvaren framgår att en majoritet av myndigheterna, 68 procent (107), hanterar känsliga personuppgifter i sin kärnverksamhet. Här finns också en mer jämn fördelning när det gäller myndighetsstorlek (tabell 4.6).

Tabell 4.6 Myndigheter som hanterar känsliga personuppgifter

Fördelning på myndighetsstorlek

	Antal svar
Små myndigheter	14
Medelsmå myndigheter	24
Medelstora myndigheter	16
Stora myndigheter	53
Totalt antal svarande: 107	

Källa: Enkätundersökning.

4.2.3 Myndigheternas informationssäkerhet

Informationssäkerhet och ett systematiskt informationssäkerhetsarbete är grunden för att kunna avgöra vilken typ av uppgifter som hanteras i verksamheten och vilket skydd som uppgiftshanteringen kräver. Begreppet informationssäkerhet definieras som bevarande av konfidentialitet, riktighet och tillgänglighet hos information. Med *konfidentialitet* aves att endast behöriga personer kan ta del av informationen, med *riktighet* menas att man kan lita på att informationen är korrekt och inte manipulerad och med *tillgänglighet* avses att informationen finns tillgänglig för behöriga användare när den behövs.

MSB meddelade i september 2020 nya föreskrifter om informationssäkerhet för statliga myndigheter med tillhörande allmänna råd (MSBFS 2020:6). De nya föreskrifterna började gälla den 1 oktober 2020. Den största förändringen gentemot tidigare gällande föreskrifter är betoningen på behandling av information liksom på risker.

Av MSB:s föreskrifter framgår att myndigheter ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av ett antal angivna standarder. Informationssäkerhetsarbetet ska utformas utifrån de risker och behov som myndigheten definierar. Det ska omfatta all behandling av information som myndigheten ansvarar för och integreras med myndighetens befintliga sätt att leda och styra sin organisation. I föreskrifterna anges hur informationssäkerhetsarbetet ska utformas och bedrivas, bl.a. avseende informationsklassning, riskbedömning och vidtagande av säkerhetsåtgärder (se vidare avsnitt 6.3.2).

Hälften av myndigheterna har delar av informationssäkerhetsarbetet på plats, men arbete återstår

I enkäten fick myndigheterna uppskatta hur långt de kommit i sitt informationssäkerhetsarbete. Detta utifrån en skala från 1–6, där nivå 1 innebär att myndigheten inte påbörjat något systematiskt informationssäkerhetsarbete och nivå 6 innebär att det finns ett systematiskt och dokumenterat informationssäkerhetsarbete i hela organisationen. Skalan utgick från de då gällande föreskrifterna och allmänna råden för myndigheters informationssäkerhetsarbete (MSBFS 2016:1).

Av tabell 4.7 nedan framgår att medianen ligger på nivå 4. Flest antal myndigheter (43 av 158 svarande) har uppskattat att de ligger på nivå 4. Det finns därefter en övervikt för nivå 2 och 3 (totalt 64 av 158 myndigheter), dvs. den något lägre nivån. 13 myndigheter har angett att de ligger på nivå 1, och 12 myndigheter att de ligger på nivå 6.

En central del i ett informationssäkerhetsarbete är att få kontroll på vilken typ av information som hanteras i verksamheten och klassa informationen utifrån behovet av skyddsnivå utifrån olika regelverk (se tidigare avsnitt). Informationsklassning ingår som en del i informationssäkerhetsarbetet enligt kategori 4 i enkäten. Knappt hälften av myndigheterna har angett att de ligger på nivå 1–3. Enligt svaren har hälften av myndigheterna alltså inte genomfört en informationsklassning. Samtidigt har ändå de flesta av myndigheterna kunnat svara på enkätfrågorna om vilken typ av uppgifter som de hanterar i verksamheten.

Tidigare kartläggningar om myndigheters it-kostnader och it-mognad (se kapitel 3) har också omfattat frågor om informationssäkerhet och hur långt myndigheterna bedömt att de kommit i sitt

informationssäkerhetsarbete. Myndigheten för digital förvaltning (Digg) redovisar i sin rapport *Myndigheters digitala mognad och it-kostnader* (2019) resultatet av en enkät till statliga myndigheter. 14 procent av de myndigheter som ingick i enkätundersökningen hade en väl fungerande informationssäkerhetsstrategi på plats som var införd och tillämpades fullt ut på myndigheten. 25 procent av myndigheterna hade implementerat en informationssäkerhetsstrategi i verksamheten som skulle utvärderas och utvecklas. Ungefär lika stor andel hade påbörjat implementeringen av en strategi, medan 30 procent antingen hade påbörjat ett arbete med att ta fram en strategi eller beslutat om en strategi. Knappt tio procent av myndigheterna uppgav att de endast påbörjat en diskussion om att göra något på området. Även om svarsalternativen i Digg:s enkät skiljer sig åt jämfört med våra är de ändå någorlunda jämförbara. Vissa myndigheter har kommit långt i sitt informationssäkerhetsarbete, medan andra avser att påbörja arbetet inom kort eller arbetar med frågorna. En mindre andel myndigheter har inte gjort något alls på området. Digg:s enkät ger dock en något mer positiv bild av hur långt myndigheterna kommit i sitt arbete jämfört med vår enkät. I Digg:s enkät har myndigheterna även fått uppskatta hur arbetet med informationssäkerhet kommer att se ut på myndigheten år 2021 jämfört med 2019. Drygt 70 procent av myndigheterna bedömer att de år 2021 kommer att ha implementerat en informationssäkerhetsstrategi eller ha en väl fungerande informationssäkerhetsstrategi som tillämpas fullt ut på myndigheten. Det innebär alltså nästan en dubblering jämfört med läget år 2019.

Tabell 4.7 Hur långt har myndigheterna kommit i arbetet med informationssäkerhet – enligt myndigheternas egen uppskattning

Svar per kategori

	Antal svar
1. Vi har inte påbörjat ett systematiskt informationssäkerhetsarbete enligt MSBFS 2016:1.	13
2. Vi har påbörjat arbetet genom att ha utsett en ansvarig att leda arbetet och börja analysera hur föreskrifterna MSBFS 2016:1 ska införas i myndigheten.	35
3. Vi har tagit fram en informationssäkerhetspolicy och påbörjat arbetet med styrande interna regelverk. Ledningen har beslutat om informationssäkerhetspolicyn och vi har beslutade styrande interna regelverk för allt informationssäkerhetsarbete enligt MSBFS 2016:1.	29
4. Vi har förutom av ledningen beslutad informationssäkerhetspolicy och styrande interna regelverk, arbetssätt i delar av organisationen som säkerställer att vi genomför informationsklassning och riskbedömning samt inför säkerhetsåtgärder utifrån dessa underlag.	43
5. Vi har förutom av ledningen beslutad informationssäkerhetspolicy och styrande interna regelverk, arbetssätt i hela organisationen som säkerställer att vi genomför informationsklassning och riskbedömning samt inför säkerhetsåtgärder utifrån dessa underlag.	26
6. Allt informationssäkerhetsarbete i hela organisationen sker systematiskt enligt framtaget arbetssätt dokumenterat i interna regler och stöd. Arbetet och de interna regelverken och stöden utvärderas och vidareutvecklas regelbundet.	12
Totalt antal svarande: 158	

Källa: Enkätundersökning.

I vår enkät ställde vi också frågan om myndigheterna utgår från någon standard eller modell som stöd för ett systematiskt informationssäkerhetsarbete. 77 procent av myndigheterna har svarat att de utgår från en standard som stöd för ett systematiskt informationssäkerhetsarbete. Bland dessa utgår alla myndigheter utom en från ISO 27001. Det är en av de standarder som rekommenderas i de nya föreskrifterna från MSB. Knappt 20 procent av myndigheterna anger att de inte utgår från någon standard och sex myndigheter (4 procent) har svarat att de inte vet om de gör det.

Detsamma gäller för informationssäkerhet vid it-upphandling

MSB har gett ut en särskild vägledning om att upphandla informationssäkert (MSB1177). I vägledningen beskrivs bl.a. aktiviteter för att uppnå informationssäkerhet i upphandlingens tre steg – förbereda, upphandla och realisera.

I enkäten fick myndigheterna besvara ett antal frågor om informationssäkerhet vid it-upphandling där utgångspunkt tagits i vägledningen. Myndigheterna har fått uppskatta var de står på en tregradig skala, där den lägsta nivån innebär att man inte reflekterat över frågan på myndigheten och den högsta att myndigheten har ett etablerat arbetssätt på plats. Svaren på de fyra frågorna visar i sig myndigheternas mognadsgrad i olika steg i upphandlingsprocessen.

Tabell 4.8 Har myndigheten en kravkatalog med säkerhetskrav vid it-upphandling?

Antal svar per kategori

	Antal svar
Vi har inte reflekterat över frågan på myndigheten	16
Vi har påbörjat en diskussion om att vi behöver en kravkatalog med säkerhetskrav att utgå ifrån	83
Vi har en säkerhetskravkatalog som vi använder oss av vid upphandling	46
Totalt antal svarande: 154	

Källa: Enkätundersökning.

Tabell 4.9 Har myndigheten ett etablerat arbetssätt för att verifiera säkerhetskrav i anbudssvar vid it-upphandling?

Antal svar per kategori

	Antal svar
Vi har inte reflekterat över frågan på myndigheten	41
Vi har ett påbörjat arbetssätt att verifiera säkerhetskraven i anbudssvar	85
Vi har ett etablerat arbetssätt att verifiera säkerhetskraven i anbudssvar	30
Totalt antal svarande: 156	

Källa: Enkätundersökning.

Tabell 4.10 Har myndigheten ett etablerat arbetssätt att verifiera säkerhetskraven i leverans/acceptanstest/driftsättning (eller motsvarande)?

Antal svar per kategori

	Antal svar
Vi har inte reflekterat över frågan på myndigheten	40
Vi har ett påbörjat arbetssätt att verifiera säkerhetskraven i leverans/ acceptanstest/driftsättning (eller motsvarande)	92
Vi har ett etablerat arbetssätt att verifiera säkerhetskraven i leverans/acceptanstest/driftsättning (eller motsvarande)	25
Totalt antal svarande: 157	

Källa: Enkätundersökning.

Tabell 4.11 Har myndigheten ett etablerat arbetssätt att verifiera säkerhetskraven under avtalets/kontraktets giltighetstid?

Antal svar per kategori

	Antal svar
Vi har inte reflekterat över frågan på myndigheten	45
Vi har ett påbörjat arbetssätt att verifiera säkerhetskraven under avtalets/kontraktets giltighetstid	90
Vi har ett etablerat arbetssätt att verifiera säkerhetskraven under avtalets/kontraktets giltighetstid	20
Totalt antal svarande: 155	

Källa: Enkätundersökning.

Av svaren framgår att en majoritet av myndigheterna har påbörjat en diskussion om kravkatalog eller har en kravkatalog med säkerhetskrav på plats som används vid upphandling och för att värdera anbudssvar. Myndigheterna tycks inte ha kommit lika långt när det gäller att verifiera säkerhetskrav vid leverans och driftsättning eller att verifiera kraven under avtalets giltighetstid.

4.2.4 Fallstudiemyndigheterna

Fallstudierna av de fem typmyndigheterna bekräftar till stora delar den bild som enkätundersökningen ger avseende verksamhet, uppgifter och informationssäkerhet. Av de fem fallstudiemyndigheterna bedriver såväl en stor som en mindre myndighet samhällsviktig verksamhet, vilket ställer särskilda krav på it-driftslösningar och säker-

het. Samtliga fem myndigheter hanterar i större eller mindre omfattning skyddsvärda uppgifter, där olika typer av sekretessreglerade uppgifter och känsliga personuppgifter är vanligast förekommande. Två av myndigheterna hanterar även säkerhetsskyddsklassificerade uppgifter. Några fallstudiemyndigheter lyfter svårigheten att bedöma skyddsvärdet på aggregerade uppgifter i verksamheten. De upplever också att det är svårt att få stöd i denna typ av bedömningar, exempelvis från expertmyndigheter.

Företrädare för några fallstudiemyndigheter framhåller att det kan vara svårt att avgöra vilka krav på it-driftslösningar som ställs för olika typer av uppgifter som hanteras i verksamheten. Det gäller framför allt känsliga personuppgifter och uppgifter som omfattas av ett omvänt skaderekvisit, dvs. där det finns en presumtion för sekretess. För att värna säkerheten hanterar de aktuella myndigheterna denna typ av uppgifter i egen regi.

Fallstudiemyndigheterna har kommit olika långt i sitt informationssäkerhetsarbete. Det finns ingen tydlig koppling till myndighetsstorlek. Stora myndigheter hanterar i regel en större mängd uppgifter och måste därför lägga mer tid på informationsklassificering jämfört med mindre myndigheter. En av de mindre myndigheterna pekar på att informationssäkerhetsarbetet kräver att myndigheten har egen kompetens och förmåga att arbeta med informationssäkerhet, vilket kan vara svårt att uppnå.

Den sammantagna bilden är att kraven på it-drift styrs av vilken typ av verksamhet en myndighet bedriver och vilken typ av uppgifter myndigheten hanterar. Små myndigheter kan därmed behöva ställa lika höga krav på säkra it-driftslösningar som större myndigheter.

4.3 Hinder för säker och kostnadseffektiv it-drift

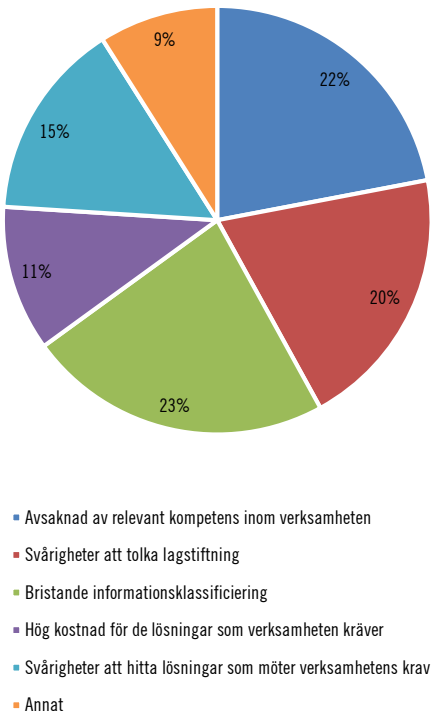
Pensionsmyndigheten konstaterade i sitt uppdrag om molntjänster i staten år 2015 att de största upplevda hindren för statliga myndigheter att använda molntjänster handlade om säkerhet och oklarheter kring de juridiska förutsättningarna för att använda molntjänster. Att tillämpa gällande regelverk och balansera integritetsskydd och effektivitet upplevdes också som svårt.

I vår enkätundersökning har vi ställt frågor om hinder för och bristande förutsättningar för säker och kostnadseffektiv it-drift. Myndigheterna har fått välja mellan ett antal angivna hinder, men också fått ange andra eventuella hinder i fritext. De har också fått ange varför de har angett ett visst hinder.

4.3.1 Hinder för säker it-drift

Det kan finnas flera hinder för myndigheter att säkerställa en säker it-drift. Hindren kan finnas både inom den egna myndigheten och utanför myndigheten. Av Figur 4.3 framgår svarsfördelningen för de förangivna svarsalternativen i enkäten.

Figur 4.3 Hinder för säker it-drift enligt myndigheternas enkätsvar



Källa: Enkätundersökning.

För de 143 myndigheter som svarat på frågan är bristande informationsklassificering tillsammans med avsaknad av relevant kompetens inom verksamheten och svårigheter att tolka lagstiftning de största hindren för en säker it-drift. Detta är särskilt tydligt för de stora myndigheterna. För små myndigheter är rangordningen följande: avsaknad av relevant kompetens, svårigheter att tolka lagstiftning och därefter hög kostnad för de lösningar som verksamheten kräver.

Att myndigheterna angett bristande informationsklassificering överensstämmer med myndigheternas uppskattningar av det egna informationssäkerhetsarbetet (se avsnitt 4.2.3). I myndigheternas kommentarer om bristande informationsklassificering framkommer att det pågår arbete på flera myndigheter. Myndigheterna har i flera fall klassat delar av informationen, men inte all information. Bristande kompetens och resurser lyfts fram som problem i sammanhanget, men även tidsbrist anges. En myndighet anger att de saknar systemstöd för informationsklassificering. En annan myndighet menar att det är svårt att översätta informationsklassificeringen till konkreta säkerhetsnivåer i både hård- och mjukvara. Ytterligare ett problem som lyfts fram är svårigheten att informationsklassa aggregerad information.

Avsaknad av relevant kompetens upplevs som ett lika stort hinder för säker it-drift som bristande informationsklassificering. Flera små myndigheter skriver i sina kommentarer att det är svårt att som liten myndighet ha egen kompetens såväl inom it och säkerhet som beställarkompetens. Det kan också vara svårt att hitta och rekrytera rätt kompetens, exempelvis när nyckelpersoner slutar. Flera myndigheter köper in kompetens från antingen en annan myndighet eller från företag, vilket i sig innebär ett beroende av extern kompetens. Enligt flera myndigheter ses kompetensbrist som en riskfaktor.

Det tredje största hindret som myndigheterna ser är svårigheter att tolka gällande lagstiftning. Oklarheter vad gäller användning av molntjänster verkar vara vanligast. Svårigheten att göra bedömningar av säkerhetsskydd lyfts också fram som ett problem av flera myndigheter, liksom oklarheter kring krav på datalagring och dataskydd. En myndighet menar att det är svårt att få en sammanhängande bild av samtliga regelverk och hur de ska tolkas beroende på vilken tjänst som ska utvärderas. En annan myndighet pekar på att det är svårt att få juridik, it och informationssäkerhet att mötas. Ytterligare en myndighet lyfter fram att det inte är tolkningen av lagstiftningen som är

problemet, utan snarare effekterna av tolkningen som medför svårigheter att genomföra upphandlingar och upprätthålla en stabil it-drift över tid.

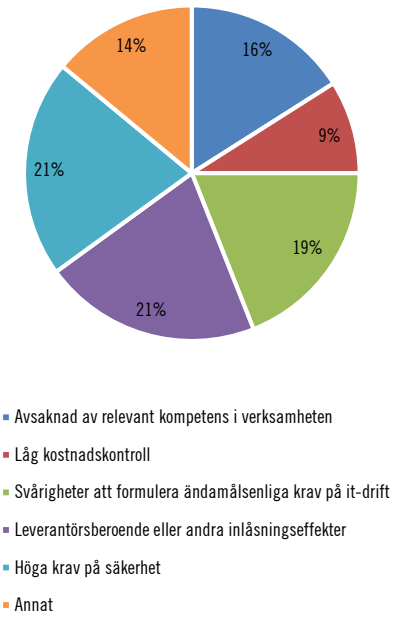
Hög kostnad för de lösningar som verksamheten kräver anges som ytterligare ett hinder för säker it-drift. Flera myndigheter pekar på att säkerhet kostar. Alternativet egen drift bedöms som relativt kostsamt av flera myndigheter. Någon myndighet påpekar att även samordnad it-drift kan vara en relativt dyr lösning. Även svårigheter att hitta lösningar som möter verksamhetens krav upplevs som ett hinder. När fler tjänster blir molnbaserade blir det svårare att hitta lösningar som uppfyller säkerhetskraven. Hårda säkerhetskrav påverkar i sig möjligheterna att nyttja billigare och effektiva it-driftstjänster. Flera myndigheter lyfter svårigheten att kravställa. Verksamhetens krav på digitalisering och kostnadseffektiva lösningar ställs ofta mot krav på säkerhet.

Andra hinder för säker it-drift som lyfts fram i enkäten är bl.a. att det finns för lite resurser för it och säkerhet och att säkerhet inte prioriteras tillräckligt i verksamheten. Några myndigheter lyfter att de har en teknikskuld att hantera, vilket påverkar förutsättningarna att arbeta med säkerhetsfrågor. En myndighet menar att avsaknaden av en samlad statlig strategi leder till att varje myndighet gör egna utredningar, bedömningar och bygger egna lösningar för att uppfylla säkerhetskraven.

4.3.2 Hinder för kostnadseffektiv it-drift

Myndigheterna har också fått ange vilka hinder de ser för att upprätthålla en kostnadseffektiv it-drift. Det var något färre myndigheter (132) som besvarade denna fråga jämfört med frågan om hinder för säker it-drift. En förklaring kan vara att färre myndigheter ser hinder för kostnadseffektivitet, en annan förklaring kan vara att kostnadseffektivitet inte står lika högt på agendan som frågan om säkerhet.

Figur 4.4 Hinder för kostnadseffektiv it-drift enligt myndigheternas enkätsvar



Källa: Enkätundersökning.

Som framgår av Figur 4.4 ovan anger flest myndigheter höga krav på säkerhet och leverantörsberoende eller andra inlåsningseffekter som hinder för en kostnadseffektiv it-drift. Bland stora myndigheter är även svårigheten att formulera ändamålsenliga krav på it-drift ett hinder som många anger. För små myndigheter är även här avsaknad av relevant kompetens det största hindret.

Den vanligaste kommentaren är att säkerhet kostar och att säkerhetskrav påverkar möjligheterna att använda kostnadseffektiva it-lösningar. En myndighet konstaterar att om en myndighet hanterar känsliga uppgifter är det nödvändigt med höga krav på säkerhet. En annan myndighet pekar på att säkerhetsåtgärder kan vara kostnadsdrivande, men frånvaro av korrekta åtgärder kan skada verksamheten och orsaka andra större kostnader.

När det gäller leverantörsberoende anger flera myndigheter att de sitter fast i enskilda leverantörers lösningar. På vissa områden och tjänster finns endast ett fåtal leverantörer. Det handlar inte enbart om privata tjänsteleverantörer, utan även om myndigheter eller konsortier som erbjuder lösningar för it-drift. Att byta leverantör kan vara både komplext och kostsamt. Krav på regelbunden upphandling och ny konkurrensutsättning kan i sig minska inlåsningseffekterna, men det kan också vara problematiskt om myndigheten är nöjd med befintliga lösningar. Myndigheter har i regel investerat såväl kunskap, lösningar och licenser i relation till enskilda leverantörer. För att undvika kompetensproblem vid leverantörsbyte är det viktigt att säkerställa krav på dokumentation. Långa avtalsperioder är ett problem om myndigheten inte är nöjd med leverantören. I övrigt anger en myndighet att de saknar ramavtal för it-drift som de kan avropa ifrån, medan en annan myndighet menar att ramavtal kan innebära onödigt höga kostnader för små myndigheter.

Svårigheter att formulera ändamålsenliga krav för it-drift kan också påverka kostnadseffektiviteten. Att hitta rätt kravnivå (inte för höga eller för låga krav) som dessutom håller under hela avtalsperioden är en stor utmaning. Myndigheterna har ofta många krav som dessutom kan förändras över tid. De krav myndigheterna ställer stämmer inte alltid överens med de standardlösningar som leverantörer erbjuder, vilket ger höga kostnader. I myndigheternas arbete med kravställning är det viktigt att it- respektive kärnverksamheten samverkar och förstår varandra, vilket inte alltid fungerar.

Även avsaknad av kompetens, och särskilt beställarkompetens, anges som hinder för kostnadseffektiv it-drift. Konkurrensen om experter är stor. Låg kostnadskontroll ses också som ett hinder men inte i lika stor omfattning. Några myndigheter anger att det inte finns ekonomiska strukturer för att följa upp kostnader på ett bra sätt. En annan myndighet utvecklar en modell för kostnadsuppföljning och uppföljning av kostnad i relation till nytta.

4.4 Myndigheternas it-drift i dag

4.4.1 Ungefär två tredjedelar av myndigheterna har eget datacenter

Datacenter har flera besläktade begrepp såsom datorhall och serverhall. De beskriver alla särskilda anläggningar eller utrymmen avsedda för att inrymma servrar och annan utrustning och hårdvara för lagring och kommunikation samt infrastruktur för kraftförsörjning, kylning, brandsläckning, säkerhetsskydd etc. Som referens till vad ett datacenter innehåller har Kammarkollegiet ett ramavtal för datacenter där begreppet ”driftstjänst” används. Begreppet datacenter definieras inte direkt, däremot beskrivs att leverantörer av datacentertjänster tillhandahåller tjänster

> […] som minst innefattar strömförsörjning, kylning, brandskydd, fysisk säkerhet och tillhörande övervakning. Drifttjänst kan dessutom inkludera Hårdvara och/eller Programvara.

Regeringen preciserade i lagrådsremissen Vissa frågor på elskatteområdet från den 9 juni 2016 datorhallar som

> […] anläggningar där en näringsidkare, som huvudsakligen bedriver informationstjänstverksamhet, informationsbehandling eller uthyrning av serverutrymme och tillhörande tjänster, utövar sådan verksamhet, och vars sammanlagda installerade effekt uppgår till minst 0,1 megawatt [effekten för kyl- och fläktanläggningar räknas ej med i den installerade effekten]

Vidare beskrivs att utrustningen i ett datacenter består av

> […] it-utrustning och reserv- och skyddssystem för denna utrustning. Den förstnämnda typen av utrustning är naturligtvis det centrala, medan förekomsten och omfattningen av sistnämnda system kan variera. […] IT-utrustningen i ett datacenter består av servrar, lagringssystem och utrustning för datakommunikation […] Utrustningen kan ägas av den som driver datorhallen eller av dennes kunder.

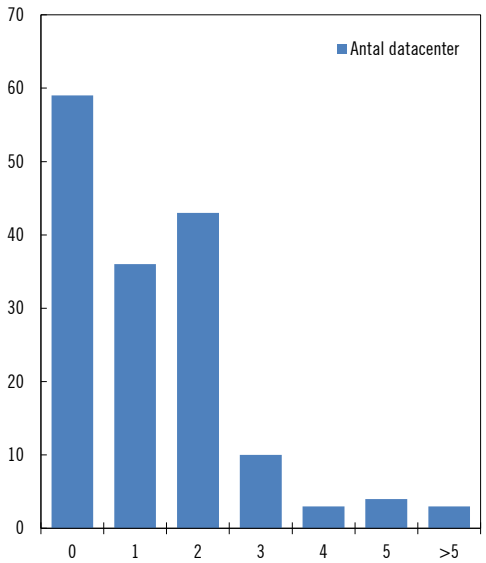
I vår enkät har begreppet datacenter definierats som

> ett fysiskt utrymme där hela eller merparten av er utrustning för servrar, lagring och kommunikationsutrustning finns. Utrymmet kan vara anpassat med avseende på t.ex. kylsystem, elförsörjning, brand- och skalskydd.

Definitionen är formulerad på ett allmänt sätt utan krav på t.ex. viss installerad effekt i syfte att fånga både mer avancerade anläggningar såväl som mindre serverutrymmen i myndigheternas lokaler. Definitionen medger även viss möjlighet till jämförelse med resultatet från den enkätundersökning Statens servicecenter (SSC) genomförde år 2016 och som också berörde myndigheternas datacenter.

Av 158 respondenter som svarat på frågan om datacenter i vår enkät har 58 procent (100) uppgivit att de har egna datacenter. Tillsammans har de sammanlagt 220 datacenter, då flera av de som har datacenter har fler än ett.

Figur 4.5 Antal datacenter per svarande



Källa: Enkätundersökning.

Det finns ett visst samband mellan storlek på myndigheten och andelen med datacenter.

Tabell 4.12 Myndigheter med egna datacenter

Myndighetens storlek	Antal	Andel myndigheter som uppgett att de har egna datacenter	Totalt antal datacenter
Små myndigheter (1–49)	11	38 %	12
Medelsmå myndigheter (50–199)	16	39 %	24
Medelstora myndigheter (200–499)	24	80 %	38
Stora myndigheter (500–)	49	84 %	146
Totalt	**100**	**58 %**	**220**

Källa: Enkätundersökning.

Vidare går det att se ett visst samband mellan storlek på myndigheten och antalet fysiska servrar myndigheten har i sin verksamhet.

Fallstudiemyndigheterna

Resultatet från vår enkätundersökning bekräftas i intervjuerna med fallstudiemyndigheterna. Fyra av de fem intervjuade myndigheterna har egna datacenter.

- En av myndigheterna är ett lärosäte som har fem datacenter. Två av dessa beskrivs som fullt redundanta datacenter med reservkraft, redundant kyla och avbrottsfri kraftförsörjning, medan tre av dem beskrivs som serverrum.
- En annan myndighet har två datacenter. Det ena är ett serverrum i myndighetens lokaler. Myndigheten flyttade för två år sedan, i samband med att ett hyreskontrakt löpte ut, in i ett datacenter hos en tjänsteleverantör där den hyr en ”säker bur” som endast myndigheten har åtkomst till. Myndigheten sköter driften själv på båda platserna och anser att det är mer kostnadseffektivt med samlokalisering än om den skulle expanderat genom att hyra egna lokaler.
- En stor myndighet har utrustning i fyra datacenter, varav två är i myndighetens egna lokaler och de två andra tillhör en annan myndighet respektive ett kommunalt bolag. Myndigheten beskriver att den även hyr en säker bur hos det kommunala bolaget där de

placerat utrustning. Två av myndighetens datacenter är fullt speglade på ett sätt som ställer tekniska krav på geografisk närhet.

- Den minsta myndigheten som ingått i fallstudien har inga egna datacenter utan erhåller it-arbetsplatser och andra it-tjänster från en annan myndighet inom ramen för ett helhetsåtagande.

Flera av fallstudiemyndigheterna framhåller att det är viktigt att de datacenter de använder är nära belägna, både för att de ska vara lättillgängliga för verksamheten, men i vissa fall även på grund av tekniska krav på accesstid. För de myndigheter som använder samlokalisering har myndigheterna bl.a. värdesatt kostnad, leverantörens erfarenhet och om leverantören har andra kunder från offentlig sektor.

Då det finns stor spridning inom varje storleksgrupp av myndigheter bör genomsnittet tolkas med viss försiktighet. Resultatet överensstämmer relativt väl med den enkätundersökning SSC genomförde år 2016 där 67 procent av myndigheterna uppgav att de tillsammans hade sammanlagt 206 datacenter. Givet att urvalet av myndigheter som svarade på vår respektive SSC:s enkät skiljer sig åt går det dock inte att dra slutsatsen att andelen myndigheter med eget datacenter minskat. Det ger dock viss tillförlitlighet i att andelen myndigheter med eget datacenter är ungefär två tredjedelar. Det är vidare vanligare bland medelstora och stora myndigheter att ha egna datacenter.

4.4.2 Användningen av molntjänster från privata tjänsteleverantörer är utbredd i statsförvaltningen

I vår enkät har vi ställt frågor om myndigheternas användning av molntjänster[1] från privata tjänsteleverantörer. Användning av publika molntjänster medför i regel en utkontraktering av den it-drift som tjänsten kräver. Det bör poängteras att det finns andra typer av it-driftsrelaterade tjänster än molntjänster. Vi har försökt komplettera bilden av behoven genom fallstudierna.

[1] Se definition i avsnitt 2.2.4.

Tabell 4.13 Myndigheter som använder molntjänster

Andel som använder molntjänster inom respektive storleksgrupp (och antal svarande)

Myndighetens storlek	IaaS	PaaS	SaaS
Små myndigheter (1–49)	17 % (5)	21 % (6)	79 % (23)
Medelsmå myndigheter (50–199)	41 % (17)	32 % (13)	78 % (32)
Medelstora myndigheter (200–499)	33 % (10)	30 % (9)	93 % (28)
Stora myndigheter (500–)	40 % (23)	36 % (21)	100 % (58)
Totalt	**35 % (55)**	**31 % (49)**	**89 % (141)**

Källa: Enkätundersökning.

Andelen myndigheter som använder IaaS-tjänster är nästan genomgående större än motsvarande andel för PaaS-tjänster. Användningen är som mest utbredd av SaaS-tjänster. Samtliga stora myndigheter uppger att de använder SaaS-tjänster.

Drift i egen regi är inte ett substitut till användning av molntjänster

Genom att undersöka andelen myndigheter som använder molntjänster och även har datacenter och drift i egen regi kan vi analysera om molntjänster används som ett likvärdigt alternativ till drift i egen regi.

Tabell 4.14 Myndigheter som använder molntjänster och har egna datacenter

Andel som använder molntjänster inom respektive storleksgrupp (och antal svarande)

Myndighetens storlek	IaaS	PaaS	SaaS
Små myndigheter (1–49)	18 % (2)	9 % (1)	91 % (10)
Medelsmå myndigheter (50–199)	25 % (4)	25 % (4)	88 % (14)
Medelstora myndigheter (200–499)	25 % (6)	25 % (6)	92 % (22)
Stora myndigheter (500–)	43 % (21)	43 % (21)	100 % (49)
Totalt	**33 % (33)**	**32 % (32)**	**95 % (95)**

Källa: Enkätundersökning.

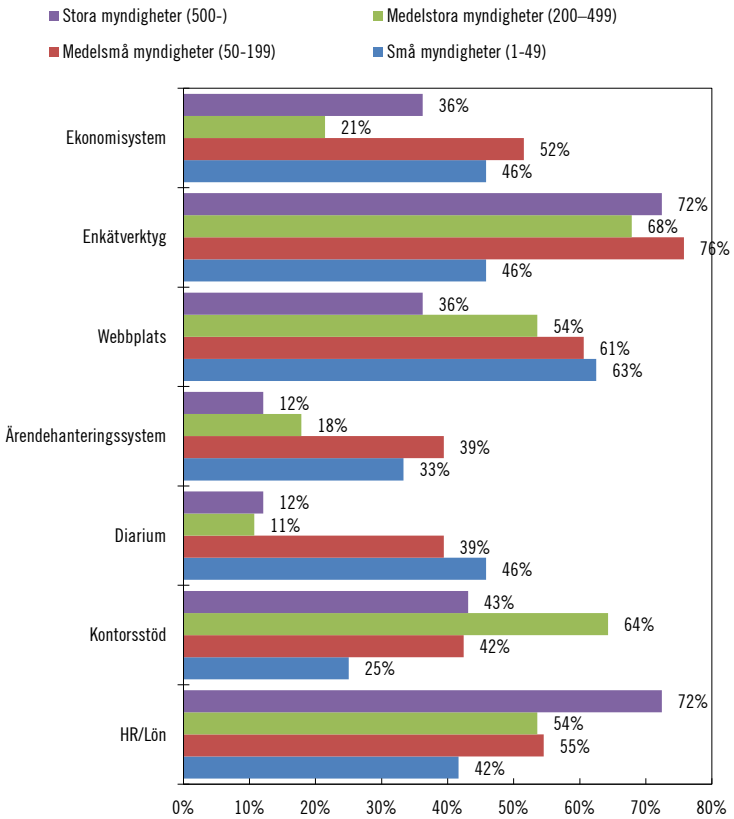
Det är små skillnader i andelen myndigheter som använder IaaS- och PaaS-tjänster beroende på om myndigheterna har egna datacenter eller inte. En tolkning av detta är att drift i egen regi som regel inte utgör ett substitut till att använda sådana molntjänster.

SaaS-tjänster används för flera olika funktioner

Vi har i enkäten frågat om vanliga funktioner för vilka SaaS-tjänster används på myndigheterna, i syfte att ge en övergripande bild av användning och funktioner.

Figur 4.6 Andel myndigheter som använder SaaS

Fasta svarsalternativ



Källa: Enkätundersökning.

Av enkätsvaren framgår att SaaS-tjänster används till alla de funktioner och användningsområden som vi exemplifierat med. Exempelvis upphandlar många myndigheter, oavsett storlek, enkätverktyg som SaaS-tjänst. De exakta andelarna för Ekonomisystem respektive HR och lön bör tolkas med viss försiktighet eftersom vissa myndigheter kan ha uppgett de tjänster de erhåller från SSC, trots att molntjänster som upphandlats från privata tjänsteleverantörer efterfrågades i enkäten. Utöver de exemplifierade funktionerna för SaaS-tjänster gav myndigheter även andra exempel i fritext, däribland: spamfilter, upphandlingsverktyg, rekryteringsverktyg, resebokningss- och reseräkningsverktyg, verktyg för schemaläggning och planering, samarbetsytor samt Microsoft Office 365. Det bör noteras att eftersom begreppet kontorsstöd inte definierades i enkäten kan myndigheter som angett detta även avsett t.ex. Microsoft Office 365.

Fallstudiemyndigheterna

Myndigheterna i fallstudien har genomgående en restriktiv hållning till användning av publika molntjänster från privata tjänsteleverantörer. I den utsträckning de använder publika molntjänster handlar det ofta om stödverktyg eller lösningar som myndigheterna inte har möjlighet att drifta i egen regi. Samtidigt är det ingen av myndigheterna som vi har intervjuat som har fattat ett formellt beslut eller har en uttalad princip om att inte använda publika molntjänster.

- En stor myndighet beskriver att de använder ett kontorsstöd som körs på egna servrar men med en molnbaserad katalogtjänst. Myndigheten ser behov av att bygga upp en hybridmiljö.
- En annan stor myndighet beskriver att de använder molntjänster i begränsad omfattning. Myndigheten är samtidigt positivt inställd till att använda molntjänster där det går, främst av det skälet att myndigheten har svårt med kompetensförsörjning och ser molntjänster som ett sätt att dra nytta av extern kompetens.
- Det universitet som finns med bland fallstudiemyndigheterna använder vissa publika molntjänster för studenter, t.ex. Microsoft Office 365, men har en mer restriktiv hållning för andra användare och har för dessa valt on-premlösningar. I de fall där det gått att välja datalokalisering har universitetet valt datacenter inom EU

eller EES. Universitetet köper även tjänster från SUNET vars drift i vissa fall är utkontrakterad till privata tjänsteleverantörer.

Flera av de intervjuade myndigheterna understryker att nyckeln till en flexibel och kostnadseffektiv användning av molntjänster är en väl utförd informationsklassificering. I förlängningen innebär det även att informationsseparation är nödvändigt, då många informationsresurser består av både skyddsvärd och icke skyddsvärd information.

4.4.3 Nästan var fjärde myndighet får någon form av it-drift tillhandahållen av en annan myndighet

Bland de 158 myndigheterna som svarat på enkäten får 23 procent (36) it-drift från en annan myndighet, medan 9 procent (14) uppger att de tillhandahåller it-drift till annan myndighet. Inga små myndigheter som svarat på enkäten tillhandahåller it-drift till någon annan myndighet.

Tabell 4.15 Myndigheter med samordnad it-drift

Samordnad it-drift omfattar allt från helhetsåtagande för it till drift av enskilda applikationer. Andel myndigheter inom respektive storleksgrupp som får it-drift av, respektive tillhandahåller it-drift till, annan myndighet (antal)

Myndighetens storlek	Annan myndighet hanterar respondentens it-drift		Respondenten hanterar annan myndighets it-drift
	Inkl. de myndigheter som endast uppgett SSC	*Exkl. de myndigheter som endast uppgett SSC*	
Små myndigheter (1–49)	28 % (8)	25 % (7)	-
Medelsmå myndigheter (50–199)	15 % (6)	13 % (5)	12 % (5)
Medelstora myndigheter (200–499)	20 % (6)	11 % (3)	10 % (3)
Stora myndigheter (500–)	29 % (16)	27 % (14)	10 % (6)
Totalt	**23 % (36)**	**20 % (29)**	**9 % (14)**

Källa: Enkät.

Samordnad it-drift förekommer i olika former

Bland exemplen på samordnad it-drift finns allt från myndigheter som tillhandahåller specifika tjänster, såsom de HR- och lönerelaterade tjänster som SSC tillhandahåller, till helhetsåtagande i de fall en myndighet hanterar all it åt en annan myndighet. Ett exempel på det senare är en mindre myndighet som tillhandahåller it-arbetsplatser och andra tjänster och applikationer till en liten myndighet. Det finns även fler exempel på mindre myndigheter som erbjuds ett helhetsåtagande för it av den värdmyndighet hos vilka de är lokaliserade. Vidare finns exempel på myndigheter som sköter drift och förvaltning av tjänster för hela förvaltningen, såsom digital post. I enkäten finns det även exempel på samordnad it-drift i form av att en myndighet får låna utrymme i en annan myndighets datacenter.

Olika sektorer och områden inom statsförvaltningen är olika samordnade

Från enkätresultatet går det att se att vissa områden och sektorer har samordnat sin it-verksamhet i större utsträckning än andra. Det gäller bl.a. domstolar, länsstyrelser och lärosäten. Många universitet och högskolor både får och tillhandahåller it-drift av respektive till varandra. SUNET, som administreras av Vetenskapsrådet, erbjuder tjänster för datorkommunikation, identitetshantering och it-drift för bl.a. universitet och högskolor. Det pågår för närvarande en utredning som har till uppgift att se över forskningsinfrastruktur på nationell nivå, där bl.a. e-infrastruktur såsom SUNET särskilt pekas ut (Dir. 2020:52). Flera myndigheter med värdmyndighet har uppgett att värdmyndigheten hanterar deras it-drift (oftast nämnder och råd). Slutligen rapporterar flera myndigheter att de samordnat sin it-drift med Försäkringskassan, som en del av myndighetens uppdrag att tillhandahålla samordnad och säker statlig it-drift. Även Skatteverket nämns i detta sammanhang.

Fallstudiemyndigheterna

Fyra av de fem intervjuade myndigheterna har samordnat sin it-drift på något sätt med andra myndigheter.

- För universitetet handlar det om den e-infrastruktur som finns inom högskole- och universitetssektorn med ett antal gemensamma tjänster som förvaltas av Vetenskapsrådet och SUNET, UHR och genom konsortium. Några exempel på tjänster är betygsregistret LADOK, kulturarvsplattformen Alvin och publikationsarkivet DiVA. Till detta tillkommer även infrastruktur från SUNET såsom universitetsdatanätverket, identitetsfederationer m.m.
- En stor myndighet har samordnat sig med en annan stor myndighet som är lokaliserade i närheten. De båda myndigheterna har lånat ut utrymme i varandras datacenter för att möjliggöra redundans och säkerhetskopiering.
- En liten myndighet vi intervjuat får nästan samtliga it-relaterade tjänster de har behov av från en värdmyndighet. Myndigheten har aldrig haft it-drift i egen regi och för i dag en dialog med Försäkringskassan i syfte att kunna få tjänster inom ramen för uppdraget om Samordnad och säker statlig it-drift.

Alla fallstudiemyndigheter är försiktigt positiva till en samordnad statlig it-drift. De har både positiva och negativa erfarenheter av samordnade tjänster. Myndigheterna ser en risk att samordnade tjänster kan bli dyrare än om myndigheterna själva anskaffar motsvarande tjänster. Enligt myndigheterna finns det samordnade tjänster som håller lägre servicenivå. De ser också att det skulle kunna innebära en viss förlust av kontroll om anslutningen till en samordnad it-drift skulle bli förordningsstyrd.

4.4.4 Nästan en tredjedel av myndigheterna använder samlokalisering

Utrustningen i ett datacenter kan ägas av den som driver datorhallen eller av någon annan. Det sistnämnda är vanligen fallet i fråga om s.k. samlokalisering där ett företag hyr ut utrymme i sitt datacenter. Samlokalisering kallas ibland även co-location eller Housing as a Ser-

vice (HaaS). Begreppet samlokalisering används vanligen för att benämna en kommersiell tjänst, men förekommer även i de fall myndigheter tillhandahåller utrymme i sina datacenter till andra myndigheter. Det bör tilläggas att den som erbjuder samlokalisering inte nödvändigtvis måste äga den byggnad som rymmer ett datacenter.

Ungefär en tredjedel av myndigheterna uppger att de använder samlokalisering. Mest vanligt är det bland medelsmå myndigheter där nästan hälften av de svarande använder samlokalisering.

Tabell 4.16 Myndigheter som använder samlokalisering från en privat tjänsteleverantör

Myndighetens storlek	Antal	Andel
Små myndigheter (1–49)	10	34 %
Medelsmå myndigheter (50–199)	19	46 %
Medelstora myndigheter (200–499)	8	27 %
Stora myndigheter (500–)	15	26 %
Totalt	**52**	**33 %**

Källa: Enkätundersökning.

4.4.5 Vanligare med it-arbetsplats och stödtjänster från privata leverantörer än från andra myndigheter

För att även fånga andra typer av it-verksamheter som myndigheterna kan utkontraktera eller samordna sig kring, har vi i enkäten undersökt om myndigheterna själva hanterar sina it-arbetsplatser och stödtjänster. It-arbetsplatser definieras i enkäten som administration, underhåll och leverans av paketerade stationära eller bärbara arbetsdatorer med tillbehör och programvara. Stödtjänster definieras i enkäten som helpdesk, stöd och support till myndighetens personal i it-relaterade frågor.

Tabell 4.17 Myndigheter med it-arbetsplats från privat leverantör respektive annan myndighet

Andel myndigheter med stödtjänster (samt antal)

Myndighetens storlek	It-arbetsplats från privat leverantör	It-arbetsplats från annan myndighet
Små myndigheter (1–49)	31 % (9)	28 % (8)
Medelsmå myndigheter (50–199)	49 % (20)	7 % (3)
Medelstora myndigheter (200–499)	13 % (4)	0 % (0)
Stora myndigheter (500–)	14 % (8)	3 % (2)
Totalt	**26 % (41)**	**8 % (13)**

Källa: Enkätundersökning.

Små och medelsmå myndigheter köper färdigpaketerade it-arbetsplatser i större utsträckning från privata tjänsteleverantörer. För små myndigheter är det heller inte ovanligt att få it-arbetsplatser tillhandahållna av en annan myndighet. Det senare resultatet ligger i linje med att mindre myndigheter i vissa fall får sin it tillhandahållen som ett helhetsåtagande av en större myndighet, där it-arbetsplatser då ingår.

Tabell 4.18 Myndigheter med stödtjänster från en privat tjänsteleverantör respektive annan myndighet

Andel myndigheter med stödtjänster (samt antal)

Myndighetens storlek	Stödtjänster från privat tjänsteleverantör	Stödtjänster från annan myndighet
Små myndigheter (1–49)	62 % (18)	31 % (9)
Medelsmå myndigheter (50–199)	46 % (19)	12 % (5)
Medelstora myndigheter (200–499)	23 % (7)	3 % (1)
Stora myndigheter (500–)	16 % (9)	7 % (4)
Totalt	**34 % (53)**	**12 % (19)**

Källa: Enkätundersökning.

Stödtjänster har i ännu högre grad än it-arbetsplatser utkontrakterats till privata tjänsteleverantörer, och i nästa led till en annan myndighet. Det är framför allt mindre myndigheter som utkontrakterat funktioner såsom helpdesk och support.

4.5 Kostnader för it-drift

För att uppskatta kostnaderna för it-drift i statsförvaltningen har vi i enkäten ställt frågor om platsbundna och icke platsbundna kostnader för datacenter, kostnader för upphandlade molntjänster och kostnader för samordnad it-drift. Uppdelningen i platsbundna och icke platsbundna kostnader syftar till att särskilja de kostnader för myndigheters datacenter som vid konsolidering skulle utgå respektive kvarstå. Platsbundna kostnader definieras som

> […] summan av kostnader för lokaler, el, kylsystem, larm, skal- och brandskydd. Dvs. kostnaden för alla tillgångar som är knutna till den fysiska platsen för datacentret.

4.5.1 Platsbundna och icke platsbundna kostnader

Myndigheternas platsbundna kostnader uppgår till 126 miljoner kronor årligen

Av de 158 myndigheter som svarat på enkäten har 100 uppgett att de har egna datacenter. Av dessa har 79 vidare uppgett att de har platsbundna kostnader som uppgår till sammanlagt 126 miljoner kronor årligen. Sex myndigheter har uppgett att de inte har egna datacenter, men ändå platsbundna kostnader för sammanlagt 2,6 miljoner kronor. Samtliga av dessa sex använder samlokalisering, antingen hos en privat tjänsteleverantör eller i en annan myndighets datacenter. 21 myndigheter har angett att de har egna datacenter, men har inte uppgett några platsbundna kostnader. Flera av dessa 21 myndigheter hänvisar till att de platsbundna kostnaderna är del av lokalhyran som inte går att särredovisa.[2]

[2] De 21 myndigheterna har en liknande storleksfördelning som de 79 som svarat på frågan om platsbundna kostnader. Med antagandet att dessa myndigheters platsbundna kostnader är samma som de genomsnittliga kostnaderna för de som svarat på frågan (inom respektive storleksgrupp), skulle det innebära att ytterligare cirka 30 miljoner kronor för platsbundna kostnader tillkommer.

Tabell 4.19 Platsbundna kostnader

Myndighetens storlek	Antal svarande	Årliga genomsnittliga kostnader i tkr	
		Medel	Median
Små myndigheter (1–49)	8	113	50
Medelsmå myndigheter (50–199)	12	620	190
Medelstora myndigheter (200–499)	22	874	195
Stora myndigheter (500–)	37	2 668	1 150
Totalt	**79**	**1 599**	**400**

Källa: Enkätundersökning.

Det går att se ett visst samband mellan storleken på myndigheterna och deras platsbundna kostnader. Samtidigt är det viktigt att notera att ett fåtal myndigheter står för en stor del av de sammanlagda platsbundna kostnaderna. Denna skevhet i fördelningen finns även i olika grupper av myndigheter av samma storlek.

Myndigheternas icke platsbundna kostnader uppgår till ungefär 810 miljoner kronor årligen

De icke platsbundna kostnader som efterfrågats i enkäten har definierats som

> […] kostnader för servrar, nätverksutrustning, lagring, kringutrustning etc. som potentiellt kan flyttas till ett nytt datacenter.

Av 100 myndigheter med eget datacenter har 87 svarat att de har icke platsbundna kostnader motsvarande sammanlagt 810 miljoner kronor per år. Även tre myndigheter utan egna datacenter, men som använder samlokalisering, har uppgett att deras icke platsbundna kostnader uppgår till sammanlagt ungefär 5 miljoner kronor per år. Det finns ett bortfall om 13 myndigheter som har svarat att de har datacenter men inte några icke platsbundna kostnader.

Tabell 4.20 Icke platsbundna kostnader

Myndighetens storlek	Antal svarande	Årliga genomsnittliga kostnader i tkr	
		Medel	Median
Små myndigheter (1–49)	10	259	205
Medelsmå myndigheter (50–199)	13	2 011	350
Medelstora myndigheter (200–499)	21	1 602	898
Stora myndigheter (500–)	43	17 393	6 000
Totalt	**87**	**9 313**	**1 454**

Källa: Enkätundersökning.

På samma sätt som med de platsbundna kostnaderna är de icke platsbundna kostnaderna ojämnt fördelade, både sett till helheten men även inom grupper av myndigheter av liknande storlek. Det finns inget uppenbart samband mellan platsbundna och icke platsbundna kostnader på myndigheterna, såsom att kvoten mellan dessa kostnader är ungefär densamma för olika myndigheter.

4.5.2 Kostnader för molntjänster

Myndigheterna spenderar sammanlagt 700 miljoner kronor per år på molntjänster

Myndigheterna spenderar sammanlagt 137, 66 och 497 miljoner kronor för IaaS-, PaaS- respektive SaaS-tjänster. Summorna är baserade på myndigheternas årliga genomsnittliga kostnader. På liknande sätt som med de plats- och icke platsbundna kostnaderna, står ett antal myndigheter för en större andel av de sammanlagda kostnaderna för molntjänster.

Tabell 4.21 Kostnader IaaS

Myndighetens storlek	Antal svarande	Årliga genomsnittliga kostnader i tkr	
		Medel	Median
Små myndigheter (1–49)	4	176	147
Medelsmå myndigheter (50–199)	14	2 269	1 722
Medelstora myndigheter (200–499)	9	2 762	325
Stora myndigheter (500–)	17	4 687	220
Totalt	**44**	**3 114**	**343**

Källa: Enkätundersökning.

Tabell 4.22 Kostnader PaaS

Myndighetens storlek	Antal svarande	Årliga genomsnittliga kostnader i tkr	
		Medel	Median
Små myndigheter (1–49)	6	632	170
Medelsmå myndigheter (50–199)	12	920	500
Medelstora myndigheter (200–499)	8	621	110
Stora myndigheter (500–)	16	2 895	550
Totalt	**42**	**1 574**	**283**

Källa: Enkätundersökning.

Tabell 4.23 Kostnader SaaS

Myndighetens storlek	Antal svarande	Årliga genomsnittliga kostnader i tkr	
		Medel	Median
Små myndigheter (1–49)	16	698	650
Medelsmå myndigheter (50–199)	30	1 133	650
Medelstora myndigheter (200–499)	24	1 880	1 200
Stora myndigheter (500–)	46	8 849	2 225
Totalt	**116**	**4 287**	**1 083**

Källa: Enkätundersökning.

4.5.3 Kostnader för samordnad it-drift

Myndigheterna betalar årligen 411 miljoner kronor till andra myndigheter för olika it-relaterade tjänster

Myndigheterna betalar årligen 411 miljoner kronor till andra myndigheter för olika it-relaterade tjänster, dvs. till de som tillhandahåller samordnad it-drift. Det framgår av beskrivningarna i enkätsvaren att det är mer än bara it-drift som omfattas av överenskommelserna mellan myndigheter. I vissa fall är det frågan om att en större myndighet har ett helhetsåtagande avseende en mindre myndighets it. Flertalet myndigheter räknar SSC:s HR- och lönerelaterade tjänster som exempel på samordnad it-drift.

Tabell 4.24 Kostnader för samordnade it-tjänster

Myndighetens storlek	Antal svarande	Årliga genomsnittliga kostnader i tkr	
		Medel	Median
Små myndigheter (1–49)	8	1 557	548
Medelsmå myndigheter (50–199)	8	2 122	1 750
Medelstora myndigheter (200–499)	6	1 963	1 563
Stora myndigheter (500–)	12	30 851	14 600
Totalt	**34**	**12 101**	**1 647**

Källa: Enkätundersökning.

4.5.4 Kostnader för egen it-drift

Myndigheter med samhällsviktig verksamhet och ISK-myndigheter har högre kostnader förknippade med egen it-drift än andra myndigheter

Som vi redan konstaterat ovan finns ett visst samband mellan myndigheternas storlek och deras platsbundna och icke platsbundna kostnader. Som vi också konstaterat står ett antal myndigheter i respektive grupp för en större del av kostnaden. Genom att redovisa kostnaderna för egen drift (summan av platsbundna och icke platsbundna kostnader), för de myndigheter som har egna datacenter, går det att se att den genomsnittliga årliga kostnaden är högre för myndigheter som ska följa förordningen (2007:603) om intern styrning och kontroll (ISK) och de myndigheter som uppgett att de bedriver samhällsviktig verksamhet.

Tabell 4.25 Skillnad i kostnader för datacenter mellan myndigheter av olika storlek och typ av verksamhet

	Genomsnitt av icke platsbundna och platsbundna kostnader per år i (tkr)		
Myndighetens storlek	Alla myndigheter	ISK-myndigheter	Myndigheter med samhällsviktig verksamhet
Små myndigheter (1–49)	391	-	203
Medelsmå myndigheter (50–199)	1 905	4 314	3 009
Medelstora myndigheter (200–499)	2 403	4 314	3 832
Stora myndigheter (500–)	18 135	23 006	26 682
Totalt	**9 537**	**19 815**	**19 836**

Källa: Enkätundersökning.

Med andra ord har myndighetens storlek betydelse för dess kostnader förknippade med egna datacenter, men även typen av verksamhet är av stor betydelse. Sett till de totala kostnaderna för egna datacenter i staten utgör ISK-myndigheterna och de som bedriver samhällsviktig verksamhet 80 respektive 86 procent.

Ungefär 450 årsarbetskrafter arbetar med drift på myndigheternas datacenter

Av de myndigheter som uppger att de har egna datacenter uppger 98 att de sammanlagt lägger ungefär 450 årsarbetskrafter på driften av sina datacenter.

Tabell 4.26 Årsarbetskrafter som arbetar med drift i myndigheternas datacenter

Myndighetens storlek	Antal svarande	Årsarbetskrafter	
		Medel	Median
Små myndigheter (1–49)	10	0,8	0,6
Medelsmå myndigheter (50–199)	19	1,4	1
Medelstora myndigheter (200–499)	22	2,1	2
Stora myndigheter (500–)	47	7,8	4
Totalt	**98**	**4,6**	**2**

Källa: Enkätundersökning.

Flera myndigheter betonar samtidigt att de gjort grova uppskattningar eftersom de inte har personal som uteslutande arbetar med it-drift. Drift är ofta en av flera arbetsuppgifter för den personal som arbetar inom myndigheternas it-verksamhet. Antalet om 450 årsarbetskrafter kan jämföras med Statistiska centralbyråns (SCB) statistik över anställda i olika yrkesgrupper i staten där 390 var registrerade som it-driftstekniker 2019.[3] Det bör understrykas att det är rimligt att antalet anställda inom yrkeskategorin Driftstekniker, IT är lägre än antalet årsarbetskrafter eftersom den senare siffran dels innefattar arbetsinsatser från inhyrd personal, och att det sannolikt även finns anställda som utför it-driftsrelaterade uppgifter, men som inte kategoriseras som Driftstekniker, IT enligt SSYK-standarden.

[3] SCB, lönestrukturstatistik, statlig sektor 2019. https://www.scb.se/hitta-statistik/statistik-efter-amne/arbetsmarknad/loner-och-arbetskostnader/lonestrukturstatistik-statlig-sektor/.

Tabell 4.27 Antal anställda i staten inom it 2019

Enligt SSYK 2012

Yrke	Antal
1311 IT-chefer, nivå 1	170
1312 IT-chefer, nivå 2	630
2511 Systemanalytiker och IT-arkitekter m.fl.	640
2512 Mjukvaru- och systemutvecklare m.fl.	1 700
2513 Utvecklare inom spel och digitala media	410
2514 Systemtestare och testledare	1 300
2515 Systemförvaltare m.fl.	1 400
2516 IT-säkerhetsspecialister	280
2519 Övriga IT-specialister	1 900
3511 Drifttekniker, IT	390
3512 Supporttekniker, IT	780
3513 Systemadministratörer	530
3514 Nätverks- och systemtekniker m.fl.	580
Totalt	**10 710**

Källa: SCB.

Det bör även noteras att vår enkät gett ett väsentligen annorlunda svar jämfört med den enkät SSC genomförde år 2016 och som visade att 800 heltidsekvivalenter arbetar med drift och underhåll av datacenter i staten. Flera faktorer kan förklara skillnaden, bl.a. att SSC:s enkät hade något högre svarsfrekvens på den aktuella frågan men även att ett antal myndigheter, som svarat på båda enkäterna, uppgett högre siffror i SSC:s enkät än på motsvarande fråga i vår enkät. Om detta beror på att frågan tolkats annorlunda, eller om antalet årsarbetskrafter fokuserade på it-drift faktiskt minskat, har inte varit möjligt att klarlägga.

4.5.5 Myndigheternas totala kostnader för it-drift

Myndigheternas kostnader för it-drift uppgår till 2,1 miljarder kronor per år

För att ge en uppskattning av de totala kostnaderna för myndigheternas it-drift summeras här kostnaderna för myndigheternas datacenter (platsbundna och icke platsbundna kostnader), det myndig-

heterna betalar för IaaS- och PaaS-tjänster, samt för personal. Kostnaderna hos de 158 myndigheter som svarat på enkäten har även använts för att uppskatta kostnaderna för hela den statliga redovisningsorganisationen som omfattar 215 myndigheter. För de myndigheter som svarat på enkäten och för samtliga myndigheter i redovisningsorganisationen uppgick kostnader för it-drift till 1,4 respektive 2,1 miljarder kronor år 2019.

Tabell 4.28 Sammanräknade kostnader för it-drift

Kostnad	Miljoner kronor	
	Svarat på enkät (158 myndigheter)	Hela statliga redovisningsorganisationen (215 myndigheter)[4]
Datacenter (platsbundna och icke platsbundna kostnader)	936	1 369
MoIntjänster (IaaS och PaaS)	203	293
Lönekostnader[5]	219	439
Totalt	**1 433**	**2 101**

Källa: Enkätundersökning och egna beräkningar.

Den sammanräknade kostnaden för it-drift i staten kan jämföras med att SSC år 2016 uppskattade den samlade kostnaden för it-drift hos 111 myndigheter till 2,2 miljarder kronor. En bidragande orsak till skillnaderna är sannolikt de olika uppskattningarna av lönekostnader, vilket vi berört ovan.

Kostnaden för it-drift i staten kan även jämföras med statens samlade it-kostnader som Ekonomistyrningsverket (ESV) 2018 bedömde uppgick till mellan 25–30 miljarder kronor för år 2016.

Kostnader för samordnad it-drift inkluderas inte i beräkningarna ovan för att undvika dubbelräkning. Kostnader för SaaS-tjänster har inte heller inkluderats eftersom dessa typer av tjänster, utifrån vår definition, inte uteslutande kan betraktas som en typ av it-driftstjänst.

[4] Kostnader för hela statliga redovisningsorganisationen har uppskattats genom att justera upp kostnader baserat på kvoten mellan anställda på samtliga myndigheter och de som svarat på vår enkät för respektive storleksgrupp.
[5] Lönekostnader har uppskattats schablonmässigt med hjälp av myndigheternas uppgifter om årsarbetskrafter, antagande om fördelning om hälften inhyrd och hälften anställd personal, samt SCB:s lönestatistik för Driftstekniker, IT 2019 i staten (38 600 kronor).

För närliggande tjänster såsom it-arbetsplatser finns sedan tidigare uppskattningar från Digg av kostnader för it-arbetsplatser i staten.[6] Digg uppskattade i rapporten *Myndigheters digitala mognad och it-kostnader* (2019) den genomsnittliga kostnaden år 2018 till 7 000 kronor per it-arbetsplats och år. Med antagande om att det finns lika många it-arbetsplatser som anställda i staten uppgår denna kostnad till ytterligare ungefär 1,9 miljarder kronor om året. Detta bör dock ses som en mycket grov uppskattning då det finns betydande spridning i kostnader för it-arbetsplatser mellan olika myndigheter och då antalet it-arbetsplatser i praktiken inte heller är samma som antalet anställda.

4.5.6 Fallstudiemyndigheterna

Fallstudiemyndigheterna vittnar om att det inte finns något enhetligt sätt att följa upp it-kostnader i allmänhet som underlag för jämförelser mellan myndigheter, och i synnerhet inte för it-drift. Vidare beskriver de stora myndigheterna att de har mindre kontroll över de it-kostnader som uppstår ute i verksamheterna, jämfört med de centrala it-avdelningarnas kostnader.

- En stor myndighet beskriver att ökade lagringsbehov kommer att driva kostnader inom infrastruktur och it-drift. För it generellt är det däremot utvecklingskostnaderna som är störst, där lönekostnader är de största kostnaderna inom ramen för utveckling. It-arbetsplatser har över tid blivit något billigare då avskrivningstiden ökat.
- En annan stor myndighet skiljer mellan anläggnings- och verksamhetsnära it-lösningar, där myndigheten har relativt många verksamhetsnära it-lösningar som stödjer kärnprocesserna. För sina datacenter betalar man årligen cirka 80 och 30 miljoner kronor för inköp av hårdvara respektive för licenser och support.
- Det universitet som ingått i fallstudien har en decentraliserad organisation där en stor del av it-kostnaderna uppstår ute i verksamheten men räknas in till de centrala it-kostnaderna. Myndig-

[6] Baserat på Kammarkollegiets definition ”stationära och bärbara datorer (inklusive surfplattor som fungerar som arbetsplats) med bl.a. tillbehör, programvara, bakomliggande stödsystem och infrastruktur/plattformar som stöttar drift, support och service med mera.”

hetens centrala it-verksamhet kostar cirka 240 miljoner kronor om året, men det kan variera beroende på bl.a. konsultbehov. För it-driften är det framför allt infrastruktur som driver kostnaderna, dvs. utrustning och hårdvara. Däremot har universitetet lyckats sänka kostnaderna för it-arbetsplatser.

- En mellanstor myndighet har fokuserat mycket på effektivitet genom att förbättra hantering av avtal och licenser, bl.a. genom hjälp av licensmäklare. Det som driver it-driftskostnader på myndigheten bedöms vara inköp av hårdvara. För it generellt medför bl.a. krav på hög säkerhet i regel höga it-kostnader.
- En liten myndighet får all it tillhandahållen genom en överenskommelse med sin värdmyndighet. Inom ramen för denna överenskommelse ingår bl.a. it-arbetsplatser och vanligen förekommande kontorsstöd. Myndigheten betalar värdmyndigheten motsvarande tre procent av sina verksamhetskostnader för dessa leveranser.

Fallstudiemyndigheterna framhåller att de har stort fokus på säkerhet vilket kan ha lett till dyrare it-driftslösningar än vad som vore möjligt med lägre ställda säkerhetskrav.

4.6 Myndigheternas framtida behov av it-drift

4.6.1 Framtida behov

Myndigheterna har i enkäten fått beskriva hur de uppskattar sina behov av it-drift de kommande fem åren. Som utgångspunkt svarar många myndigheter att deras beskrivning förutsätter att deras uppdrag inte förändras och att de rättsliga förutsättningarna för att utkontraktera it-drift klarläggs. Flera myndigheter uppger även att de nyligen förnyat avtal för den it-drift de utkontrakterat och att deras framtida behov är samma som deras nutida. Några myndigheter lyfter fram utmaningar med kompetensförsörjning och ökat behov av specialister. Därtill ser flera myndigheter behov av större kapacitet till följd av ökat lagringsbehov, större transaktionsvolymer och högre krav på redundans och informationssäkerhet.

Som en konsekvens av trenden på marknaden mot att erbjuda allt mer mjukvara som tjänster, understryker många myndigheter att det finns behov av tydliga rättsliga förutsättningar för att kunna använda

molntjänster. Här skiljer sig beskrivningarna något mellan myndigheter, där vissa framhåller att behovet av drift i egen regi kommer att minska, till följd av ökad användning av molntjänster, medan vissa tillägger att behov av egna datacenter kommer bestå för den mest skyddsvärda informationen. En myndighet (50–199 anställda) beskriver det på följande sätt:

> X har sedan 2011 utkontrakterat större delen av sin IT-drift (serverdrift, klienthantering Windows, nätverksdrift) till en privat leverantör. Den utveckling som skett de senaste åren är en utveckling mot att nya tjänster upphandlas som webbaserade SaaS-tjänster, dels för att detta har visat sig vara mer kostnadseffektivt samtidigt som tjänsterna har blivit mer plattformsoberoende och gett en större nytta till verksamheten. Det naturliga steget vore för X att likt utvecklingen generellt även hantera IT-driften i molnbaserade verktyg som t.ex. Google Cloud, Microsoft Azure eller i en statlig modell. Dessa strategiska val skulle göra IT-driften mer kostnadseffektiv, säkrare och ge mer nytta till verksamheten jämfört med den typen av traditionell IT-drift som X har hos privat leverantör i dag. Vi tror att rätt väg att gå är att välja lätthanterade och användarvänliga tjänster och undvika sådana system som kräver omfattande konsultinsatser. X kommer sannolikt i framtiden att behöva extern hjälp med expertis inom serverdrift och nätverksdrift, samt utveckling och integration av olika verksamhetssystem. Diskussionerna kring de amerikanska molntjänsterna följs aktivt då den typen av tjänster är intressanta för myndigheter och organisationer motsvarande X verksamhet, förutsatt att de kan bedömas följa lagar, förordningar och säkerhetskrav. Behovet av att ansluta sig till en samordnad IT-drift upplevs därför inte som stora om den data och information X hanterar klassas som säker att hantera hos de amerikanska molntjänsterna, men i annat fall skulle en samordnad statlig IT-drift kunna ta över de tjänster som för närvarande köps från privata leverantörer förutsatt att den är kostnadseffektivare och har lika hög kompetens och resurser inom området.

Bilden nyanseras av myndigheter som har tillräckliga resurser för att kunna drifta lösningar kostnadseffektivt på egen hand.

> Vi ser att andelen IaaS går ner en del då flera systemleverantörer gärna vill sälja sina programvaror som PaaS eller SaaS. Vi ser dock inte uppenbara fördelar med detta då totalkostnaden jämfört med att köpa systemen separat och drifta dem inom ramen för vårt IT-driftsavtal ofta är högre. Detta beror delvis på att vi har en relativt hög fast andel i vårt IT-driftsavtal vilket gör att rörlig kostnad för att drifta ett nytt system blir relativt låg.

Flera myndigheter framhåller behov av att fortsatt kunna utkontraktera drift, både av system där det finns möjlighet att sköta driften i egen regi men där det finns andra skäl att inte göra det, och i de fall där vissa funktioner endast går att erhålla som tjänst genom en extern driftsleverantör. Driftsmiljön är komplex på de flesta myndigheter i bemärkelsen att olika system från olika leverantörer är integrerade mot varandra. En liten myndighet beskriver situationen på följande sätt:

> Myndighetens verksamhetskritiska system kommer troligtvis även i framtiden att bestå av en mix av tjänster och produkter från den konkurrensutsatta marknaden, tjänster och produkter som endast en specifik aktör tillhandahåller respektive egenutvecklade applikationer.

På en övergripande nivå betonar flera myndigheter att den framtida it-driften kommer ställa högre krav på flexibilitet, skalbarhet och tillgänglighet. Det finns t.ex. ett växande behov att tillgängliggöra data till olika intressenter, samarbeta med externa parter både nationellt och internationellt och att snabbt kunna ställa om verksamheter vid förändrade förutsättningar.

4.6.2 Samordnad it-drift

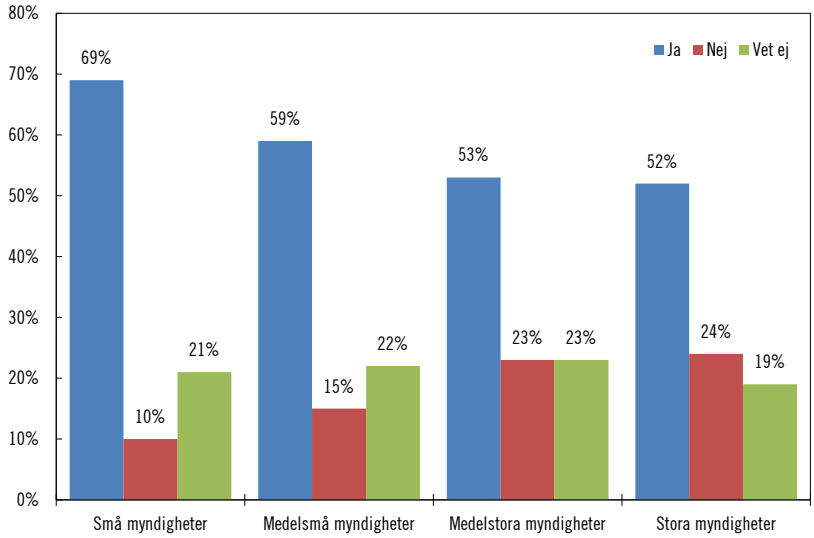
Vi har också ställt frågor om myndigheternas intresse och behov av att ansluta sig till en samordnad statlig it-drift. Frågorna har varit hypotetisk formulerade eftersom eventuella förslag om hur en samordnad it-drift bör utformas kvarstår att utreda. Svaren ger dock en bild på övergripande nivå över vilka funktioner myndigheter har intresse att överlåta och deras attityd till samordnad it-drift. Av myndigheternas svar har det bl.a. framgått att många ser en samordnad statlig it-drift som ett komplement till den egna it-driften snarare än ett substitut. Flera myndigheter uttrycker även oro för att ökad samordning och standardisering kan leda till oflexibla och dyra lösningar som inte tar hänsyn till verksamheters olika behov och att myndigheterna riskerar att förlora kontroll över kritiska it-lösningar.

Över hälften av myndigheterna är intresserade av att ansluta sig till en samordnad statlig it-drift

Enkätsvaren visar att över hälften (57 procent) av myndigheterna är intresserade av att ansluta sig till en samordnad statlig it-drift. Det finns ett visst samband mellan storlek på myndighet och intresse, då mindre myndigheter i större utsträckning är intresserade av att ansluta sig. Omvänt är större myndigheter mindre intresserade av att ansluta sig och ungefär en fjärdedel av de stora myndigheterna uppger att de inte är intresserade.

Figur 4.7 **Har myndigheten intresse/behov av att i framtiden ansluta sig till en samordnad statlig it-drift?**

Andel av myndigheter utifrån storlek

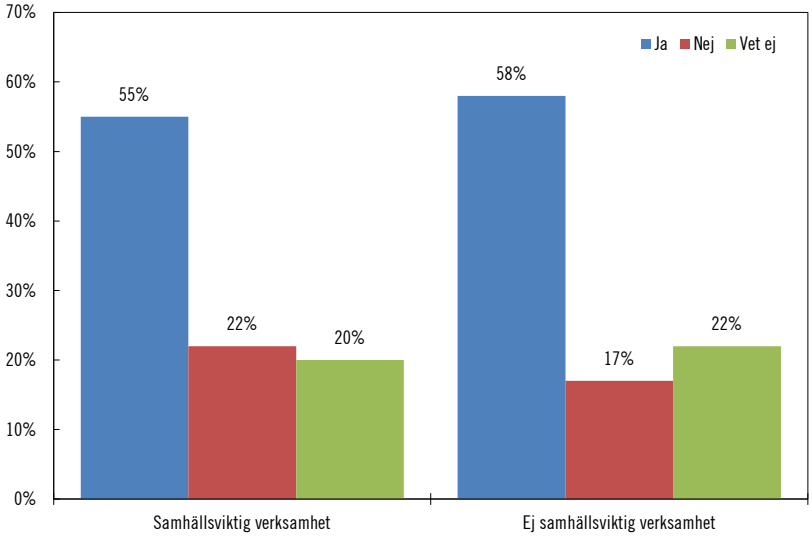


Källa: Enkätundersökning.

Bland de myndigheter som svarat att de inte är intresserade av att ansluta sig till en samordnad statlig it-drift är flera lärosäten eller större myndigheter som har uppgett att de har tillräcklig skala och kompetens för att sköta it-driften på ett effektivt sätt själva.

Figur 4.8 Har myndigheten intresse/behov av att i framtiden ansluta sig till en samordnad statlig it-drift?

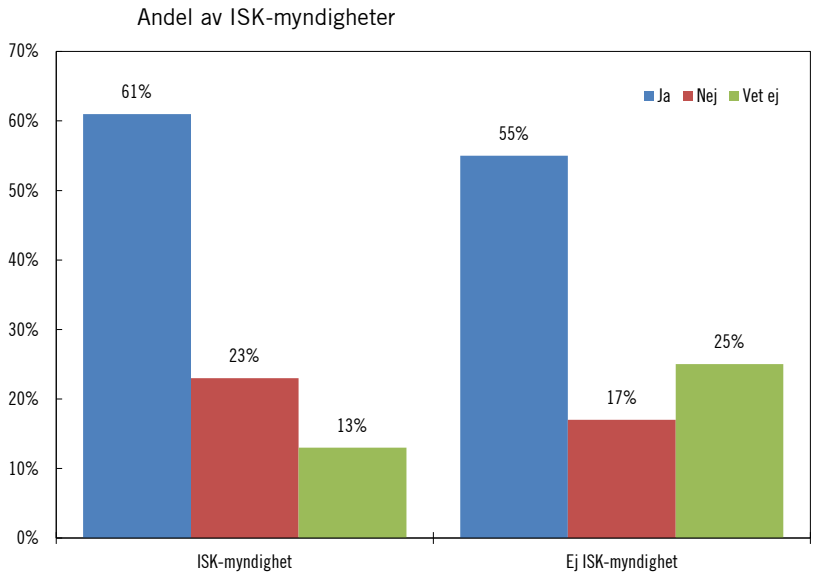
Andel av myndigheter som bedriver samhällsviktig verksamhet



Källa: Enkätundersökning.

Det förefaller inte finnas något tydligt samband mellan intresse av att ansluta sig till en samordnad statlig it-drift och om myndigheten omfattas av förordningen (2007:603) om intern styrning och kontroll (ISK) eller bedriver samhällsviktig verksamhet.

Figur 4.9 Har myndigheten intresse/behov av att i framtiden ansluta sig till en samordnad statlig it-drift?



Källa: Enkätundersökning.

Som skäl att vilja ansluta sig uppger myndigheterna möjligheten att realisera kostnadsbesparingar, förbättra säkerheten och förenkla den digitala samverkan, i nästan lika stor utsträckning.

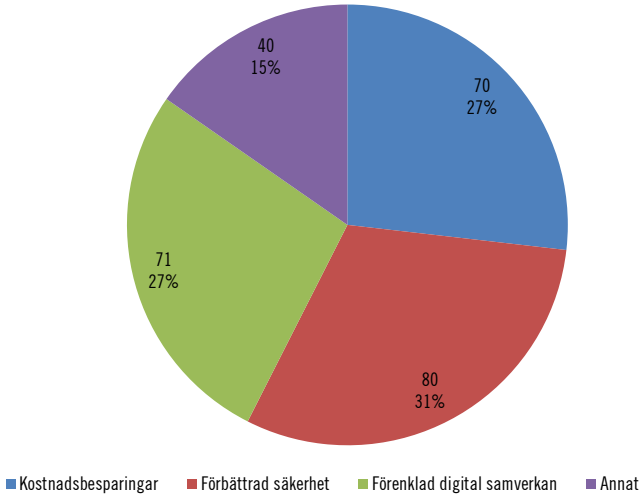
Tillgång till relevant kompetens är utöver kostnader, säkerhet och samverkan ett viktigt skäl till att vilja ansluta sig till samordnad it-drift,

Många myndigheter uppger att de har svårt att rekrytera eller få tillgång till relevant kompetens inom it-drift. Vidare framhåller ett antal myndigheter även att det vore effektivt för staten som helhet att samordna och koncentrera kompetens inom området, samt att en samordnad it-drift skulle innebära minskad administration förknippad med upphandling.

Ett annat återkommande tema är att samordnad it-drift kan höja robustheten om den möjliggör säkerhetskopiering och ökad redundans.

Figur 4.10 Vilka är de huvudsakliga skälen för intresse/behov att ansluta sig till en samordnad statlig it-drift?

Antal gånger skäl uppgetts (flervalsfråga) och andel av total



Källa: Enkätundersökning.

Myndigheterna är intresserade av ett helhetsåtagande, av serverdrift och av administrativa tjänster

Myndigheterna har själva fått formulera vilka funktioner de är intresserade av att överlåta vid en samordnad statlig it-drift. Svaren bör ses i ljuset av att myndigheterna inte haft information om villkoren för anslutning, finansiering eller utformning. Det finns dock några återkommande teman och svaren ger en viss bild av myndigheternas behov.

Av de 57 procent av myndigheterna som svarat att de är intresserade eller har behov av att ansluta sig till en samordnad it-drift uppger en fjärdedel att de önskar ett helhetsåtagande för it-drift. Det framgår indirekt av svaren att flera myndigheter ser helhetsåtagandet som mer omfattande än endast it-drift. Exempelvis önskar flera myndigheter att närliggande tjänster såsom it-arbetsplatser och telefoni skulle kunna överlåtas. Detsamma gäller annan verksamhet än drift såsom support, förvaltning och utveckling. I övrigt uttrycks intresse för flera andra områden:

- Flera myndigheter uttrycker intresse för serverdrift och IaaS.
- Flera myndigheter uttrycker intresse för samordnad säkerhetskopiering, backup- eller lagringslösningar.
- Flera myndigheter uttrycker intresse för administrativa tjänster och kontorsstöd exempelvis e-arkiv, diarium, ärendehantering, webbplats, e-post och Office-paketet.
- Ett antal myndigheter uttrycker intresse för samlokalisering eller drift av datacenter.
- Ett antal myndigheter uttrycker behov av samordnade containertjänster.

Av svaren framgår att mindre myndigheter i större utsträckning än större myndigheter är intresserade av helhetsåtaganden. Vidare framför flera myndigheter att en eventuell samordnad statlig it-drift bör fokusera på system och tjänster av administrativ och standardiserad karaktär där det går att uppnå skalfördelar. Ett antal myndigheter är även tydliga med att det endast är relevant att ansluta sig till en samordnad it-drift om det medför en minskad kostnad och bibehållen informationssäkerhet.

25 myndigheter uttrycker intresse för att erbjuda it-drift

Nästan 16 procent (25) av myndigheterna uttrycker intresse för att erbjuda it-drift till andra myndigheter. Bland dessa är de allra flesta stora eller medelstora myndigheter och flera hanterar redan i dag viss it-drift åt andra myndigheter såsom Skatteverket, Försäkringskassan och Länsstyrelsen i Västra Götalands län. Det är samtidigt 13 myndigheter som uppgett att de är intresserade av att erbjuda it-drift som i dag inte gör det. Flera myndigheter, huvudsakligen lärosäten, som har möjlighet att erbjuda it-drifttjänster uppger att det främst är relevant gentemot den egna sektorn. På frågan vilka funktioner dessa myndigheter har möjlighet att erbjuda uppges huvudsakligen samlokalisering och infrastrukturtjänster såsom IaaS och PaaS.

För att tillhandahålla it-drift uppger de 25 myndigheterna att det krävs ett utpekat ansvar från regeringen (i instruktion eller genom uppdrag), klarlagda rättsliga förutsättningar för denna typ av sam-

verkan inom statsförvaltningen, ytterligare ekonomiska resurser och tid för att bygga upp förmågan.

4.6.3 Fallstudiemyndigheterna

Flera fallstudiemyndigheter ser ökade behov av it-säkerhetsspecialister och att arbeta strukturerat med informationsklassificering. Flera understryker även fortsatta behov av att kunna använda kommersiella molntjänster där det är möjligt och ändamålsenligt.

- En liten myndighet vill i fortsättningen ha möjlighet att kunna använda molntjänster i större utsträckning och att skydda känsliga personuppgifter genom drift i statlig regi. För att möta det sistnämnda behovet har myndigheten inlett en dialog med Försäkringskassan om ett helhetsåtagande för it.
- Universitetet håller på att slutföra en större organisatorisk förändring av sin förvaltningsgemensamma it-verksamhet och säger bl.a. att högre krav på säkerhet kommer ha stor betydelse för it-driftslösningar framöver. Universitetet vill även fortsatt tillhandahålla molntjänster till andra lärosäten och geografiskt närbelägna myndigheter.
- En stor myndighet bedömer att kapacitetsbehovet inom it-drift kommer ligga kvar eller öka något de kommande åren. Inom verksamheten kommer ökade behov av automatisering och tillgänglighet ställa krav på it-driften. Även säkerhetsskyddslagen har sedan den trätt i kraft medfört stora konsekvenser för kärnverksamheten och it, vilket innebär stora kostnader.
- En annan stor myndighet ser generellt ökade krav på automatisering, lagring och redundans. Myndigheten ser även specifika behov av molnbaserade samarbetslösningar.

Beträffande möjligheterna till en samordnad statlig it-drift uttrycker sig fallstudiemyndigheterna försiktigt positivt. De framhåller att det finns flera villkor som måste uppfyllas för att det ska vara intressant. En myndighet understryker betydelsen av att den har rådighet över verksamhetsnära it-system och att det inte är lämpligt att sådana system hanteras av en annan myndighet. Flera aktörer är redan i

dagsläget involverade i leveransen av dessa system och myndigheten betonar att färre involverade leder till ökad kontroll och säkerhet.

4.7 Analys och slutsatser

It-drift inom den statliga förvaltningen har under de senaste åren gått från att vara en teknisk fråga för en myndighets it-avdelning till att bli en strategisk fråga för myndigheten. Det finns flera faktorer som ligger bakom detta, som ökade krav på digitalisering, ett större fokus på data- och säkerhetsskydd generellt men också enskilda myndighetsexempel som visat på behovet av att balansera både kostnadseffektivitet och säkerhet i valet av it-driftslösningar. Utkontraktering av it-drift och användning av molntjänster har också ställts mot nya hotbilder och ökade krav på dataskydd och säkerhet.

Statliga myndigheter har krav på sig att välja kostnadseffektiva lösningar i sin verksamhet. Kraven på säkerhet påverkas av en myndighets verksamhet och tillämpliga verksamhetskrav samt vilken typ av uppgifter som myndigheten hanterar. Samhällskritisk verksamhet och myndigheter som hanterar särskilt skyddsvärda uppgifter har störst behov av säkra it-driftslösningar. Men även myndigheter som hanterar olika typer av sekretessreglerade uppgifter eller känsliga personuppgifter måste göra säkerhetsavvägningar för sin it-drift. Balansen mellan säkerhet och kostnadseffektivitet är inte alltid enkel att hitta. Ett systematiskt informationssäkerhetsarbete och informationsklassificering är grunden för att kunna göra rätt avvägningar.

Verksamhet och informationshantering påverkar myndigheters behov av it-drift

Vår kartläggning visar att de allra flesta myndigheter (90 procent) som besvarat vår enkät hanterar någon form av skyddsvärd information i sin verksamhet. Även om enkäten inte ger svar på omfattningen av skyddsvärd information i respektive myndighet så är det tydligt att så gott som samtliga myndigheter har att ta ställning till olika grad av säkerhetsaspekter i valet av it-driftslösningar. Vanligast är att myndigheter hanterar olika typer av känsliga personuppgifter eller uppgifter som regleras av sekretess med rakt skaderekvisit. 40 procent av myndigheterna hanterar säkerhetsskyddsklassificerade

uppgifter. Större myndigheter hanterar i högre grad säkerhetsskyddsklassificerade uppgifter än vad mindre myndigheter gör. Det är dock viktigt att poängtera att det inte är faktorer som myndighetsstorlek som påverkar säkerhetskraven, utan snarare verksamhetens karaktär och vilken typ av uppgifter som myndigheten hanterar. Även mindre myndigheter bedriver samhällsviktig verksamhet och hanterar uppgifter som ställer höga krav på säkra it-driftslösningar. Detta bekräftas också i våra fallstudier.

Myndigheterna behöver fortsätta att utveckla sitt systematiska informationssäkerhetsarbete

Att ha kunskap om vilka uppgifter myndigheten hanterar och vilka krav som ställs på uppgiftshanteringen är viktigt för att kunna göra rätt avvägningar när det gäller it-drift. Informationsklassificering som en del i ett systematiskt informationssäkerhetsarbete är av central betydelse. Vår enkätundersökning visar att ungefär hälften av myndigheterna bedömer att de arbetar med informationssäkerhet och har genomfört informationsklassning i hela eller delar av verksamheten. Hälften av myndigheterna har påbörjat ett informationssäkerhetsarbete på myndigheten men har inte klassat sin information. Ett fåtal myndigheter har inte gjort något alls på området. Denna bild bekräftas av Digg:s kartläggning från 2019. Små och medelsmå myndigheter har i regel inte kommit lika långt i sitt informationssäkerhetsarbete som medelstora och stora myndigheter.

Att säkerställa informationssäkerhetskrav i samband med it-upphandling är också viktigt för en säker it-drift. Drygt hälften av myndigheterna i enkätundersökningen har påbörjat ett arbete med säkerhetskrav i olika skeden av en it-upphandling. Var femte myndighet har ett etablerat arbetssätt för att verifiera säkerhetskrav hela vägen – från kravkatalog och verifiering av säkerhetskrav i anbudssvar och leverans till att följa upp säkerhetskraven under avtalets gång. En ungefär lika stor andel av myndigheterna har inte reflekterat över frågan. Även här framkommer att större myndigheter har kommit längre i sitt arbete än mindre myndigheter. Det får anses naturligt eftersom större myndigheter gör fler och större upphandlingar och därmed behöver ha rutiner för detta på plats. Flera stora myndigheter behöver dock utveckla sitt arbete med att verifiera säkerhetskraven under avtalets giltighetstid.

Det återstår med andra ord en del arbete med att få informationssäkerheten på plats bland de statliga myndigheterna som grund för säkra it-driftslösningar. MSB:s nya föreskrifter på området stärker kraven, men det saknas sanktioner om en myndighet inte genomför systematiska informationssäkerhetsåtgärder. Det finns inte heller någon tillsynsmyndighet på området.

Kompetensbrist är en riskfaktor för säker it-drift

Enkätundersökningen visar att såväl stora som små myndigheter ser bristande informationsklassificering och avsaknad av relevant kompetens som de största hindren för säker it-drift. Kompetensfrågan lyfts fram som en orsak till brister i informationsklassificeringen, men är ett mer generellt problem. Myndigheterna saknar kompetens inom både it och säkerhet och beställarkompetens lyfts fram som ett särskilt problem. För små myndigheter är kompetensbristen i mångt och mycket en resursfråga, medan det för stora myndigheter handlar om hård konkurrens om kunnig och erfaren personal. Det kan vara svårt att ersättningsrekrytera när nyckelpersoner slutar. Detta bekräftas också av fallstudiemyndigheterna. För att kunna översätta lagkrav och informationsklassificering till konkreta krav på säker och kostnadseffektiv it-drift måste olika kompetenser i verksamheten dessutom samverka och förstå varandra. Flera myndigheter pekar på att det är en utmaning. Ett oklart rättsläge vad gäller användning av molntjänster bidrar ytterligare till svårigheterna. Sammantaget framstår kompetensbristen som en stor riskfaktor för säker it-drift i myndigheterna.

Höga krav på säkerhet och inlåsningseffekter utgör hinder mot kostnadseffektiv it-drift

De största hindren för kostnadseffektiv it-drift är enligt enkätundersökningen höga krav på säkerhet och olika typer av inlåsningseffekter. Myndigheterna beskriver det som att säkerhetskrav utöver standard är dyrare och att det därför är viktigt att kunna kravställa på rätt säkerhetsnivå. Särskilt större myndigheter framhåller detta. För små myndigheter är kompetensfaktorn viktig även här. Hinder i form av inlåsningseffekter (t.ex. leverantörsberoende) kan ta sig olika uttryck.

Flera myndigheter lyfter fram att de sitter fast i enskilda privata tjänsteleverantörers lösningar och att de har investerat i såväl kompetens som licenser som är kopplade till leverantören. Byte av tjänsteleverantör kan i sig vara både komplext och kostsamt. Är en myndighet nöjd med den befintliga lösningen kan det ta emot att genomföra ett omfattande arbete för att hitta en ny leverantör. Oavsett situation så ställs även här krav på förmåga att kravställa och på beställarkompetens.

Myndigheterna har likartade behov av it-driftslösningar för grundläggande funktioner

Enkätundersökningen och fallstudierna visar både på olikheter och likheter mellan myndigheternas it-miljöer och deras behov. Även om specifika lösningar och system skiljer sig åt mellan statliga verksamheter är deras behov på en övergripande nivå förhållandevis lika. Många myndigheter behöver, utöver it-arbetsplatser till sina medarbetare, it-drift av olika system och applikationer för sina verksamheter. Dessa system och applikationer kan i sin tur delas in utifrån målgrupp i de som är ämnade för internt bruk alternativt externt (i de fall målgruppen är enskilda eller andra myndigheter). Vidare finns det oftast integrationer mellan system som gör att de kan utbyta information.

För att möta behoven har många myndigheter en blandning av it-drift de själva hanterar (dvs. drift där myndigheten själv äger hårdvara och mjukvara) och drift de utkontrakterat till en privat tjänsteleverantör eller samordnat med annan myndighet (dvs. it-drift som tjänst). Faktorer som påverkar myndigheters val av driftsform är enligt fallstudierna

- myndighetens uppfattning om vilka krav som uppställs i olika regelverk (dataskydd, sekretess, säkerhetsskydd, etc.) på uppgiftshanteringen och i vilken utsträckning dessa krav uppfylls vid anlitandet av en privat tjänsteleverantör,
- om myndigheten har tillgång till nödvändig kompetens för att själva hantera driften av en specifik funktion,

– marknadens utbud och villkor för de system och applikationer myndigheten har behov av (exempelvis om de säljs som licens eller enbart som tjänst), och
– om det finns kostnadsmässiga fördelar med en driftsform framför en annan.

Av intervjuerna med fallstudiemyndigheterna framgår att även mer praktiska omständigheter kan vara styrande. Det kan t.ex. vara möjligheten att samordna sig med en annan myndighet eller om en driftsform gör att det går snabbare att implementera en ny funktion.

Myndigheterna kommer även fortsättningsvis ha visst behov av drift i egen regi

För de två tredjedelar av myndigheter som har egna datacenter bör enkätresultatet ses i ljuset av hur myndigheternas it-verksamhet växt fram över tid. Historiskt har det varit nödvändigt för många myndigheter att ha en egen it-driftsmiljö varför de inrättat utrymmen i sina egna lokaler för servrar och annan hårdvara. I takt med förvaltningens digitalisering har vissa myndigheter med större kapacitetsbehov etablerat egna datacenter eller upphandlat samlokalisering. Sammantaget har de myndigheter som svarat på vår enkät 220 datacenter vilket kan jämföras med 206 när SSC ställde en liknande fråga i sin enkätundersökning från 2016. Även om det finns viss effektiviseringspotential i att konsolidera lokalanvändningen för datacenter i statsförvaltningen är det viktigt att notera att en del av utrymmen för servrar och hårdvara ingår i myndigheternas lokaler på ett sätt som kan göra dem svåra att rationalisera bort med mindre än att hyreskontrakt omförhandlas. Några av fallstudiemyndigheterna framhåller dock att de övergått till samlokalisering eftersom de bedömt att det varken är nödvändigt eller effektivt att ha egna datacenter. Även om det är möjligt att antalet serverutrymmen och mindre datacenter i statsförvaltningen på sikt kommer minska som en konsekvens av effektiviseringstryck och större möjligheter till utkontraktering framgår det att myndigheter även i fortsättningen har behov av it-drift i egen regi.

Enligt myndigheterna beror det på att

- behovet av kontroll över de uppgifter som behandlas, eller den funktion som tillhandahålls, är så stort att det är mest praktiskt att hantera driften i egna lokaler och på egen utrustning,
- myndigheten inte har klassificerat eller separerat sin data i tillräcklig utsträckning för att det ska vara utan risk eller ens möjligt att utkontraktera driften,
- myndigheten har en teknikskuld (legacy) i form av gamla system och applikationer (eller integrationer mot sådana) som gör det svårt att migrera till extern drift, och
- myndigheten är tillräckligt stor och har tillräckligt förutsägbara kapacitetsbehov för att kunna producera sin drift själv på ett kostnadseffektivt sätt.

Myndigheternas användning av molntjänster från privata tjänsteleverantörer är utbredd och drift i egen regi är inte alltid ett alternativ

När det gäller kommersiella molntjänster är användningen inom statsförvaltningen i dag utbredd. Vanligast är SaaS-tjänster följt av IaaS- och PaaS-tjänster. Pensionsmyndigheten genomförde år 2015 en enkät där 30, 23 och 78 procent av respondenterna uppgav att de använde IaaS, PaaS respektive SaaS-tjänster. Det förefaller därmed som att användningen av PaaS- och SaaS-tjänster ökat något enligt vår enkät där motsvarande andel användare av IaaS-, PaaS- och SaaS-tjänster är 33, 32 respektive 95 procent. Jämförelse bör göras med viss försiktighet givet att inte exakt samma myndigheter svarat på enkäterna även om båda enkäterna haft hög svarsfrekvens. Från enkätresultaten framgår att myndigheterna använder SaaS-tjänster till många olika funktioner och ändamål. Som vi nämnt ovan finns även tecken på att andelen myndigheter som använder någon slags SaaS-tjänst ökat över tid. Användningen av SaaS-tjänster har potential att påverka dynamiken mellan verksamheter och it-avdelningar på myndigheter i den utsträckning verksamheterna själva kan upphandla de verktyg och stöd de behöver utan att involvera sina it-avdelningar. Denna möjlighet gör att verksamheter på ett flexibelt sätt kan introducera nya it-stöd för medarbetare utan längre ledtider. Men den kan

även skapa utmaningar i de fall det blir svårare att samordna kravställning och förvaltning av de många it-lösningar verksamheterna använder.

Det framgår av enkätundersökningen och från intervjuerna med fallstudiemyndigheterna att många myndigheter både bedriver it-drift i egen regi och använder kommersiella molntjänster för att tillhandahålla nödvändig it-drift till sina verksamheter. Utkontrakterad it-drift inklusive molntjänster bör därmed inte alltid betraktas som ett likvärdigt och utbytbart alternativ till it-drift i egen regi. Om dessa driftsformer kan ses som likvärdiga alternativ till varandra eller inte beror i slutändan på om myndigheten i fråga har samma möjlighet att välja endera för att möta ett specifikt behov. I praktiken finns det ofta hinder som omöjliggör någon driftsform, t.ex. att den mjukvara som krävs för en viss funktion endast säljs som SaaS-tjänst, eller att det saknas resurser eller kompetens på myndigheten för att sköta driften i egen regi. Sekretess eller säkerhetsskydd kan också ställa krav som gör det olämpligt att använda vissa kommersiella molntjänster. Sett till respektive driftsform finns det oftast många olika sätt att möta samma behov och det är därför viktigt att poängtera att alla dessa sätt är förknippade med myndigheternas egna avvägningar avseende säkerhet, kostnad och funktion. Det innebär sammanfattningsvis att myndigheter tar hänsyn både till de hinder som nämns ovan (bland annat säkerhet), samt gör avvägningar avseende kostnad och funktion, vid val av driftsform och den specifika it-driftslösningen.

Samordningen av it-drift inom statsförvaltningen har vuxit fram successivt och ser ut på många olika sätt

Beträffande samordningen av it-drift inom statsförvaltningen tyder både enkätresultatet och fallstudierna på att det är relativt vanligt att myndigheter får eller tillhandahåller it-tjänster av eller till varandra. Det handlar om allt från att tillhandahålla driften av en specifik tjänst eller applikation, till att tillhandahålla samtliga funktioner hos en normal it-avdelning åt en annan myndighet. Ofta har dessa samarbeten mellan myndigheter vuxit fram successivt utan formell styrning på departementsnivå. I vissa fall förekommer dock formell styrning, som exempelvis i fallet med Försäkringskassans uppdrag att tillhandahålla säker och samordnad it-drift, samt i fallet med SSC:s HR- och ekonomirelaterade tjänster. Den decentraliserade förvaltnings-

modellen har gett myndigheterna möjlighet att själva etablera samarbeten om it-drift utifrån sina behov. Denna situation skapar förutsättningar, åtminstone i teorin, för myndigheter att gå in i och ut ur samarbeten på ett flexibelt sätt. Samtidigt har det genom fallstudierna framkommit att vissa myndigheter som köper it-tjänster från andra myndigheter ibland upplever det som svårt att få inflytande över valet av it-lösningar och hur dessa utformas. En komplicerande omständighet i sammanhanget är att det råder osäkerhet avseende vad myndigheterna kan och bör reglera i de överenskommelser de ingår sinsemellan. Vi återkommer till denna fråga i vårt slutbetänkande.

Myndigheter med samhällsviktig verksamhet har högre kostnader för it-drift än andra myndigheter

Kostnaderna för it-drift avseende egna datacenter är ojämnt fördelade mellan myndigheterna i statsförvaltningen. Ett antal myndigheter har högre kostnader, både för drift i egen regi och för vissa molntjänster. Det finns ett visst samband mellan myndigheternas storlek och kostnader för it-drift. Den ojämna fördelningen av kostnader syns dock även om man ser till myndighetsstorlek (antal anställda). En gemensam faktor för flera av de myndigheter som har höga kostnader (relativt sin storlek) är att de bedriver samhällsviktig verksamhet eller har att tillämpa förordningen (2007:603) om intern styrning och kontroll (ISK). Sett till de totala kostnaderna för egna datacenter utgör ISK-myndigheterna och de som bedriver samhällsviktig verksamhet 80 respektive 86 procent. Dessa myndigheter står även för en majoritet av de totala it-kostnaderna, baserat på Digg:s sammanställning om strategiska it-projekt, it-kostnader och mognad. Detta tyder på att dessa två grupper av myndigheter har it-verksamhet som generellt är mer kostsam. För myndigheter som bedriver samhällsviktig verksamhet är det rimligt att den information och de system som myndigheterna förvaltar ställer högre krav på informationssäkerhet än för myndigheter som inte bedriver samhällsviktig verksamhet. Exempelvis är en påverkande faktor för flera bevakningsmyndigheter att man ska kunna utöva sin verksamhet under störda förhållanden eller höjd beredskap, vilket påverkar konstruktion och kostnader för it-driften. Vidare är de flesta ISK-myndigheter relativt stora och hanterar många transaktioner. Ett av de

kriterier som tillämpats för att avgöra om en myndighet ska omfattas av förordningen (2007:603) om intern styrning och kontroll är att verksamheten har omfattande och komplexa it-system.

Sett till hela den statliga redovisningsorganisationen om 215 myndigheter uppskattas kostnaderna för it-drift år 2019 uppgå till motsvarande 2,1 miljarder kronor. En betydande andel av denna kostnad utgörs av kostnader för egna datacenter (cirka 65 procent), medan molntjänster utgör 14 procent och kostnader för inhyrd och anställd personal 21 procent. Kostnaden för it-drift bör ställas i relation till statens samlade kostnader för it, som 2016 uppskattades till mellan 25–30 miljarder kronor av Ekonomistyrningsverket. Sett till statens samlade kostnader för it är det inte osannolikt att lönekostnaderna utgör en betydande andel. Sett till SCB:s statistik fanns det nästan 11 000 anställda år 2019 i it-relaterade yrken. En schablonmässig uppskattning av lönekostnaderna för dessa uppgår till cirka 7,3 miljarder kronor.

Flera faktorer påverkar myndigheternas framtida it-drift

Flera myndigheter i enkätundersökningen och i fallstudien betonar att de i framtiden kommer att ha större behov av flexibilitet, skalbarhet och tillgänglighet. Det finns t.ex. ett växande behov att tillgängliggöra data till olika intressenter, samarbeta med externa parter både nationellt och internationellt och att snabbt kunna ställa om verksamheter vid förändrade förutsättningar. Flera myndigheter framhåller även behov av att i fortsättningen både kunna utkontraktera drift och bedriva drift i egen regi. Verksamhetskritiska system kommer sannolikt även i framtiden bestå av tjänster och produkter från den konkurrensutsatta marknaden, tjänster och produkter som endast en specifik aktör tillhandahåller och egenutvecklade applikationer. Det ska tilläggas att ett antal myndigheter uppgett att de kommer att ha samma behov som i dag, givet att deras uppdrag inte förändras.

Det finns ett antal faktorer som kan tänkas påverka myndigheternas it-drift inom en nära framtid, däribland den tekniska utvecklingen, arbetssätt och kompetens samt styrning. Den tekniska utvecklingen avseende hård- och mjukvara har ur ett längre tidsperspektiv möjliggjort digitaliseringen av allt fler funktioner i den offentliga förvaltningen. Många verksamheter har genom digitaliseringen auto-

matiserats och effektiviserats, vilket gjort det möjligt att höja deras produktivitet och kvalitet. Det är samtidigt viktigt att notera att nya tjänster och produkter på it-området inte utan vidare medför lägre kostnader på kort sikt för offentliga verksamheter, i relation till andra kostnader. Det finns flera tänkbara skäl till detta, bl.a. att den tekniska utvecklingen ofta sker jämsides med växande förväntningar på vad som ska uträttas. Många verksamheter har dessutom en tekniskuld eller föråldrad it-arkitektur, som kan göra det svårt att snabbt ersätta gammal ineffektiv teknik med ny effektiv. Slutligen kan den tekniska utvecklingen också skapa nya kostnader, genom att t.ex. rubba balansen mellan offensiva och defensiva förmågor inom cybersäkerhet, vilket kan leda till ökade kostnader för verksamheter för att försvara sig mot angrepp och hot. Vissa tekniktrender har, om de extrapoleras, även fortsatt potential att påverka myndigheternas it-drift. Däribland den generella trenden mot att allt mer hård- och mjukvara paketeras och säljs som tjänster över internet, att ett fåtal dominerande plattformsföretag har en dominerande ställning på marknaden för molntjänster, samt att vissa kritiska byggstenar i den mjuka infrastrukturen fortsätter vara öppen källkod och utvecklas i en gynnsam riktning.

Utöver teknikutvecklingen är även arbetssätt och kompetenser på it-området en faktor som kommer att påverka myndigheternas framtida it-drift. Nya arbetssätt och relevanta kompetenser hänger förstås nära ihop med den tekniska utvecklingen. Exempelvis har ett antal innovationer som underlättat digitalt samarbete och att snabbt gå mellan utveckling till produktion, banat väg för nya metoder och arbetssätt inom systemutveckling. Dessa trender har inneburit att gamla gränser mellan drift, förvaltning och utveckling delvis har suddats ut. De nya arbetssätten och den snabba teknikutvecklingen ställer som följd nya krav på vad som anses vara aktuella och relevanta kompetenser hos it-specialister. Olika verksamheters förutsättningar att attrahera dessa kompetenser blir därmed av stor betydelse för om de kan anamma nya arbetssätt och tekniker. Mer generellt, och som en konsekvens av samhällets digitalisering, ökar även kraven på it-kompetens hos roller i organisationer som traditionellt inte haft det. Det kan t.ex. handla om relevant kompetens att ställa krav vid upphandling och utformning av system och applikationer – det som ibland benämns som beställarkompetens. Vår kartläggning har visat att många myndigheter ser kompetensbrist, och då särskilt

bristande beställarkompetens, som ett hinder och en riskfaktor för säker och kostnadseffektiv it-drift.

Slutligen är styrningen av myndigheterna, inklusive myndigheternas rättsliga förutsättningar att utkontraktera it-verksamhet, en faktor med stor påverkan på statsförvaltningens framtida it-drift. På denna punkt kan vi konstatera att det både funnits ökade förväntningar på myndigheter att digitalisera sina verksamheter och att samverka över organisationsgränser, samtidigt som det funnits en osäkerhet om hur information som omfattas av sekretess, data- eller säkerhetsskydd ska hanteras.

Myndigheterna uttrycker intresse för en samordnad statlig it-drift även om de har olika behov

Över hälften av myndigheterna i enkätundersökningen uttrycker intresse för en samordnad statlig it-drift. Många framhåller samtidigt att intresset att ansluta sig beror på tjänsteutbudet, priser och anslutningsvillkor. Bilden har nyanserats något i fallstudierna där vissa myndigheter lyft fram exempel på samordnad it-drift som de tycker fungerat mindre bra. Bl.a. har faktorer som minskad kontroll och service samt höga priser lyfts fram.

Myndigheterna har något varierande syn på vad som bör ingå i en samordnad statlig it-drift. Flera mindre myndigheter önskar t.ex. mer omfattande åtaganden, som it-arbetsplatser och support utöver it-drift av specifika system. Flera myndigheter lyfter även fram specifika behov som de bedömer skulle kunna hanteras inom ramen för en samordnad it-drift. Det handlar t.ex. om samlokalisering, serverdrift eller IaaS, containerplattform, applikationsdrift och säkerhetskopiering. Myndigheterna tror bl.a. att en samordnad statlig it-drift kan leda till kostnadseffektivitet, högre säkerhet och förenklad samverkan. Utöver dessa skäl framhåller myndigheterna att en samordnad statlig it-drift kan underlätta kompetensförsörjningen som många myndigheter ser som en utmaning.

Generellt framhåller flera myndigheter att en samordnad statlig it-drift bör fokusera på att tillhandahålla standardiserade och administrativa tjänster. Att fokusera på standardiserade och administrativa tjänster framhölls även som en framgångsfaktor av några länder i omvärldsanalysen som samordnat sin it-drift.

Ett antal större myndigheter framhåller att de har möjlighet att tillhandahålla it-drift. De flesta av dessa myndigheter tillhandahåller redan i dag it-drift i någon form till andra myndigheter. Dessa myndigheter anser att tydlig styrning och ett tydligt mandat är viktiga förutsättningar för att kunna tillhandahålla it-drift.

5 Omvärldsanalys

Enligt utredningsdirektiven ska vi kartlägga och analysera relevanta modeller för statliga myndigheters it-drift såväl nationellt som i ett urval av särskilt intressanta länder med såväl samordnad it-drift som offentlig-privat samverkan kring samordnad it-drift. Vi har valt att närmare studera Norge, Danmark, Finland, Nederländerna och Storbritannien eftersom dessa länder antingen

- har förvaltningsmodeller som påminner om den svenska, vilket bör underlätta jämförelse och möjligheten att generalisera lärdomar,
- är EU-länder med liknande regulatoriska krav, eller
- haft en annan inriktning avseende offentlig-privat samverkan för att tillgodose förvaltningens behov (i fallet med Storbritannien) som inte täcks in av det övriga urvalet.

Omvärldsanalysen beskriver förvaltningsstrukturen i respektive land, hur politiken organiserat arbetet med e-förvaltning och statsförvaltningens digitalisering, styrning av förvaltningens användning av molntjänster, datacenter och synen på cybersäkerhet. Kapitlet avslutas med en sammanfattande diskussion.

5.1 Tidigare studier av samordnad it-drift i andra länder

5.1.1 Statens servicecenters rapport om en gemensam statlig molntjänst

Statens servicecenter (SSC) har i rapporten *En gemensam molntjänst för myndigheternas it-drift* (2016) belyst frågan om en samordnad it-drift i Danmark, Finland, Frankrike, Kanada, Nederländerna och

Storbritannien. SSC konstaterar att det pågår en uppbyggnad av statliga molntjänster samt en konsolidering av statlig it-drift i flera länder. Några generella lärdomar är dock att det tagit längre tid att genomföra samordning av it-driften än väntat och att samordningen är komplicerad och beroende av hur många tjänster som ska samordnas. SSC konstaterar även att viljan bland myndigheter att ansluta sig till samordnade tjänster minskar när de fråntas självbestämmande över sin it.

5.1.2 E-delegationens förstudie om effektiv it-drift inom staten

I förstudien *Effektiv IT-drift inom staten* som togs fram av E-delegationen år 2012 genomfördes en omvärldsanalys av förhållandena i Danmark, Finland, Nederländerna, Storbritannien, Australien, USA, Kanada samt övriga Europa. Förstudien byggde på en bilaga framtagen av konsultföretaget KPMG som studerat Australien, Kanada, Nederländerna, Nya Zeeland och Storbritannien. I förstudien konstaterades att den dåvarande utvecklingen på it-tjänstemarknaden gick mot standardiserade och paketerade lösningar. Förstudien lyfte även fram följande trender inom de respektive ländernas statsförvaltningar:

- Andelen egenproducerad it-drift minskar.
- I många länder pågick olika initiativ för att konsolidera statlig it-drift för att uppnå skalfördelar och samordningsvinster. Flera länder försöker (eller har försökt) inrätta statliga servicecenter.
- Myndighetsperspektivet har fått ge vika till förmån för koncernperspektivet och it-styrning har i högre grad flyttat från myndighetsnivå till central nivå.
- Molntjänster kommer (såsom det 2012 formulerades) om några år vara den dominerande leveransformen för utkontrakterade leverantörer, Shared Service Centers och driftstjänster.
- Mer konkurrens kombinerat med utvecklingen runt molntjänster kommer att pressa styckpriser på it-driftstjänster.
- Utkontraktering av it-drift (till privata tjänsteleverantörer) är vanligare än drift via gemensamma initiativ.

I förstudien konstaterades även att det går att uttyda två ansatser där den ena gått ut på att konkurrensutsätta it-driften på den öppna marknaden (Storbritannien, Nya Zeeland och till viss del i Finland) och den andra på att konsolidera och bygga upp statliga servicecenter (Danmark, Nederländerna och Kanada). Drivkrafterna bakom de två olika ansatserna har dock varit desamma, dvs. lägre kostnader och ökad kostnadskontroll. Andra nyttor som anförts har varit mer fokus på kärnverksamheten, ökad flexibilitet, bättre tillgänglighet, bättre möjlighet att ta fasta på den tekniska utvecklingen, bättre driftsstabilitet, underlättad kompetensförsörjning och grönare it-produktion. Förstudien slår fast att inga länder kommit så långt att det varit möjligt att göra en utvärdering av de totala nettoeffekterna av större effektiviseringsprogram.

5.2 Norge

Norge har liksom Sverige tre förvaltningsnivåer med stat, regioner (fylken) och kommuner. Till statsförvaltningen hör, utöver regeringens departement (departemang), ett 70-tal myndigheter (direktorat) och andra typer av statliga verksamheter. Totalt rör det sig om cirka 250 organisationer. Norge tillämpar en blandning av ministerstyre och samordning mellan departementen i större frågor och har sedan en förvaltningspolitisk reform under 1990-talet relativt självständiga statliga myndigheter. Den kommunala sektorn består av cirka 350 kommuner och 19 fylken.

5.2.1 Organisering och strategi

Den norska regeringen antog år 2016 *Digital agenda for Norge – IKT for en enklere hverdag og økt produktivitet* som innehåller prioriteringar för politiken avseende informations- och kommunikationsteknologi (IKT) och den offentliga sektorns digitalisering. I agendan framhålls att förvaltningens digitalisering bör ske på ett sätt som minimerar risker och komplexitet. Vidare ska marknaden användas där det är lämpligt, förvaltningsgemensamma lösningar byggas för gemensamma behov och interoperabilitet med EU-lösningar främjas. Sedan agendan lades fram har den norska regeringen genom Kommunal- og moderniseringsdepartementet (KMD) bl.a. tagit fram en

molntjänststrategi (2016b), en strategi för den offentliga sektorns digitalisering (2016c) och en cybersäkerhetsstrategi (2016d).

Regeringen förtydligar årligen styrningen av den offentliga förvaltningens digitalisering genom det s.k. Digitaliseringsrundskrivet som innehåller en sammanställning av regeringens beslut, rekommendationer och beskriver KMD:s bedömning av it-relaterade investeringsförslag i kommande års budget. I 2016 års cirkulär framhöll regeringen att statliga myndigheter ska överväga molntjänster när de upphandlar IKT-lösningar. Inriktningen nyanserades år 2019 i molntjänststrategin i vilken regeringen belyste flera aspekter som bör beaktas när den offentliga förvaltningen överväger att använda molntjänster.

Den offentliga sektorns digitaliseringsstrategi är en uppföljning av den digitala agendan från år 2016 och bygger på en överenskommelse mellan regeringen och intresseorganisationen för kommuner och regioner (KS). I agendan beskrivs en rad prioriterade initiativ och e-tjänster under åren 2019–2025. Strategin berör inte uttryckligen it-drift eller molntjänster. Det gör inte heller cybersäkerhetsstrategin, även om den behandlar behovet av samarbete mellan det offentliga och privata respektive det civila och militära samt samarbete på den internationella arenan i syfte att stärka cybersäkerheten i samhället.

I takt med att synen på digitalisering och IKT förändrats från att vara en särfråga till att bli en tvärgående fråga, har också den departementala organiseringen av ansvaret för digitaliseringsfrågor utvecklats i Norge. Under åren 2005–2014 ansvarade Moderniseringsdepartemanget för frågorna och dessförinnan Fornyings-, administrasjons- og kirkedepartementet. Genom en ny departementsindelning år 2014 samlades frågan på KMD tillsammans med frågor om bl.a. kommunernas ekonomi och lokalförvaltning. KMD har ansvar för förvaltningens gemensamma digitalisering medan fackdepartementen har ansvar för digitalisering inom sina respektive områden (t.ex. ansvarar Forsvarsdepartemanget för cybersäkerhetsfrågor). Regeringen har även inrättat Digitaliseringsdirektoratet (tidigare kallat Direktoratet for forvaltning og IKT) med ansvar för att samordna den offentliga förvaltningens digitalisering och år 2019 utsåg den norska regeringen för första gången en digitaliseringsminister.

5.2.2 Digitaliseringsdirektoratet

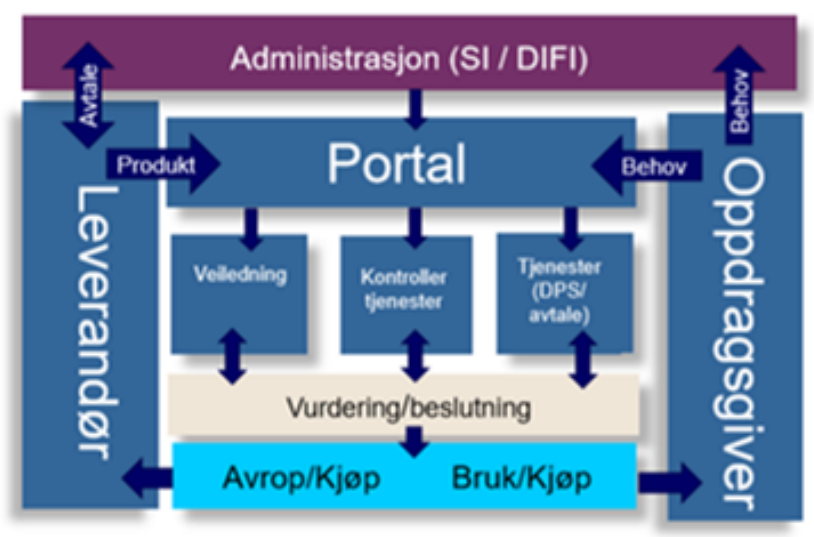
Norge har nyligen genomfört en omorganisering av den myndighet som har det huvudsakliga ansvaret för den offentliga förvaltningens digitalisering. Myndigheten, som tidigare hette Direktoratet for forvaltning og IKT (Difi), inrättades 1 januari 2008 efter en sammanslagning av dåvarande Statskonsult, E-handelssekretariatet samt Norge.no. Direktoratet ansvarade fram till år 2020 för upphandlingsfrågor, rådgivning och utveckling av gemensamma standarder och komponenter. Den 31 december 2019 bytte Difi namn till Digitaliseringsdirektoratet (Digidir) och tog över förvaltningen av e-tjänstplattformen Altinn samt viss verksamhet från den nationella kontroll- och registermyndigheten Brønnøysundregistrene. Digidir fick även utpekat ansvar för informationssäkerhet, drift av förvaltningsgemensamma komponenter, medfinansieringsordningen, Stimulab och tillsynen av universell utformning. Digidir ska fortsatt arbeta nära KS som har ansvar för att involvera och förankra utvecklingen av åtgärder i kommunerna. Vissa frågor, såsom analys och upphandling, som tidigare sköttes av Difi, har överförts till Direktoratet for forvaltning og økonomistyring. Företrädare på Digidir framhåller att reformen syftat till att renodla verksamheten och höja den tekniska utvecklingsförmågan. Reformen innebär även att direktoratet har fått ett tydligare mandat att samordna kommunernas digitalisering. Organisationen för ekonomiskt samarbete och utveckling (OECD) har i genomlysningen *Digital Government Review of Norway* (2017) av den norska e-förvaltningen framhållit att ett av motiven till att ursprungligen inrätta Difi var att förbättra regeringens förmåga att vägleda departementen och myndigheterna i implementation av IKT-projekt. Reformen föranleddes av att Statskonsult omvandlades från myndighet till statligt bolag år 2004, vilket resulterat i utmaningar för organisationens roll att erbjuda sammanhängande strategisk rådgivning till förvaltningen, enligt OECD (2005). När Difi inrättades år 2008 hade myndigheten ungefär 100 anställda vilket ökat till 370 i och med etableringen av den nya organisationen årsskiftet 2019/2000.

5.2.3 Molntjänster i offentlig förvaltning

Företrädare på Digidir framhåller att användningen av molntjänster i den norska offentlig förvaltningen är utbredd, både i leveransen av administrativa tjänster och i annan central infrastruktur såsom Altinn[1]. I den norska molntjänststrategin från år 2017 betonar regeringen flera olika nyttor med användningen av molntjänster, däribland ökad kostnadseffektivitet, flexibilitet, säkerhet och minskat klimatavtryck. Strategin nyanserar den riktlinje som lades fast i digitaliseringscirkuläret år 2016 genom att också belysa lagstiftning som ställer särskilda krav på hur offentliga informationsresurser får hanteras. Exempel på sådan lagstiftning är lagstiftning om arkiv, bokföring och säkerhetsskydd. Mot bakgrund av detta har den norska regeringen beslutat att inte införa en s.k. Cloud First-princip (se avsnitt 5.6). Detta beslut nyanseras dock i strategin med att stora etablerade molntjänstleverantörer ofta kan tillhandahålla bättre säkerhet än vad små organisationer själva kan åstadkomma, enligt en tidigare utredning om digital sårbarhet som regeringen hänvisar till (NOU 2015:13). Regeringen konstaterar i strategin att den offentliga förvaltningen är i behov av tydlig vägledning i upphandlingsfrågor och kring hur avtal bör formuleras för att säkerställa att rättsliga krav följs. För att möta dessa behov ska KMD överväga om det är motiverat att etablera en marknadsplats för molntjänster i offentlig sektor, där leverantörer i förväg kan kvalificera sig, inspirerad av motsvarande lösning i Storbritannien (G-Cloud). Sedan molntjänststrategin publicerats genomförde Difi en förstudie (Difi 2018) om etableringen av en sådan marknadsplats. Enligt förstudien att det är möjligt att realisera en samhällsekonomisk nytta motsvarande 2,2–3,4 miljarder norska kronor perioden 2019–2029 genom att etablera en marknadsplats för molntjänster (Figur 5.1). Regeringen gav år 2019 Digidir och Statens innkjøpssenter i uppdrag att påbörja etableringen av marknadsplatsen senast år 2020. Enligt regeringens uppdrag ska marknadsplatsen bidra till en säker och kostnadseffektiv molntjänstanvändning samt kunna användas av hela den offentliga förvaltningen.

[1] Altinn är en portal med en samling tjänster för dialog mellan privatpersoner, näringsliv och förvaltning. Det är även namnet på den underliggande tekniska plattformen. https://www.altinn.no/om-altinn/hva-er-altinn/.

Figur 5.1 Modell av marknadsplats för skytjenester



Källa: Statens innkjøpssenter.

5.2.4 Datacenter i norsk förvaltning

Under år 2015 lät KMD ett konsultföretag genomföra en kartläggning (Nexia Management Consulting 2015) av offentliga datacenter i Norge. Baserat på intervjuer med it-ansvariga på myndigheter, kommuner och regioner slår studien fast att många kommuner och regioner har samordnat sin it-drift. Kommuner och regioner uppskattades tillsammans ha 100 datacenter jämfört med statsförvaltningen som hade mellan 50–100 stycken. It-ansvariga inom den offentliga sektorn uppgav att de överlag var nöjda med sina driftsmiljöer men framhöll att dessa sannolikt inte kommer kunna tillfredsställa framtida behov. Vidare framkom att större kommuner inte upplevde samma fördelar med samordnad it-drift som mindre, då de uppnådde vissa skalfördelar på egen hand. Studien visade på fortsatta trender mot konsolidering av datacenter och ökad användning av molntjänster. Beträffande molntjänster framhöll dock it-ansvariga att de rättsliga förutsättningarna upplevdes som oklara och de efterfrågade därför förtydliganden. I studien drogs slutsatsen att trenden mot konsolideringen inte varit formellt påkallad utan skett spontant till följd av förvaltningens decentralisering.

Den norska regeringen bedömer i sin molntjänststrategi att det finns behov av en mer resurseffektiv användning av offentliga datacenter. Regeringen menar dock att den inte kunnat identifiera ett behov av gemensamma datacenter eller centralt förhandlade avtal för datacenter. Som konsekvens uppmanas myndigheter, som inte kan använda molntjänster och behöver etablera nya datacenter, att i första hand använda outnyttjad kapacitet hos andra myndigheter alternativt att samordna sig med myndigheter med liknande behov. Digidir pekas ut som ansvarig myndighet att leda denna samordning.

5.2.5 Informations- och cybersäkerhet

I Norge har Justitie- och beredskapsdepartementet ansvar för informationssäkerhet. Den nationella säkerhetsmyndigheten Nasjonal sikkerhetsmyndighet (NSM) har det övergripande ansvaret för samhällets informationssäkerhet. På myndigheten finns avdelningen Nasjonalt cybersikkerhetssenter (NCSC) som etablerades år 2018 och som samordnar it-säkerhetsarbetet genom offentlig-privat samverkan inom flera sektorer. NSM sorterar under Justitie- och beredskapsdepartementet men rapporterar också till Försvarsdepartementet.

På liknande sätt som i flera andra länder finns det i den norska förvaltningen en pågående diskussion om informationssäkerhet och en upplevd osäkerhet avseende de rättsliga förutsättningarna att använda molntjänster. Den norska cybersäkerhetsstrategin berör inte uttryckligen frågan om molntjänster. Däremot betonas i molntjänststrategin att myndigheter måste genomföra risk- och sårbarhetsanalyser vid större förändringar av sina it-miljöer (t.ex. vid övergång till molntjänster). Analyserna bör beakta tillgänglighet, konfidentialitet och integritet hos system och lösningar. Strategin understryker även vikten av att myndigheter löpande klassificerar sin information, då myndigheten själv (på motsvarande sätt som i Sverige) har ansvar för att skydda sin egen information. Informationen bör enligt strategin klassificeras utifrån kategorierna: information som behöver lagras i Norge, information som kan lagras utomlands men tas hem till Norge vid behov samt information som kan lagras utomlands utan några restriktioner. Digidir har fått i ansvar att vägleda myndigheter i hur denna klassificering bör gå till med utgångspunkt i sektorer inom förvaltningen. För att stärka informationssäkerheten

uppmanar regeringen även upphandlande myndigheter att ställa krav på leverantörer med hänvisning till relevanta standarder och certifieringar. Här avses såväl internationella ramverk som t.ex. ISO 27001 och 27018 som andra länders ramverk t.ex. FedRAMP från USA och G-Cloud från Storbritannien. Den norska regeringen har samtidigt aviserat att vägledningar för riskanalyser och annat stöd för upphandling kommer tas fram centralt.

5.3 Danmark

Den offentliga förvaltningen i Danmark är indelad i tre administrativa nivåer: den centrala med ministerier (departement) och 176 myndigheter, fem regioner och 98 kommuner. På central nivå ansvarar en minister ensam för ett departement och som utgångspunkt för beslutsfattande i både enskilda och allmänna fall. Under departementen lyder direktorat eller styrelser, jämförbara med förvaltningsmyndigheter. Vid sidan av förvaltningsmyndigheter finns mer självständiga organ, benämnda nævn eller råd.

5.3.1 Organisering och strategi

Det danska Finansdepartementet ansvarar för en övergripande vision och strategi på e-förvaltningsområdet på central nivå. För att underlätta den offentliga förvaltningens digitalisering bildades år 2011 Digitaliseringsstyrelsen som en sammanslagning av dåvarande IT- og Telestyrelsen och Økonomistyrelsen. Styrelsen är en del av Finansdepartementet och arbetar på strategisk nivå med att utveckla och koordinera den offentliga förvaltningens digitalisering och digitala infrastruktur.

Det finns flera aktuella strategier för den digitala förvaltningen, däribland regeringens digitaliseringsstrategi för den offentliga sektorn (Digitaliseringsstyrelsen 2016), en specifik strategi för statsförvaltningen (Digitaliseringsstyrelsen 2017) samt en övergripande cyber- och informationssäkerhetsstrategi (Digitaliseringsstyrelsen 2018). I mars 2019 ingicks även ett samarbetsavtal mellan regeringen och den danska kommun- och regionsektorn om den offentliga förvaltningens digitalisering.

Från och med den 1 juli 2018 ska all ny lagstiftning som införs efterleva sju principer som gör den lättare att förena med en digital förvaltning (”digitaliseringsklar lovgivning”). Principerna involverar bl.a. digital kommunikation med enskilda, att bygga på existerande digital infrastruktur och standarder i den offentliga förvaltningen samt att återanvända data och tekniska koncept i förvaltningen.

5.3.2 Statens IT

I strategin för statsförvaltningens digitalisering från november 2017 konstaterar regeringen att staten i allt högre grad måste dra nytta av fördelarna med att använda gemensamma it-lösningar och samla grundläggande it-verksamhet för ökad professionalisering och stordriftsfördelar. Redan år 2008 beslutade Finansdepartementet om att inleda ett projekt med uppgift att föreslå hur organisationen av datacenter och it-infrastruktur i staten kunde effektiviseras baserat på en rapport som visat på skalfördelar med en konsolidering av datacenter. Projektgruppen identifierade flera praktiska utmaningar gällande hur konsolideringen skulle gå till, vilken ny it-infrastruktur som behövdes och hur helheten skulle utformas. Enligt projektgruppens bedömning krävdes det bl.a. ny hårdvara för att säkerställa stabiliteten för vissa applikationer och tjänster i statsförvaltningen. Projektgruppen bedömde även att det skulle behövas 2,5 datacenter i den nya organiseringen – två som speglade varandra och ett (halvt) där all lagring säkerhetskopierades. Med utgångspunkt i olika antaganden för utformningen togs ett antal business case fram varefter den danska regeringen beslutade att projektet inledningsvis endast skulle omfatta frivilliga departement. År 2010 bildades myndigheten Statens IT (SIT) genom en sammanslagning av åtta departements it-avdelningar som flyttade in i nya lokaler. Åren 2011–2012 fick SIT även tillgång till de nya datacenter som projektet planerat för och började även upphandla ny hårdvara och utrustning för dessa.

Vid SIT:s inrättande levererade styrelsen tjänster till cirka 10 000 användare vilket i dag ökat till 26 000 användare på 16 departement och 132 organisationer. SIT har cirka 450 anställda och erbjuder huvudsakligen arbetsplatslösningar, it-drift och servicedesk. Kunder har i dag även möjlighet att få visst stöd med utveckling och säkerhet. Eftersom SIT även tar över kontrakt med befintliga leverantörer blir

en naturlig del i arbetet även att integrera och paketera dessa som tjänster gentemot kundmyndigheterna.[2] Vissa myndigheter såsom Skatteverket, Polisen och försvarsmyndigheterna använder inte SIT eftersom de på egen hand kan uppnå skalfördelar eller har högre ställda krav på informationssäkerhet än vad SIT kan tillgodose. Verksamheten är helt avgiftsfinansierad sedan år 2015. Innan dess finansierades verksamheten delvis genom avgifter och delvis genom en överföring av anslag från kundmyndigheter till SIT. Anslutning av kundmyndigheter till SIT inleds med en dialog mellan SIT och potentiell kundmyndigheten. Därefter tas ett business case fram som klargör befintliga kostnader för it-verksamheten, övergångskostnader samt framtida kostnader när berörd it-verksamhet överförts till SIT. För att ge rätt incitament till involverade parter betalar SIT hälften av övergångskostnaderna medan kundmyndigheten får behålla hälften av besparingen (principen kallas ”shared risk, shared reward”). I ett business case görs också en avgränsning av vilken it-verksamhet som bör flyttas över genom att kundmyndighetens behov jämförs med SIT:s tjänstekatalog. Därefter tas ett beslutsunderlag fram som signeras av två ansvariga ministrar och en resolution som skrivs under av drottningen (Kongelig resolution). Resolutionen delegerar ansvaret för it-verksamheten hos berörd myndighet till Finansdepartementet som sedan delegerar det vidare till SIT. Det förekommer även verksamhetsövergångar från kundmyndigheter till SIT. Eftersom berörd personal ofta även har andra uppgifter, som inte övertas av SIT, sker verksamhetsövergångar endast undantagsvis. Företrädare på SIT uppger att myndigheten har arbetat framgångsrikt med att bli en attraktiv arbetsgivare för att kunna bibehålla övertagen personal. Relationen mellan SIT och kundmyndigheter regleras i ett s.k. kundkontrakt. Kontraktet är inte formellt bindande eftersom staten är en juridisk person och skulle en tvist uppstå så hanteras denna inom eller mellan berörda departement.

De tjänster SIT erbjuder har utvecklats över tid från att inledningsvis konsolidera och paketera den it som övertagits från myndigheter, till att erbjuda nya tjänster baserad på hårdvara upphandlad av SIT. Om de anslutande kundmyndigheterna behöver upphandla de tjänster de erhåller från SIT eller inte har hittills berott på vilken typ av tjänst det handlat om. Standardiserade tjänster som paketerade it-arbetsplatser (arbetsdator och licenser) har kundmyndigheterna

[2] Även kallat Service Integration and Management (SIAM).

kunnat nyttja utan att genomföra egna upphandlingar. I de fall verksamheterna haft specifika behov har kundmyndigheterna själva genomfört upphandlingen.

Under år 2020 planerar SIT att lansera en molntjänst för staten kallad GovCloud. Tjänsten har hittills endast tagits i drift i mindre skala. Företrädare på Digitaliseringsstyrelsen framhåller att det funnits flera drivkrafter bakom lanseringen, bl.a. lägre kostnader, förenklad hantering av dataskydd och ett mål att stärka viss teknisk kompetens inom staten.

5.3.3 Molntjänster

Användningen av publika molntjänster är utbredd i den danska offentliga förvaltningen. Precis som i Sverige finns en osäkerhet om de rättsliga förutsättningarna och det pågår en diskussion om potentiella risker och möjligheter med molntjänster.

SIT framhåller i en intervju med konsultföretaget McKinsey & Company (2019) att det finns stora fördelar både med privata och publika molntjänster som gör det möjligt för användare att arbeta på nya sätt och att anpassa sig efter föränderliga behov. SIT:s direktör Michael Ørnø har konstaterat att det finns stor besparingspotential i att konsolidera datacenter, genom lägre hyreskostnader och elförbrukning. I jämförelsen mellan privata och publika molntjänster framhåller Ørnø viktiga skillnader avseende funktionalitet, rättsliga förutsättningar och finansiell risk. Publika molntjänster erbjuder i dagsläget mer funktionalitet, varför det blir naturligt för förvaltningen att också fortsättningsvis använda publika molntjänster där det är lämpligt. När det gäller de rättsliga förutsättningarna finns fortfarande utmaningar förknippade med hur känsliga data bör skyddas i publika molntjänster. När det gäller finansiella risker kan efterfrågan på molntjänster vara svår att prognostisera vilket, kombinerat med flexibel prissättning, kan bli kostnadsdrivande. Det finns även risker med inlåsning mot vissa molntjänster.

Informationsklassificering är enligt Ørnø en förutsättning för att en myndighet ska kunna göra ett korrekt val mellan privata eller publika molntjänster. Att utgå från att all data är känslig och bygga lösningar med hög säkerhet för att skydda den kommer att bli orimligt dyrt. Genom god informationsklassificering blir det däremot möj-

ligt att segmentera data och välja de mest kostnadseffektiva lösningarna utifrån behovet av skydd. Även variationen i efterfrågan på tjänster är viktig för valet mellan privata och publika molntjänster. Ørnø framhåller att publika molntjänster gör det möjligt att snabbt utveckla och testa nya lösningar, men att transaktionstunga applikationer med förhållandevis jämn efterfrågan kan vara dyrare att produktionssätta i publika molntjänster jämfört med privata. Vidare är det av strategisk betydelse för förvaltningen att ha fortsatt kontroll över sina it-lösningar. För att kunna bibehålla denna kontroll, ha förmåga att specificera krav samt utmana priser och villkor i förhållande till leverantörer är det viktigt att bibehålla viss teknisk kompetens inom förvaltningen.

5.3.4 Informations- och cybersäkerhet

I Danmark ansvarar Försvarsdepartementet för samordningen inom it-säkerhetsområdet på central nivå. Under Försvarsdepartementet ligger det nationella centret för cybersäkerhet Center for Cybersikkerhed (CFCS) som grundades år 2012. Centret fungerar som kompetenscenter för både offentlig sektor och näringsliv. CFCS ansvarar även för informationssäkerhet och beredskap inom telekommunikationssektorn. I ansvaret ingår att upptäcka, analysera och bidra till att avvärja avancerade it-attacker mot myndigheter och företag som hanterar samhällsviktiga funktioner i finanssektorn, staten, telenätet, vattenförsörjningen. Centret förbereder även hotbedömningar halvårsvis. Digitaliseringsstyrelsen har till uppgift att stärka statens it-säkerhet genom att främja att myndigheter efterlever ISO 27001.

År 2014 trädde lov om Center for Cybersikkerhed i kraft. Lagen pekar ut CFCS som ansvarig för hantering av incidentrapportering, tillsyn och andra normerande uppgifter. Av lagen följer att CFCS ska ha en nätverkssäkerhetstjänst till vilken vissa myndigheter och företag ska ansluta sig för att CFCS ska kunna övervaka nätverkskommunikation.

Den danska regeringen har antagit en strategi för cyber- och informationssäkerhet som gäller under åren 2018–2021 (Digitaliseringsstyrelsen 2018). Strategin berör hela samhället men pekar ut sex specifika sektorer där cyber- och informationssäkerheten behöver stärkas (telekom, finans, energi, vård, transport och sjöfart). I stra-

tegin konstaterar regeringen att det finns risker med komplexa och föråldrade it-lösningar i den offentliga förvaltningen och att det blir svårt och dyrt att trygga en god nivå på säkerheten. Molntjänster och koncept som digital suveränitet belyses dock inte särskilt i strategin.

Vägledningen *Vejledning til anvendelse af cloud* från Digitaliseringsstyrelsen (2019) är ett försök att ge klarhet i vad molntjänster är samt när de bör, alternativt inte bör, användas i offentlig förvaltning. Organisationer i den offentlig förvaltningen behöver enligt vägledningen säkerställa att det finns rättsliga förutsättningar för användande av molntjänster, att de vidtagit nödvändiga säkerhetsåtgärder och att de gjort en riskbedömning av lösningen som svarar upp mot krav som ställs samt att det är möjligt att kontrollera om leverantörer lever upp till dessa krav. Överväganden av de rättsliga förutsättningarna bör göras med utgångspunkt i bl.a. lagstiftning om offentlig upphandling och dataskydd (om lösningen innebär behandling av personuppgifter). Då molntjänsternas karaktär i regel gör det svårt för kunden att kontrollera leverantören bör den riskbaserade bedömningen baseras på tillgänglig dokumentation, möjliga certifieringar och revisionsberättelser, både innan avtal ingås och även löpande under avtalstiden. I vägledningen noteras även att det kan vara svårt att påverka villkor i standardavtal med stora internationella leverantörer som bestämmer säkerhetspolicy på global nivå. Samtidigt har flera stora molntjänstleverantörer avancerade tjänster och stor expertis vilket kan göra det möjligt att uppnå god teknisk säkerhet, redundans och tillgänglighet.

Sammanfattningsvis framhålls i vägledningen att kommersiella molntjänster möjliggör nya lösningar och innovation i den offentliga förvaltningen. Samtidigt betonas också att de risker som finns förknippade med säkerhet och kostnad kräver noggranna affärsmässiga, juridiska och säkerhetsmässiga överväganden.

5.4 Finland

Den finländska förvaltningen är indelad i tre administrativa nivåer. Statens centralförvaltning består av ministerierna (jfr departement) och de riksomfattande ämbetsverken (jfr myndigheter) inklusive inrättningarna inom deras respektive förvaltningsområden. Regional nivå innefattar regionförvaltningsmyndigheter samt närings-, trafik-

och miljöcentralerna. Lokal nivå utgörs av kommuner som anordnar den lagstadgade basservicen för kommuninvånarna och är självstyrande med beskattningsrätt. Styrningen av den finländska statsförvaltningen påminner om den svenska genom att ha relativt självständiga myndigheter samtidigt som enskilda statsråd inte tar beslut i enskilda ärenden.

5.4.1 Organisering och strategi

I Finland ansvarar Finansdepartementet för förvaltningens digitalisering och e-förvaltning på en övergripande nivå. Inom detta område ingår styrning av den offentliga förvaltningens informationshantering och förvaltningsgemensamma digitala tjänster. Övriga sakdepartement styr informationshantering och relaterade projekt inom sina respektive ansvarsområden. Sedan år 2011 är arbetet med informationshantering på Finansdepartementet förlagt till Enheten för offentlig sektors IKT.

Finansdepartementet har vidare tillsatt Delegationen för informationsförvaltningen inom den offentliga förvaltningen (JUHTA) och Ledningsgruppen för digital säkerhet inom den offentliga förvaltningen (VAHTI). JUHTA är ministeriernas och kommunalförvaltningens samarbets- och förhandlingsorgan i frågor som rör digital informationsförvaltning, medan VAHTI är ett samarbetsorgan för styrning och utveckling av informationssäkerheten inom den offentliga förvaltningen.

Under departementet finns två myndigheter med särskilt ansvar för digitalisering i offentlig förvaltning: Valtori, ett servicecenter med ansvarar för försörjning av gemensamma informations- och kommunikationstekniska tjänster och Myndigheten för digitalisering och befolkningsdata. Den senare inrättades den 1 januari 2020 och har tagit över VAHTI:s operativa verksamhet. Myndigheten har även särskilt ansvar för vissa förvaltningsgemensamma digitala komponenter såsom den nationella portalen Suomi.fi, elektroniska myndighetsmeddelanden och en fullmaktstjänst.

Den strategiska inriktningen för den offentliga sektorns digitalisering utgår från ett regeringsprogram som läggs fast i samband med att en ny regeringen tillträder. Det senaste programmet, som utgår från regeringen Marin (2019a), har som mål att bl.a. utveckla den

digitala tillgängligheten i digitala tjänster, stärka skyddet för den personliga integriteten samt satsa på kompetensförsörjning som möjliggör digital transformation av den offentliga förvaltningen. Av programmet framgår även att en nationell cybersäkerhetsstrategi ska tas fram.

5.4.2 Valtori och reformen av statens it

Under en period innan 2010-talet hade den finländska statsförvaltningen flera servicecenter med uppgift att hantera it- och kommunikationslösningar. Ett mål i statsminister Jyrki Katainens regeringsprogram år 2011 var att samla dessa uppgifter på ett ställe för att uppnå skalfördelar.[3] År 2012 tog riksdagen beslut om en it-reform i enlighet med regeringens förslag för att effektivisera förvaltningen.[4] Riksdagens beslut blev startskottet för det s.k. TORI-projektet som leddes från Finansdepartementet under åren 2012–2015 med uppgiften att koncentrera verksamhetsoberoende it- och kommunikationslösningar så att

– koncentreringen klart kunde visas ge helhetsekonomiska besparingar inom statsförvaltningen,
– tjänsternas funktionssäkerhet och serviceförmåga garanterades även i ett övergångsskede,
– ett servicecenter som producerar nya branschoberoende informations- och kommunikationstekniska tjänster åt statsförvaltningen kunde inleda sin verksamhet enligt TORI-projektets tidsplan och
– att den statliga personalpolicyn och statsrådets (statsministerns) principbeslut om tjänstemäns rättigheter vid organisationsförändringar efterlevs.[5]

Parallellt med TORI-projektet infördes en rad nya lagar och förordningar som övergripande syftade till kostnadsbesparingar och högre kvalitet genom en mer effektiv digital förvaltning. År 2011 infördes lagen om informationshantering inom den offentliga förvaltningen

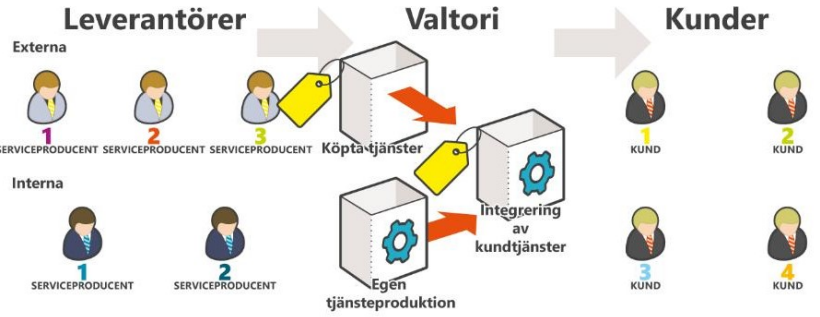
[3] Finlands regering (2011a, 2011b).
[4] Finlands finansutskott (2012).
[5] Finlands regering (2016).

(634/2011). Lagen innehåller bestämmelser bl.a. om informationssäkerhet, arkivering och elektronisk kommunikation mellan myndigheter och har som uttalat syfte att bl.a. främja interoperabilitet mellan it-system i förvaltningen.[6] Två år senare infördes ytterligare lagstiftning som gav regeringen möjlighet att peka ut ett servicecenter med ansvar att tillhandahålla gemensamma stödtjänster för e-tjänster och e-förvaltning till statsförvaltningen samt en skyldighet att använda dessa tjänster.[7] År 2014 pekade regeringen ut det nyligen bildade servicecentret Valtori som ansvarigt för att tillhandahålla de förvaltningsgemensamma stödtjänsterna.[8] Valtori inrättades med stöd av ny lagstiftning och i linje med TORI-projektets ursprungliga tidsplan. Valtori har cirka 1 400 anställda på 30 filialer runtom i Finland. Myndighetens uppdrag är att tillhandahålla verksamhetsoberoende it-lösningar och integrationstjänster till statsförvaltningen. Målet är att produktion och organisering av de tjänster Valtori erbjuder inte ska kräva betydande kunskaper om enskilda kunders verksamhet och att tjänsterna ska grundas på allmänt använda programvarulösningar och vanligt förekommande teknik. Kundmyndigheter är enligt lag skyldiga att använda de flesta av Valtoris tjänster, men det finns även tjänster som är valfria att använda. Exempel på de tjänster Valtori erbjuder är kommunikationstjänster (e-post, webbmöten och videokonferens etc.), arbetsplatstjänster (arbetsdator, mobiltelefon, programvaror och licenser etc.), datacentertjänster och plattformstjänster. Valtori erbjuder även konsultationstjänster inom it-arkitektur och cybersäkerhet.[9]

Driftstjänster (också benämnda som datacenter- och kapacitetstjänster av Valtori) är indelade i tre kategorier utifrån var de produceras. Den första kategorin produceras i Valtoris egna datacenter i Finland. Den andra kategorin produceras av partners både i Finland och inom EES med krav på att leverantörer lever upp till krav på vissa skyddsnivåer. Den tredje kategorin är driftstjänster producerade i publika molntjänster, såsom Microsoft Azure och Amazon Web Services. Den sistnämnda kategorin produceras i huvudsak i Finland eller inom EES.

[6] Lag om styrning av informationsförvaltningen inom den offentliga förvaltningen (634/2011).
[7] Lagen om anordnande av statens gemensamma informations- och kommunikationstekniska tjänster (1226/2013).
[8] 4 § Statsrådets förordning om anordnande av statens gemensamma informations- och kommunikationstekniska tjänster (132/2014).
[9] En fullständig tjänstekatalog finns på Valtoris webbplats (https://valtori.fi/sv/tjanster).

Figur 5.2 Valtoris illustration av Service Integration and Management (SIAM)



Källa: Valtori.

Tjänsterna produceras i vissa fall inom Valtori men är i regel en kombination av tjänster och produkter från olika tjänsteleverantörer som Valtori integrerar och paketerar gentemot kund (Figur 5.2). Kundmyndigheter behöver dock inte göra egna upphandlingar för att använda Valtoris tjänster.

5.4.3 Statens Revisionsverks granskning

Genom att samla visst ansvar för it- och kommunikationslösningar på Valtori, samt genom att ge Valtori och den statliga inköpscentralen Hansel AB ansvar för it-upphandlingar, räknade den finländska regeringen med att spara 47 miljoner euro till år 2018. Mål för reformen sattes i regeringsprogrammet år 2011. Statens revisionsverk granskade reformen år 2018 och slog fast att regeringen inte fullt ut lyckats nå de uppställda målen. TORI-projektet hade planerats utifrån en kartläggning genomförd år 2012 där endast en grov uppskattning gjorts av projektets besparingspotential. Valtori och Finansdepartementet, som står för ämbetsverkets resultatstyrning, ansåg att de besparingsmål som uppställts när Valtori inrättades i huvudsak uppnåtts. Revisionsverket menade dock att de huvudsakliga besparingarna uppstått till följd av Hansels ramavtal och att kostnadseffektiviteten minskat hos de tjänster som överförts från myndigheterna till Valtori, särskilt i fråga om användarstöd och driftstjänster. Enligt Revisionsverket kan de nya centraliserade tjänsterna enligt tillgängliga beräk-

ningar inte anses mer kostnadseffektiva än de tidigare arrangemangen eller tjänster som finns på marknaden. Samtidigt framhåller Revisionsverket att Valtori år 2017 genomfört utvecklingsinsatser som ännu inte hunnit påverka revisionens slutsatser. Revisionsverket rekommenderar regeringen att centralisera det övergripande ansvaret för upphandling av grundläggande informationsteknik till en aktör och att utöka användningen av kostnads- och kvalitetsindikatorer i styrningen av Valtori. Avseende upphandling beskriver Riksrevisionsverket att produktion och anskaffning av grundläggande informationsteknik sker i Valtori medan konkurrensutsättning görs av Hansel.[10]

5.4.4 Finansdepartementets utvärdering

Finansdepartementet har under år 2019 låtit utvärdera Valtori och Palkeet – ett mindre servicecenter ansvarigt för HR- och ekonomiverktyg. I utvärderingen konstateras att kostnadseffektiviteten hos Valtori varierar utifrån serviceområde. Jämfört med marknadspriserna är Valtori konkurrenskraftig när det gäller expertkonsultation och kommunikationstekniska tjänster. Däremot är arbetsplats- och driftstjänster enligt utvärderingen dyrare än på marknaden. För driftstjänster specifikt förklaras skillnaderna i pris delvis med Valtoris relativt omfattande skyldigheter avseende säkerhetsskydd och delvis med att myndigheten köpt och nyttjat kapacitet i publika molntjänster på ett sätt som drivit kostnader. I utvärderingen konstateras samtidigt att Valtori är billigare än andra jämförbara servicecenter i Norden. Finansministeriet har inlett ett åtgärdsprogram för att utveckla Valtoris verksamhet.[11]

5.4.5 Informations- och cybersäkerhet

I Finland ansvarar Finansdepartement för den offentliga sektorns digitalisering inklusive frågor om it-säkerhet. Kommunikationsdepartementet ansvarar för it-säkerhet i samhället som helhet och elektronisk kommunikation. Bland myndigheterna har Kommunikationsverket (FICORA) centralt ansvar för it-säkerhetsfrågor. FICORA är underordnat Kommunikationsdepartementet och National Cyber Secu-

[10] Statens Revisionsverk (2019).
[11] Finlands regering (2020b).

rity Center Finland (NCSC-FI), som bl.a. ansvarar för den nationella it-incidenthanteringsfunktionen (CERT). I Finland finns sektorsspecifik it-säkerhetslagstiftning. Lagen om tjänster inom elektronisk kommunikation (917/2014) är av central betydelse i sammanhanget. I lagens regleras e-tjänster och den uppställer också it-säkerhetskrav på leverantörer av e-tjänster. Stora incidenter och risker som utgör hot mot samhällets informationssäkerhet måste rapporteras till Kommunikationsverket. Lagen ställer övergripande säkerhetskrav och ger Kommunikationsverket befogenhet att föreskriva detaljerade krav. I statsrådets förordning om informationssäkerheten inom statsförvaltningen (681/2010) uppställs krav på hur statliga myndigheter ska skydda känslig information, klassificera uppgifter som kan leda till skada för allmänna eller enskilda intressen om de kommer i händerna på obehöriga.

Den 3 oktober 2019 antog den finländska regeringen ny cybersäkerhetsstrategi med nationella mål för cybersäkerhet och för skyddet av samhällsviktiga funktioner. I strategin behandlas inte molntjänster specifikt men strategin fastslår att en ny roll som Cybersäkerhetsdirektör ska upprättas på Transport- och kommunikationsdepartementet. Cybersäkerhetsdirektören kommer att ansvara för att, i nära samråd med representanter från offentlig förvaltning och näringsliv, ta fram och driva ett utvecklingsprogram som ska höja beredskapen inom cybersäkerhet.[12]

5.5 Nederländerna

Den offentliga förvaltningen i Nederländerna är organiserad i fyra nivåer: den centrala med statliga myndigheter, den regionala med 12 provinser, samt den lokala med 393 kommuner och vattenförvaltningar. Regionerna och kommunerna har visst självbestämmande. Statsförvaltningen utgörs av elva departement med 574 myndigheter under sig som sammanlagt består av 116 000 anställda.

[12] Finland's Cyber Security Strategy (2019).

5.5.1 Organisering och strategi

En digital agenda[13] för den offentliga förvaltningen antogs av den nederländska regeringen år 2018. Agendan, som är kopplad till en bredare digital agenda för hela samhället, har fem fokusområden: innovation, data, inkludering, digital identitet och datakontroll. Statssekreteraren på Inrikesdepartementet ansvarar för genomförandet av agendan medan sektorsansvariga statsråd är ansvariga för IKT inom sina respektive sektorer. Utöver den digitala agendan för den offentliga förvaltningen finns även en särskild agenda för cybersäkerhet[14] samt en egen agenda för data[15].

5.5.2 Molntjänster

År 2010 uppdrog det nederländska parlamentet åt regeringen att ta fram en molnstrategi som efterliknade motsvarande strategier som antagits i Japan, Storbritannien och USA. Regeringen ombads även analysera för- och nackdelar med att inrätta ett privat moln för staten. Regeringen meddelade[16] parlamentet år 2011 att det visserligen fanns nyttor med användning av molntjänster i staten men att nackdelarna övervägde fördelarna, givet marknadens mognad vid tillfället. I meddelandet beskrevs bl.a. de informationssäkerhetsrisker som är förknippade med att lagra känslig information i publika molntjänster utanför Nederländerna. Mot denna bakgrund, och i linje med ett bredare reformprogram för statsförvaltningen (se avsnitt 5.5.3), beslutade regeringen år 2011 att inrätta ett privat statligt moln i egen regi. Det finns i dagsläget inget ramavtal för publika molntjänster på central nivå.

Från och med år 2016 öppnade regeringen även upp för att viss användning av publika molntjänster inom statsförvaltningen var tillåten, givet att ett antal villkor vad uppfyllda.[17] Några år senare (år 2019) genomförde det nederländska cybersäkerhetscentret (NCSC) en undersökning på begäran av Inrikesdepartementet i syfte att ge underlag till en ny molnstrategi. I undersökningen framhölls att det finns fördelar med användning av publika molntjänster, som ökad

[13] Nederländernas regering (2018a).
[14] Nederländernas regering (2018b).
[15] Nederländernas regering (2019a).
[16] Nederländernas regering (2011a).
[17] Nederländernas regering (2016).

flexibilitet genom att göra det lättare att anamma ny teknik och därmed snabbare kunna svara upp mot ändrade lagar och förordningar. Vidare konstaterades att publika molntjänster kan vara lämpliga för tillfälliga behov, t.ex. vid utveckling av proof-of-concepts, eftersom de inte behöver kräva stora initiala investeringar. I undersökningen belystes samtidigt en rad risker, bl.a. att oförutsedd efterfrågan kan leda till stora kostnader samt att vissa molntjänstleverantörer är stora globala aktörer vilket kan göra det svårare att säkerställa eller verifiera hur de lever upp till ställda krav.

5.5.3 Datacenter

Inrikesdepartementet i Nederländerna beslutade år 2011 om ett reformprogram för att effektivisera statsförvaltningen och sänka de offentliga utgifterna med drygt 6 miljarder euro till och med år 2015.[18] I programmet beskrevs statsförvaltningens it som fragmentiserad. Det sades också att det fanns stora skillnader mellan departementen avseende it-säkerhet, identitetshantering, upphandlingar av it-lösningar och i hanteringen av datacenter. För att minska denna fragmentisering aviserade regeringen i programmet att den bl.a. avsåg att reducera antalet datacenter under departementen från 64 till 4, vilket skulle ta fyra år och innebar att departementen fick överföra sina dåvarande datacenter till nya statligt centralt förvaltade datacenter. Försvarsdepartementet skulle vara involverat under etableringen för att säkerställa att relevanta rutiner och funktioner upprättades. De fyra förvaltningsgemensamma datacenter (Figur 5.3) som därefter etablerades hanteras i dag av den statliga organisationen för gemensamma IKT-tjänster (SSC-IT). SSC-IT etablerades 2003 och har sedan dess successivt tagit över it-verksamhet från allt fler departement. I dag drivs SSC-IT som ett bolag som samägs av sju departement med cirka 1 200 anställda. Cirka 40 000 tjänstemän arbetar i dag i it-miljöer som tillhandahålls av SSC-IT. Verksamheten tillhandahåller bl.a. utveckling och förvaltning av applikationer och tjänster och digitala arbetsmiljöer för tjänstemän. Företrädare på SSC-IT:s menar att konsolideringen av datacenter i statsförvaltningen gett

– bättre förutsättningar för digital utveckling genom en moderniserad driftsorganisation och ny teknik,

[18] Nederländernas regering (2011b).

– högre säkerhet genom ökad kontroll, samt
– möjlighet att realisera skalfördelar.

De fyra datacentren är klassificerade som tier 3[19] och är förbundna med ett fibernät som förvaltas av staten (Figur 5.3). Två av anläggningarna ägs av staten medan två hyrs av privata fastighetsägare. Personalen på datacentren är huvudsakligen anställda på SSC-IT.

Figur 5.3 SSC-IT:s fyra datacenter

Källa: SSC-IT.

År 2013 öppnades det första av de fyra centren, ODC-Noord (ODCN), som inledningsvis hade Utbildnings-, kultur- och vetenskapsdepartementet som kund. I dag är även Justitie-, Infrastruktur och Inrikesdepartementet kunder till ODCN. Cirka 50 personer arbetar på datacentret varav 37 tekniker (år 2018). Till en början erbjöd ODCN enbart samlokalisering vilket år 2014 kompletterades

[19] Ett datacenter klassat som tier 3 kräver bl.a. inga avstängningar för byte av utrustning, reservdelar och underhåll.

med vissa infrastrukturtjänster. Tjänsteerbjudandet har utvecklats stegvis från samlokalisering, infrastrukturtjänster, lagring, plattformstjänster, till att nu även omfatta vissa SaaS-tjänster samt stöd vid migration till centrets tjänster. Företrädare på SSC-IT framhåller att fördelarna med de statliga datacentren är att kunderna betalar baserat på användning och att de kan fokusera på kärnverksamheten i stället för it-drift. Datacenterverksamheten hos SSC-IT är helt avgiftsfinansierad och baseras på självkostnadspris. En annan fördel är att erbjudna tjänster huvudsakligen bygger på öppen källkod och öppna standarder, vilket varit ett strategiskt vägval för att minska risken för inlåsningseffekter. En utvärdering av reformen med datacentren pågår och ska presenteras för parlamentet under år 2020. SSC-IT räknar dock med att ungefär 50 datacenter i statsförvaltningen har avvecklats sedan reformen påbörjades. Vidare har Utbildnings-, kultur- och vetenskapsdepartementet rapporterat om kostnadsbesparingar om 30 procent vid övergång till ODC-Noord:s molntjänster jämfört med innan.[20]

5.5.4 Riksrevisionens årsrapport 2019

Den nederländska riksrevisionen konstaterar i sin årsrapport för 2019 att många departement utkontrakterat uppgifter till delade serviceorganisationer (SSO), såsom t.ex. IT-hantering (till SSC-IT), kontorsstädning och personal- och löneadministration för cirka 130 000 tjänstemän. Riksrevisionen anser att fördelarna hittills inte varit tydliga. Exempelvis beskriver Riksrevisionen att av de sju departementen som använder SSC-IT har flera bett om anpassade it-leveranser varför det inte gått att standardisera arbetsprocesser tillräckligt. Eftersom det heller inte är obligatoriskt att använda SSC-IT:s tjänster har departement påbörjat och avslutat samarbeten med SSC-IT på ett sätt som gjort att fokus hittills hamnat på övergångar snarare än effektivisering. Riksrevisionen menar även att departementen haft liten insyn i SSC-IT:s aktiviteter och därmed låg kostnadskontroll.[21]

[20] Open Source Observatory (2017).
[21] Riksrevisionen i Nederländerna (2019).

5.5.5 Informations- och cybersäkerhet

I Nederländerna ansvarar Justitie- och säkerhetsdepartementet för samordningen av it-säkerhetsfrågor. Bland myndigheterna ansvarar det nationella cybersäkerhetscentret (NCSC) för att samordna nationell hot- och incidenthantering, öka allmänhetens medvetenhet om it-säkerhet samt att ge råd och vägledning. Centret samordnar flera offentlig-privata forum och partnerskap på temat it-säkerhet. År 2017 antogs lagstiftningen Dutch Data Processing and Cybersecurity Notification Obligation Act. Lagen kodifierar NCSC:s uppgifter och ger bl.a. rättslig grund för centret att behandla de personuppgifter som är nödvändiga för att centret ska kunna utföra sina uppgifter. I lagen föreskrivs också en skyldighet att rapportera vissa incidenter och säkerhetsöverträdelser till NCSC. Skyldigheten riktar sig till dem som kallas vitala operatörer. Vilka verksamheter som utgör vitala operatörer specificeras i sektorsspecifik reglering för el, gas, vattenförsörjning, e-handel, finans, transport och offentlig sektor.

Den nederländska agendan för cybersäkerhet antogs år 2018 av regeringen och parlamentet med syftet att motverka växande hot och sårbarheter i den digitala sfären. Viktiga inslag i regeringens arbete med cybersäkerhet för den offentliga förvaltningen är att främja moderna standarder för it-säkerhet och åtgärder för att förbättra robustheten för samhällsviktiga tjänster. Andra initiativ som lyfts fram i agendan är en kravkatalog för säker mjuk- och hårdvara till upphandling, ett utbildningsprogram inom cybersäkerhet för statliga tjänstemän samt krav på offentliga verksamheter att använda protokoll för krypterad transport av webbdata (HTTPS) och korrekta certifikat för att säkra kommunikationen med enskilda.[22] NCSC bedömer att molntjänster bör ses som en typ av utkontraktering, dock med risker förknippade med svårigheten att kontrollera vem som har tillgång till system och information. Att använda de förvaltningsgemensamma datacentren framhålls som ett sätt att öka kontrollen av personal och det fysiska skyddet.

En milstolpe i cybersäkerhetsagendan har hittills varit lanseringen av ett gemensamt ramverk med regler om informationssäkerhet (Government Information Security Baseline på engelska vilket förkortas BIO) som trädde i kraft den 1 januari 2020. Syftet med ramverket är att minska den administrativa bördan för offentliga organisationer

[22] Nederländernas regering (2018c).

och leverantörer och att harmonisera krav med internationella regler och standarder. I ramverket delas kraven på hantering av konfidentiell information in i tre nivåer. Det nationella cybersäkerhetscentret (NCSC) bedömer att det för den lägsta skyddsnivån bör vara tillåtet att använda publika, hybrida eller privata molntjänster. För mellannivån bör dessa typer av molntjänster också vara tillåtna, förbehållet att det finns förutsättningar att identifiera och hantera avancerade och uthålliga hot (eng. Advanced Persistent Threats). Det finns även en delmängd av information i mellannivån för vilken enbart privata molntjänster eller de statliga datacentren bör vara tillåtna. För information på den högsta skyddsnivån får varken någon form av molntjänster eller de statliga datacentren användas.[23]

BIO är förpliktigande. Någon i lagstiftningen utpekad tillsynsinstans finns dock inte ännu. Offentliga verksamheter förväntas därför att på egen hand se till att regelverket efterlevs. Innan BIO trädde i kraft skiljde sig bestämmelserna om informationssäkerhet åt mellan de olika nivåerna i förvaltningen.

Utöver detta finns andra nationella regelverk som styr informationsklassificeringen i den offentliga förvaltningen, bl.a. förordningen om informationssäkerhetsföreskrifter (VIR och VIR-BI).

Det nederländska Justitiedepartementet har etablerat leverantörsansvariga för större it-leverantörer till staten, däribland Microsoft, Oracle och SAP. Leverantörsansvarig för Microsoft (SLM Rijk) beställde under år 2018 en konsekvensbedömning avseende dataskydd (DPIA) i enlighet med artikel 35 i dataskyddsförordningen av Microsoft Office i syfte att kartlägga eventuella integritetsskyddsrisker. Microsoft Office används av drygt 300 000 tjänstemän i den nederländska staten. Genom granskningen identifierades ett antal större integritetsskyddsrisker som SLM Rijk påtalade för Microsoft. SLM Rijk och Microsoft har därefter samarbetat för att hitta möjliga lösningar på de identifierade bristerna. Microsoft har även meddelat att de regelbundet kommer att rapportera om utvecklingen avseende påtalade brister. SLM Rijk har aviserat att de kan hänskjuta frågan till den nationella dataskyddsmyndigheten om de inte bedömer att utvecklingen är tillfredsställande.[24]

[23] Nederländernas regering (2019b).
[24] Nederländernas regering (2018d).

5.6 Storbritannien

Den brittiska statsförvaltningen har cirka 120 ministrar som stöds av 560 000 tjänstemän på 25 departement och deras myndigheter. Övriga delar av förvaltningen är organiserade på olika sätt beroende på riksdel.

5.6.1 Organisering och strategi

År 2011 lanserade koalitionsregeringen i Storbritannien en IKT-strategi[25] med fokus på att uppnå ökad effektivitet och kostnadsbesparingar i statsförvaltningen. Samma år inrättades även Government Digital Services (GDS), en enhet inom Cabinet Office (jfr Statsrådsberedningen), med övergripande ansvar att leda förvaltningens omställning till digitala kanaler som förstahandsval i interaktionen med enskilda (eng. digital by default). De följande åren lanserades flera nya strategier[26] på e-förvaltningsområdet. Utöver GDS har den statliga inköpscentralen Crown Commercial Services (CCS) en central roll i förvaltningens digitalisering genom att bl.a. hantera ramavtal på it-området. Det brittiska National Cyber Security Centre (NCSC) är vidare en central aktör i arbetet med cybersäkerhet och har ett övergripande ansvar för att hålla samman Storbritanniens cybersäkerhetsstrategi på nationell nivå.

5.6.2 Molntjänster

Genom en större satsning på molntjänster under tidigt 2010-tal avsåg den dåvarande brittiska regeringen främja en ökad användning av molntjänster i den offentliga förvaltningen. Molntjänster sågs som ett sätt att effektivisera förvaltningen genom att ersätta egenutvecklade lösningar med mer standardiserade sådana. Regeringen hade identifierat att förvaltningen var inlåst i stora kontrakt med ett fåtal leverantörer, med höga it-kostnader som konsekvens.[27] Reger-

[25] Storbritanniens regering (2011a) Government ICT Strategy.
[26] Storbritanniens regering (2012) Government Digital Strategy, (2016) National Cyber Security Strategy, (2017a) Government Transformation Strategy, (2017b) UK Digital Strategy. Även riksdelarna Wales, Nordirland och Skottland har sina egna strategier på e-förvaltningsområdet.
[27] Storbritanniens regering (2013a).

ingen bedömde även att det fanns ett motstånd till att använda molntjänster och att det även hade byggts upp många mindre datacenter i förvaltningen med lågt resursutnyttjande.[28] Genom att etablera en marknadsplats för molntjänster avsåg regeringen att främja bättre villkor och minskad inlåsning samtidigt som den skulle stimulera små- och medelstora företag i Storbritannien som kunde sälja tjänster till den offentliga förvaltningen.[29] I sin molntjänststrategi för år 2011 uppskattade regeringen att det skulle gå att spara sammanlagt 340 miljoner brittiska pund under åren 2011–2015 genom satsningar på upphandlingsstöd för molntjänster och datacenterkonsolidering.[30]

Cloud First

För att stimulera en ökad användning av molntjänster beslutade den brittiska regeringen år 2013 att publika molntjänster i första hand ska övervägas när verksamheter upphandlar nya eller ersätter befintliga it-tjänster. Principen benämndes Cloud First. Vid avsteg från principen, där den är relevant, behöver den upphandlande verksamheten motivera att den valda lösningen är mer kostnadseffektiv.[31] Beslutet gäller endast statsförvaltningen men regeringen har rekommenderat övriga delar av förvaltningen att också tillämpa principen. Principen omprövades 2019 och kvarstår, dock nyanserades den för att understryka att molntjänster inte passar alla behov och inte alltid leder till lägst kostnader.[32] Cloud First-principen är del av regeringens Technology Code of Practice – en samling principer som ska hjälpa förvaltningen att designa, bygga och köpa ny teknik. Statliga verksamheter kan behöva ansöka om tillstånd från GDS för att spendera pengar i teknikprojekt varvid GDS bedömer om projektet följer Technology Code of Practice.[33]

[28] Storbritanniens regering (2011b).
[29] Computer Weekly (2019) *Government 'cloud-first' policy under review by CCS and GDS.*
[30] Storbritanniens regering (2011b).
[31] Storbritanniens regering (2013b).
[32] Government Digital Services (2019a).
[33] Storbritanniens regering (2019a).

G-Cloud

En annan del av satsningen på molntjänster var lanseringen av G-Cloud, ett upphandlingsstöd för molntjänster. G-Cloud består av ramavtal, från vilka förvaltningen kan avropa olika typer av it-tjänster, samt en digital marknadsplats som samlar information om leverantörerna och deras tjänster. Alla organisationer inom den offentliga förvaltningen, inklusive offentligfinansierade verksamheter (eng. arm's length bodies), har möjlighet att göra avrop från ramavtalen.[34] Sedan G-Cloud lanserades år 2012 har ramavtalen förnyats i flera omgångar och i skrivande stund är version 11 den senaste där tecknade kontrakt får löpa 12 månader med möjlighet till förlängning ytterligare maximalt 12 månader. För att ansluta sig till ramavtalen genomgår leverantörer ackreditering och svarar på frågor om bl.a. villkor för användning, säkerhet, certifieringar, prissättning. Från och med version 9 av G-Cloud delades erbjudna tjänster in i de tre kategorierna: Cloud Hosting (IaaS och PaaS), Cloud Software (SaaS) och Cloud Support (stöd med migration till molntjänster). På den digitala marknadsplatsen finns numera även egna ramavtal för it-specialister (Digital Outcomes and Specialists) och datacentertjänster (Crown Hosting).

Från lanseringen av det första versionen av G-Cloud till och med den 31 december 2018 har ramavtalen för molntjänster genererat en försäljning om 4 miljarder GBP. Av denna försäljning svarar små- och medelstora företag (SMF) för cirka 45 procent. 81 procent av försäljningen har varit till statsförvaltningen medan 19 procent till övriga delar av den offentliga förvaltningen.[35] De små och medelstora företagens andel av försäljningen har dock minskat över tid.

Antalet leverantörer och tjänster på den digitala marknadsplatsen som säljs genom G-Cloud är i dag omfattande. På ramavtalet för G-Cloud version 11 finns cirka 4 200 leverantörer och 31 000 annonserade tjänster. Allt fler offentliga verksamheter, som t.ex. vårdorganisationen NHS, har dock upprättat egna ramavtal för molntjänster sedan G-Cloud:s tillkomst. Enligt vissa bedömare är anledningen till denna utveckling att alla behov inte kunnat tillgodoses av G-Cloud. Vissa nya ramavtal har exempelvis längre avtalstider och ger möjlighet att avropa flera tjänster, såsom co-location och hosting, på

[34] Storbritanniens regering (2019b).
[35] Storbritanniens regering (2019c).

samma avtal. Det finns samtidigt de som varnar för att nya ramavtal driver försäljning från G-Cloud till nackdel för små och medelstora företag som inte har möjlighet att delta på flera ramavtal.[36]

Det finns många vägledningar och stöd tillgängliga för offentliga verksamheter som avser att avropa molntjänster på den digitala marknadsplatsen och GDS:s webbplats. I en vägledning37 om molntjänster publicerad år 2020 föreslås att alla statliga organisationer tar fram egna molntjänststrategier som bl.a. belyser om organisationen bör ha en eller flera leverantörer, vilken påverkan verksamhetens teknikskuld har på denna strategi samt risker för inlåsning och informationssäkerhet.

5.6.3 Datacenter

År 2010 fanns ungefär 220 datacenter inom den brittiska statsförvaltningen och sannolikt ytterligare hundratals i den övriga förvaltningen. Detta enligt en enkätundersökning från samma år.[38] Den dåvarande regeringen konstaterade att dessa datacenter användes ineffektivt och beslutade att offentliga datacenter skulle konsolideras och minska i antal.[39] År 2014 etablerade regeringen samriskföretaget (joint venture) Crown Hosting Data Centres Limited (Crown Hosting) tillsammans med leverantören Ark Data Centres Limited. Ett nytt ramavtal upprättades även år 2015 med Crown Hosting som enda leverantör. Avrop från ramavtalet kan löpa i maximalt sju år. Företrädare på Crown Hosting menar att syftet med denna modell är att göra det möjligt för offentliga verksamheter att ta steget till att utkontraktera it-drift, även i de fall det finns system och lösningar som av olika skäl inte kan migreras till publika molntjänster, t.ex. på grund av teknikskuld eller speciella krav på informationssäkerhet.[40] Crown Hosting blev därmed ett viktigt komplement till regeringens Cloud First-policy. I dag använder bl.a. Department of Work and Pension, Home Office och Highways Agency tjänsterna.[41]

[36] Computer Weekly (2019b) *G-Cloud 11 goes live with 4,200 suppliers securing a place on the framework*; (2016) *The Problem With G-Cloud*; (2019c) *Competitive threats: What the growth in new public sector cloud frameworks means for G-Cloud.*
[37] Government Digital Services (2019b).
[38] Storbritanniens regering (2010).
[39] Storbritanniens regering (2011b).
[40] Public Technology (2018) *Crown Hosting CEO: We have taken away all the cloud excuses.*
[41] Storbritanniens regering (2019d).

5.6.4 Informations- och cybersäkerhet

I Storbritannien har Cabinet Office en samordnande roll inom it-säkerhet, även om varje departement ansvarar för it-säkerhet inom sitt eget sakområde. Cyber and Government Security Directorate (CGSD) är en del av Cabinet Office och rådgivande i samband med prioriteringar och strategisk inriktning för it-säkerhetsarbetet. CGSD samordnar det nationella cybersäkerhetsprogrammet (NCSP) och ansvarar för den nationella it-säkerhetsstrategin. National Cyber Security Center (NCSC) grundades år 2016 och är en del av underrättelses- och säkerhetsorganisationen Government Communications Headquarters (GCHQ). NCSC ger råd och vägledning och hanterar incidenter samt CERT-funktionen i Storbritannien. Bakgrunden till inrättandet av NCSC var en önskan om bättre samordning och entydig vägledning till myndigheterna i it-säkerhetsfrågor. Centret har nära samarbete med näringslivet och cirka 100 anställda sekonderade i näringsliv och offentlig sektor.

Storbritannien har i liten utsträckning lagstadgade krav på it-säkerhet annat än sådant som följer implementation av EU-direktiv och förordning. Regeringen har tagit fram en policy för informationsklassificering (Government Security Classification Policy) som den offentliga förvaltningen är skyldig att följa. Policyn delar upp informationstillgångar i tre skyddsklasser (OFFICIAL, SECRET och TOP SECRET) med tillhörande krav på tekniska och organisatoriska skyddsåtgärder. Vidare har NCSC tagit fram en vägledning för användning av molntjänster som baseras på följande 14 principer:

1. Säker dataöverföring (”Data in transit protection”); kundens data bör skyddas mot avlyssning och manipulation (konfidentialitet och integritet) genom en kombination av skydd av nätverk och kryptering.
2. Skydd av enheter för lagring och bearbetning av data (”Asset protection and resilience”); de enheter som lagrar och bearbetar kundens data bör skyddas mot fysisk manipulation, skada eller obehörig tillgång.
3. Separering av kunddata (”Separation between consumers”); kunders data bör separeras på så sätt att en kund inte kan manipulera eller få tillgång till en annan kunds data (konfidentialitet och integritet).

4. Ramverk för styrning av informationssäkerhet (”Governance framework”); Leverantören bör ha ett ramverk för styrning av informationssäkerhet.
5. Driftsäkerhet (”Operational security”); leverantören ska ha processer och procedurer för operativ säkerhet.
6. Screening av personal (”Personal security”); leverantörens personal bör ha genomgått screening och säkerhetsutbildning för sin roll.
7. Säker utveckling (”Secure development”); leverantörens tjänster bör utvecklas genom att hot och sårbarheter identifieras och åtgärdas.
8. Säkerhet i försörjningskedjan (”Supply chain security”); leverantörens försörjningskedja bör efterleva principerna och på det sätt leverantören kommunicerat.
9. Identifiering och autentisering av användare (”Identify and authentication”); tillgång till alla tjänstegränssnitt ska begränsas till autentiserade och auktoriserad användare.
10. Verktyg till kunder (”Secure consumer management”); kunder bör förses med verktyg för att säkert hantera sina tillgångar.
11. Säkerhet i tjänstens externa gränssnitt (”External interface protection”); Alla externa eller mindre betrodda gränssnitt i tjänsten ska identifieras och ha lämpligt skydd mot attacker.
12. Säker administration av tjänsten (”Secure service administration”); Verktyg och metoder leverantören använder för att administrera tjänsten ska härdas för att undvika att de utnyttjas.
13. Tillgång till revisionshistorik av tjänsten (”Audit information provision to consumers”); Information från tidigare revisioner och granskningar av tjänsten ska finnas tillgängliga för kunden.
14. Kundens ansvar för sin egen säkerhet (”Secure use of the service by the consumer”); Kunden har visst ansvar för att skydda sin egen data och för att motverka säkerhetsbrister genom eget handhavande.

Leverantörer till den offentliga förvaltningen uppmanas att svara på hur de uppfyller dessa principer samt välja hur de kan valideras av upphandlande verksamheter. Det finns sex valideringssätt, däribland egen försäkran, försäkran genom avtal, samt tredje parts-validering.

5.7 Internationella initiativ inom EU

5.7.1 GAIA-X

Gaia-X är ett initiativ som lanserades av Tyskland och Frankrike i samarbete år 2019 i syfte att etablera en federerad data-infrastruktur för EU. Sedan lanseringen har ytterligare länder deklarerat sitt intresse att ansluta sig till initiativet och en stiftelse har upprättats för att leda initiativet där flera företag ingår, bl.a. 3DS OUTSCALE, Amadeus, Atos, Beckhoff Automation, BMW, Bosch, CISPE, DE-CIX, Deutsche Telekom, DOCAPOSTE, EDF, Fraunhofer, GEC/Loh Group, IDS Association, IMT, Orange, OVHcloud, PlusServer, Safran, SAP, Scaleway och Siemens. Även EU-kommissionen har hänvisat till initiativet i sin datastrategi.[42]

Enligt grundarna till GAIA-X ska initiativet leda till ett öppet ekosystem av europeiska molntjänstleverantörer som kan stärka EU:s konkurrenskraft, möjliggöra digital suveränitet bland molntjänst-användare i EU samt underlätta för europeiska företag att skala upp. Den tekniska implementationen ska fokusera på att

- Implementera en säker federerad och identitetsmekanism,
- Suveräna datatjänster som säkerställer dataintegritet och identitet hos avsändare och mottagare av data,
- Tillgänglighet bland leverantörer, noder och tjänster genom federerade kataloger,
- Integration av befintliga standarder för att säkerställa interoperabilitet och portabilitet över infrastruktur, applikation och data,
- Ett compliance-ramverk och certifiering och ackrediteringstjänster,
- Bidrag till öppen mjukvara och standarder som kan stödja den federerade infrastrukturen.

Initiativet är indelat i de två arbetsströmmarna ekosystem och krav hos användare samt teknisk implementation. I den första arbetsströmmen arbetar användare med att implementera projekt inom sina respektive sektorer. I arbetsströmmen för teknisk implementation arbetar olika grupper med arkitektur, tekniska definitioner och beskrivningar av funktionaliteten i den federerade infrastruk-

[42] EU-kommissionen (2020).

turen. Det finns även en tvärgående arbetsström som arbetar med samordning mellan grupperna där det uppstår behov.[43]

GAIA-X har tydliga kopplingar till det initiativ om en europeisk molntjänstfederation (se nedan avsnitt 5.7.2) som tas upp i kommissionens meddelande från mars 2020 om en europeiska datastrategi (COM/2020/66 final). Det finns även kopplingar till det arbete som bedrivs av ENISA avseende cybersäkerhetscertifiering av molntjänster inom ramen för Europaparlamentets och rådets förordning (EU) 2019/881.[44]

Regeringen uppdrog åt Skatteverket i september 2020 att bevaka GAIA-X genom att delta i de arbetsgrupper och sammanhang som bedöms vara mest relevanta för att säkerställa en god insyn i projektet och tillvarata den offentliga förvaltningens och det privata näringslivets intressen och behov. Uppdraget ska redovisas senast den 30 juni 2021.

5.7.2 Europeiska molntjänstfederationen för offentlig förvaltning

År 2019 lanserade EU-kommissionen ett initiativ för att främja en europeisk molntjänstfederationen som syftar till att skapa nästa generations säkra, energieffektiva och interoperabla molntjänster i Europa. I en politisk deklaration[45] om molntjänster som antogs av Sverige och andra medlemsländer den 15 oktober 2020 framhålls att nyttjandegraden av molntjänster bland europeiska företag och offentlig sektor är låg. Deklarationen lyfter fram utmaningarna med att ett fåtal icke-europeiska aktörer kommit att dominera marknaden för molntjänster och att bristen på interoperabilitet skapar risker för leverantörsinlåsning. För att möta dessa utmaningar åtar sig signatärerna, inklusive EU-kommissionen, att

– Investera i ny infrastruktur för molntjänster för offentlig förvaltning,
– definiera gemensamma spelregler för dessa typer av tjänster, och

[43] GAIA-X (2020).
[44] Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten).
[45] EU-deklaration om molntjänster (2020).

– att främja en utökad förmåga till säker och energieffektiv databearbetning i små- och medelstora företag och offentlig sektor.

Initiativet om en europeisk molntjänstfederation förväntas skapa synergier med andra initiativ, såsom GAIA-X.

EU-kommissionen bjöd i sin datastrategi in medlemsländerna att saminvestera med kommissionen i en molntjänstfederation och i gemensamma datautrymmen. EU-kommissionens mål är att investera 2 miljarder euro inom detta område perioden 2021–2027 med mål om samlade investeringar som uppgår till 10 miljarder euro.

5.8 Jämförelse och diskussion

I jämförelse med tidigare internationella utblickar kan vi konstatera att de trender som tidigare beskrivits till viss del består. Nedan beskrivs dessa trender som två olika strategier som de studerade länderna har tillämpat med avseende på styrningen av sina offentliga verksamheters digitalisering.

Statens IT i Danmark, Valtori i Finland och SSC-IT i Nederländerna är exempel på strategin att koncentrera upphandling, processer och resurser som gäller statens it-verksamhet, däribland it-driftstjänster, till statliga servicecenter. Storbritannien och Norge har valt en annan strategi med fokus på att skapa stöd för myndigheterna att på egen hand upphandla molntjänster och driftsrelaterade tjänster. I sammanhanget bör det poängteras att Norge först nyligen valt att inrätta en digital marknadsplats inspirerad av G-Cloud i Storbritannien.

De två strategierna bör dock inte ses som ömsesidigt uteslutande. T.ex. har både Danmark och Norge officiella vägledningar för molntjänster i offentlig förvaltning (författade av Digitaliseringsstyrelsen respektive regeringen). Att strategierna överlappar varandra kan ses i ljuset av att satsningarna på servicecenter i Danmark, Finland och Nederländerna inte varit avgränsade till att enbart tillhandahålla it-drift, eller att det funnits en uttalad ambition om att ersätta alla kommersiella molntjänster statsförvaltningen använder med tjänster producerade av statliga servicecenter. Företrädare för de studerade länderna ger i dag uttryck för att de två strategierna bör komplettera varandra – myndigheter behöver själva kunna upphandla molntjänster utifrån egna behov, samtidigt som staten ur ett koncernperspektiv

behöver koncentrera och konsolidera viss it-verksamhet i syfte att höja effektiviteten eller säkerheten.

5.8.1 Effektivitet och motiv till reformer

Reformer och satsningar, vare sig de gällt servicecenter eller digitala marknadsplatser för molntjänster, har motiverats på flera olika sätt. Offentliga besparingar har lyfts fram som den huvudsakliga anledningen till satsningarna i flera av länderna.

Som exempel uppskattade Storbritannien i sin molntjänststrategi från år 2011 att G-Cloud skulle leda till besparingar om 340 miljoner brittiska pund under perioden 2011–2015 (från G-Cloud och datacenterkonsolidering).[46] Någon utvärdering har dock inte gjorts expost för att uppskatta vilka besparingar som faktiskt har uppnåtts. GDS framhåller nu i efterhand att de bedömer att de primära nyttorna med en ökad molntjänstanvändning främst har varit en moderniserad driftsmiljö och förbättrad skalbarhet i offentliga digitala tjänster. Till exempel har den ökade efterfrågan på vissa offentliga digitala tjänster under coronapandemin inte varit möjlig att hantera utan skalbarheten i molntjänster. Det finns dock specifika exempel på verksamheter som sänkt sina kostnader. Exempelvis har den verksamhet som arbetar med migrationsfrågor på Inrikesdepartementet (Home Office) lyckats sänka sina kostnader med 40 procent. Besparingen uppstod som en konsekvens av optimerad användning av de molntjänster departementet redan tidigare använde.[47] Det går med andra ord inte att säga att besparingen uppstod till följd av övergång från egen drift till molntjänster.

Norge har bedömt att det finns stora samhällsekonomiska vinster med att införa en marknadsplats för molntjänster. Dessa besparingar avser perioden under åren 2019–2029 och arbetet med att etablera själva marknadsplatsen pågår för närvarande. Företrädare på Digidir i Norge understryker att den nuvarande molntjänststrategin både syftar till att effektivisera och att skapa bättre förutsättningar för innovation.

[46] Storbritanniens regering (2011b).
[47] Storbritanniens regering (2019e).

Digitaliseringsstyrelsen i Danmark framhåller att potentialen i att koncentrera viss it-verksamhet till Statens IT, samt av ökad användning av kommersiella molntjänster, först och främst har varit bättre förutsättningar att utveckla nya tjänster och lösningar. Den privata molntjänst Statens IT planerar att etablera under 2020 (GovCloud) motiveras på flera olika sätt såsom lägre kostnader, förenklad hanteringen av dataskydd, men även att kunna bibehålla och stärka viss teknisk kompetens inom staten. Digitaliseringsstyrelsen betonar också att användning av kommersiella molntjänster inte utan vidare leder till lägst kostnader.

I Nederländerna och Finland har revisionsmyndigheter i de båda länderna granskat satsningarna på att koncentrera resurser, upphandlingar och processer avseende it till servicecenter. Det reformprogram som låg till grund för SSC-IT i Nederländerna syftade till att konsolidera antalet datacenter i statsförvaltningen för att minska kostnader. Riksrevisionen i Nederländerna har dock konstaterat att fördelarna med reformen ännu inte är tydliga. Det bör även betonas att granskningen inte specifikt fokuserat på it-drift. Företrädare på ODC-Noord i Nederländerna framhåller att inrättandet av statliga datacenter skapat bättre förutsättningar för en säker och hållbar digitalisering i statsförvaltningen.

I Finland har Statens Revisionsverk granskat reformen bakom Valtori men har inte kunnat påvisa tydliga kostnadsbesparingar till följd av effektiviserad it-drift. Det finländska Finansdepartementet tillstod visserligen att erbjudna driftstjänster var dyrare än på marknaden, vilket Revisionsverkets granskning visat, men att skillnaden delvis kunde förklaras med att Valtori har högre kostnader för säkerhetsskydd i jämförelse med privata tjänsteleverantörer.

Länderna i omvärldsanalysen har belyst flera andra nyttor än kostnadsbesparingar med de genomförda reformerna, däribland

– att ökad användning av kommersiella molntjänster (som alternativ till it-drift i egen regi) samt konsolidering av offentliga datacenter sannolikt leder till lägre elförbrukning,
– att det råder brist på nyckelkompetenser inom it i förvaltningen och att åtgärder för att underlätta upphandling av molntjänster, alternativt för att bygga upp servicecenter med åtagande för it-drift, gör att förvaltningarna kan dra nytta av kompetens från

näringslivet respektive vidmakthålla och stärka relevant kompetens inom förvaltningen,

– att servicecenter, men även marknadsplatser med förkvalificerade molntjänstleverantörer, skapar effektiva förutsättningar att ställa krav på leverantörer.

Sammanfattningsvis skiljer sig beskrivningen av målen för satsningarna åt i de studerade länderna före respektive efter att de har genomförts. Vissa skillnader beror sannolikt på vem som tillfrågats och möjligheten för intervjuade att nyansera bakgrunden till satsningarna, jämfört med hur målen för satsningarna ursprungligen formulerats i strategier och politisk kommunikation.

För Danmark, Finland och Nederländerna ligger resultatet i linje med forskning om Shared Service Centers i OECD-länder som visar att servicecenter etablerades i flera länder för att åstadkomma kostnadsbesparingar. I efterhand har dock andra nyttor, som t.ex. förbättrad leveranskvalitet lyfts fram när det varit svårt att påvisa kostnadsbesparingar.[48]

Sammanfattningsvis kan vi konstatera att det har visat sig svårt att påvisa kostnadsbesparingar till följd av genomförda satsningar och reformer i de studerade länderna. Detta beror delvis på metodproblem då flera av länderna inte genomfört utvärderingar före (och) eller efter satsningarna, varför det inte går att säga något om kostnadsutvecklingen. Till metodproblemet hör även att den producerade varans (it-drift) karaktär och de offentliga verksamheternas behov förändrats över tid, vilket gör det svårt att följa dess kostnadsutveckling över tid. Flera av länderna har dock identifierat andra kvalitativa nyttor med de satsningar som genomförts, som förbättrade förutsättningar till digital utveckling, underlättad kompetensförsörjning och kravställning på leverantörer vilket lett till bättre informationssäkerhet och kvalitet.

Två viktiga slutsatser är även att de beskrivna strategierna utgör komplement till varandra samt att flera av länderna betonar vikten av att börja smått och med standardiserade lösningar för att lyckas med en samordnad statlig it-drift.

[48] Paagman A m.fl. (2015).

5.8.2 Informations- och cybersäkerhet

De studerade ländernas informations- och cybersäkerhetsstrategier syftar på en övergripande nivå till att främja ett riskbaserat arbetssätt. Eftersom privata aktörer både svarar för många samhällsviktiga funktioner och offentlig förvaltning är beroende av it-tjänster och produkter från privat sektor, behöver informations- och cybersäkerhetsarbete bedrivas i offentlig-privat samverkan, vilket ländernas strategier ger uttryck för.

Sett till organiseringen hanteras frågor om informations- och cybersäkerhet av olika departement i de studerade länderna. I Nederländerna och Norge är Justitie- och säkerhetsdepartementet respektive Justitiedepartementet ansvarigt, i Danmark Försvarsdepartementet, i Finland Kommunikationsdepartementet och i Storbritannien Statsrådsberedningen (Cabinet Office). Det bör dock poängteras att frågorna i praktiken även hanteras på andra departement då de överlappar med andra politikområden.

I takt med att it- och cybersäkerhetsfrågor fått allt större betydelse har verksamheter som arbetar med frågorna i förvaltningarna konsoliderats till särskilda myndigheter. Danmark inrättade Center for Cybersikkerhed år 2012 (CFCS), Nederländerna inrättade NCSC år 2012 och Storbritannien inrättade ett center med samma namn år 2016. I Finland ligger det samordnande ansvaret för it-säkerhetsfrågor på NCSC-FI, som är del av Kommunikationsverket. I Norge ligger samordningsansvaret på Nasjonalt cybersikkerhetssenter som är del av den nationella säkerhetsmyndigheten som etablerades år 2018. Trenden mot nationellt utpekade myndigheter och center med ansvar för it- och cybersäkerhet har sannolikt drivits av behovet att underlätta samverkan samt av krav på utpekade kontaktpunkter i enlighet med NIS-direktivet.

Samtliga intervjuade i omvärldsanalysen lyfter en liknande problematik med osäkerhet avseende de rättsliga förutsättningarna för utkontraktering av it-verksamhet. Ingen av länderna har i dag generella förbud för sina offentliga verksamheter mot att utkontraktera it-drift eller att använda sig av publika molntjänster. I takt med att osäkerheten blivit problematisk har flera av länderna agerat inom befintliga strukturer och regelverk. Exempelvis håller Statens IT i Danmark på att lansera GovCloud (delvis motiverat med underlättad personuppgiftshantering). Norge har genomlyst lagstiftning som på-

verkar möjligheter att lagra och bearbeta data utanför Norge och Nederländerna har på departementsnivå förhandlat med Microsoft i dataskyddsfrågor.

Det är möjligt att koncentreringen av resurser, upphandlingar och processer till servicecenter i Danmark, Finland och Nederländerna gör det möjligt att koncentrera kompetens inom informations- och cybersäkerhet, samt att samordna it-säkerhetsrelaterade krav vid upphandling och utveckling, på ett mer effektivt sätt än vad som annars vore möjligt. Även digitala marknadsplatser, som ställer omfattande krav på leverantörer på ett sätt som är svårt för alla enskilda myndigheter att göra, kan sannolikt stärka informations- och cybersäkerheten.

Det finns risker förknippade med båda strategierna. Om ett servicecenter har sårbarheter till följd av tekniska eller organisatoriska brister, samt saknar logisk eller fysisk separation av resurser för olika verksamheter, kan dessa sårbarheter drabba flera verksamheter. Som exempel kritiserade Rigsrevisionen i Danmark år 2019 Statens IT för att inte vara tillräckligt restriktiv med de behörigheter myndigheten tilldelat sina anställda vilket gjort att anställda fått onödigt omfattande tillgång till olika system.

6 Säkerhetsskydd och informationssäkerhet

6.1 Inledning

Syftet med detta kapitel är att kartlägga de rättsliga förutsättningarna för myndigheters[1] utkontraktering av it-drift till privata tjänsteleverantörer utifrån regelverken om säkerhetsskydd och informationssäkerhet. Framställningen är främst beskrivande och inriktad på de delar av regelverken som är av särskild relevans vid utkontraktering av it-drift till privata tjänsteleverantörer. Båda regelverken måste givetvis följas i sin helhet vid all informationshantering som berörs av respektive regelverk.

Kapitlet inleds med en genomgång av relevanta bestämmelser i säkerhetsskyddsregleringen. Därefter följer en redogörelse för relevanta delar av informationssäkerhetsregelverket.

6.2 Säkerhetsskyddsregleringen

6.2.1 Inledning

Bestämmelser om säkerhetsskydd finns i säkerhetsskyddslagen (2018:585) och säkerhetsskyddsförordningen (2018:658). Säkerhetspolisens föreskrifter om säkerhetsskydd (PMFS 2019:2), Försvarsmaktens föreskrifter om säkerhetsskydd (FFS 2019:2), Transportstyrelsens föreskrifter om säkerhetsskydd (TSFS 2019:108), Affärsverket svenska kraftnäts föreskrifter om säkerhetsskydd (SvKFS 2019:1) och Försvarsmaktens föreskrifter om signalskyddstjänsten (FFS 2019:9) inne-

[1] Med myndigheter avses i detta kapitel statliga myndigheter, kommuner och regioner om inget annat framgår av sammanhanget.

håller mer detaljerade bestämmelser som kompletterar lagen och förordningen.

För riksdagen och dess myndigheter gäller säkerhetsskyddslagen med vissa begränsningar. Dessutom finns bestämmelser i lagen (2019:109) om säkerhetsskydd i riksdagen och dess myndigheter. Vi ska enligt våra direktiv kartlägga de rättsliga förutsättningarna för statliga myndigheters, kommuners och regioners utkontraktering av it-drift. De regler om säkerhetsskydd som gäller för riksdagens och dess myndigheters utkontraktering av it-drift behandlas därför inte i det följande.

Den följande genomgången tar utgångspunkt i säkerhetsskyddslagen och säkerhetsskyddsförordningen. Relevanta bestämmelser i Säkerhetspolisens respektive Försvarsmaktens föreskrifter berörs också, eftersom det är dessa föreskrifter som är av huvudsaklig relevans för statliga myndigheters, kommuners och regioners utkontraktering av it-drift.

6.2.2 Säkerhetsskyddets tillämpningsområde

Säkerhetsskyddslagen gäller för den som bedriver säkerhetskänslig verksamhet, dvs. verksamhet som är av betydelse för Sveriges säkerhet eller som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd – oavsett om verksamheten bedrivs i offentlig eller privat regi (1 kap. 1 § säkerhetsskyddslagen). Uttrycket *Sveriges säkerhet* tar sikte på förhållanden av grundläggande betydelse för Sverige. Det innebär att lagens krav på säkerhetsskydd gäller för såväl militär som civil verksamhet.

Vilka verksamheter som är av betydelse för att upprätthålla Sveriges säkerhet måste bedömas i ljuset av samhällsutvecklingen. Tidigare var uttrycket starkt förknippat med Försvarsmaktens verksamhet, eftersom det främsta hotet mot rikets säkerhet ansågs vara ett militärt angrepp. I dag är samhället och hotbilden mer komplex och föränderlig, vilket har fört med sig att uppgifter som rör förhållanden inom andra samhällssektorer också kan vara av betydelse för den nationella säkerheten. Det kan exempelvis gälla uppgifter om viktig civil infrastruktur som flygplatser, energianläggningar och förmedlingsstationer för telekommunikation (prop. 2017/18:89, s. 133). Med säkerhetsskydd avses skydd av säkerhetskänslig verksamhet mot spionerі, sabotage, terroristbrott och andra brott som kan hota

verksamheten samt skydd i andra fall av säkerhetsskyddsklassificerade uppgifter (1 kap. 2 § första stycket säkerhetsskyddslagen).

Med säkerhetsskyddsklassificerade uppgifter avses sådana uppgifter som rör säkerhetskänslig verksamhet och som därför omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400) (OSL) eller som skulle ha omfattats av sekretess enligt den lagen, om den hade varit tillämplig (enligt 1 kap. 2 § andra stycket säkerhetsskyddslagen). I specialmotivering till paragrafen anges bestämmelserna om försvarssekretess enligt 15 kap. 2 § OSL, sekretess i underrättelseverksamhet enligt 18 kap. 2 § OSL, utrikessekretess enligt 15 kap. 1 § OSL, sekretess i det internationella samarbetet enligt 15 kap. 1 a § OSL och bestämmelsen om förundersökningssekretess i 18 kap. 1 § OSL som sekretessbestämmelser som kan vara tillämpliga på den typen av uppgifter som omfattas av krav på säkerhetsskydd. Säkerhetspolisen anger dessutom i sin vägledning om säkerhetsskydd *Introduktion till säkerhetsskydd* (2019) att bestämmelsen i 18 kap. 8 § om sekretess för säkerhets- och bevakningsåtgärd som möjligt relevant för bedömningen av om en uppgift ska vara säkerhetskyddsklassificerad.

Säkerhetsskyddsklassificerade uppgifter ska delas in i följande säkerhetsskyddsklasser utifrån den skada som ett röjande av uppgiften kan medföra för Sveriges säkerhet: kvalificerat hemlig vid en synnerligen allvarlig skada, hemlig vid en allvarlig skada, konfidentiell vid en inte obetydlig skada, eller begränsat hemlig vid endast ringa skada (2 kap. 5 § första stycket säkerhetsskyddslagen).

I 3 kap. i PMFS 2019:2 och i 3 kap. i FFS 2019:2 finns bestämmelser om hantering av säkerhetsskyddsklassificerade uppgifter och handlingar.

6.2.3 Säkerhetsskyddsanalys

En säkerhetsskyddsanalys utgör grunden för säkerhetsskyddsarbetet. Av säkerhetsskyddsanalysen ska det framgå vilka delar av verksamheten som är säkerhetskänslig och ur vilket perspektiv. När säkerhetsskyddsanalysen är fastställd ska verksamhetsutövaren upprätta en säkerhetsskyddsplan av vilken det ska framgå vilka säkerhetsskyddsåtgärder som ska vidtas. Analysen och säkerhetsskyddsplanen är därför viktiga dokument när verksamhetsutövaren ska bedöma

om en utkontraktering är möjlig eller ens lämplig. Av säkerhetsskyddsregelverket framgår följande rörande säkerhetsskyddsanalys.

Den som bedriver säkerhetskänslig verksamhet ska utreda och dokumentera behovet av säkerhetsskydd genom en s.k. säkerhetsskyddsanalys (2 kap. 1 § första stycket säkerhetsskyddslagen). Av specialmotiveringen till bestämmelsen framgår att om verksamhetsutövaren är osäker på om och i vilken utsträckning verksamheten till någon del omfattas av lagen bör en analys göras för att få svar på den frågan (prop. 2017/18:89, s. 137).

Verksamhetsutövaren ska med utgångspunkt i analysen planera och vidta de säkerhetsskyddsåtgärder som behövs med hänsyn till verksamhetens art och omfattning, förekomsten av säkerhetsskyddsklassificerade uppgifter och övriga omständigheter (2 kap. 1 § andra stycket säkerhetsskyddslagen).

I 2 kap. 1 § andra stycket säkerhetsskyddsförordningen preciseras följande avseende säkerhetsskyddsanalysen. Säkerhetsskyddsanalysen innebär att säkerhetsskyddsklassificerade uppgifter och vad som i övrigt behöver ett säkerhetsskydd ska identifieras. Vilka delar av verksamheten som är skyddsvärda med hänsyn till Sveriges säkerhet samt vilka hot och sårbarheter som finns kopplade till detta skyddsvärde ska också identifieras. Säkerhetsskyddsanalysen ska även innehålla en bedömning av vilka säkerhetsskyddsåtgärder som är nödvändiga. Analysen ska hållas uppdaterad.

I Säkerhetspolisens föreskrifter om säkerhetsskydd anges bl.a. följande rörande säkerhetsskyddsanalysen. En säkerhetsskyddsanalys ska identifiera vilka skyddsvärden som finns i verksamheten, dvs. säkerhetsskyddsklassificerade uppgifter och den totala mängden sådana uppgifter som finns i verksamheten, vilka för Sverige förpliktande internationella åtaganden om säkerhetsskydd som finns i verksamheten, och vilken säkerhetskänslig verksamhet i övrigt som finns i verksamheten (2 kap. 1 § i PMFS 2019:2). Verksamhetsutövaren ska bedöma från vilket eller vilka perspektiv (konfidentialitet, tillgänglighet eller riktighet) den identifierade säkerhetskänsliga verksamheten är skyddsvärd (2 kap. 4 § PMFS 2019:2). Verksamhetsutövaren ska också utifrån hotbilden och egna identifierade hot bedöma hur hoten kan påverka den säkerhetskänsliga verksamheten och om det finns behov av att vidta säkerhetsskyddsåtgärder (2 kap. 7 § andra stycket PMFS 2019:2). Verksamhetsutövaren ska vidare göra sårbarhetsbedömningar beträffande den säkerhetskänsliga verk-

samheten. I säkerhetsskyddsanalysen ska det anges vilka övergripande sårbarheter som har identifierats. Verksamhetsutövaren ska därefter bedöma hur sårbarheterna påverkar verksamhetens säkerhetsskydd och om det finns behov av att vidta säkerhetsskyddsåtgärder (2 kap. 9 § PMFS 2019:2).

Beslut att fastställa säkerhetsskyddsanalysen fattas av verksamhetsutövarens högsta chef eller motsvarande organ, eller den som sådan chef eller sådant organ bestämmer. Säkerhetsskyddsanalysen ska uppdateras vid behov, dock minst en gång vartannat år (2 kap. 10 § PMFS 2019:2). När säkerhetsskyddsanalysen är fastställd ska verksamhetsutövaren upprätta en säkerhetsskyddsplan där det framgår vilka säkerhetsskyddsåtgärder som ska vidtas. Planen ska fastställas av säkerhetsskyddschefen eller den han eller hon bestämmer (2 kap. 11 § PMFS 2019:2).

I Försvarsmaktens föreskrifter om säkerhetsskydd anges att en säkerhetsskyddsanalys ska innehålla en beskrivning av myndighetens verksamhet och organisation samt dess skyddsvärden (verksamhetsbeskrivning) (2 kap. 3 § FFS 2019:2).

Med säkerhetsskyddsanalysen som grund ska myndigheten upprätta en säkerhetsskyddsplan. Av planen ska framgå vilka säkerhetsskyddsåtgärder som ska vidtas, vem som har ansvaret och när respektive åtgärd ska vara genomförd. Behov av resurser, ansvarsfördelning, organisation, utbildning, övning samt rutiner och bestämmelser ska särskilt framgå. Säkerhetsskyddsplanen ska även beskriva vilka åtgärder som behöver vidtas inför, under eller efter sådana avbrott och störningar i myndighetens säkerhetskänsliga verksamhet som kan medföra mer än ringa skada (2 kap. 4 § FFS 2019:2).

Myndighetens ledning ska orienteras innan myndighetens säkerhetsskyddsanalys och säkerhetsskyddsplan beslutas (2 kap. 5 § FFS 2019:2).

6.2.4 Säkerhetsskyddsavtal

Hur säkerhetsskyddet ska hanteras vid en utkontraktering regleras i bestämmelserna om säkerhetsskyddsavtal.

Myndigheter som avser att genomföra en upphandling och ingå ett avtal om varor, tjänster eller byggentreprenader ska se till att det i ett säkerhetsskyddsavtal anges hur kraven på säkerhetsskydd ska tillgodoses av leverantören om det i upphandlingen förekommer

säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen konfidentiell eller högre, eller upphandlingen i övrigt avser eller ger leverantören tillgång till säkerhetskänslig verksamhet av motsvarande betydelse för Sveriges säkerhet. Verksamhetsutövaren ska kontrollera att leverantören följer säkerhetsskyddsavtalet (2 kap. 6 § säkerhetsskyddslagen). Kravet på att ingå säkerhetsskyddsavtal gäller även för enskilda verksamhetsutövare.

Det huvudsakliga syftet med ett säkerhetsskyddsavtal är att reglera de säkerhetsskyddsåtgärder som behövs hos leverantören för den verksamhet som omfattas av ett kontrakt om varor, tjänster eller byggentreprenader. Avtalet utgör en grund för att besluta om vilka anställningar och annat deltagande i verksamheten hos leverantören som ska placeras i säkerhetsklass (prop. 2017/18:89 s. 104).

Om de säkerhetsskyddsklassificerade uppgifter som förekommer i en viss upphandling hör till kategorin begränsat hemlig finns det inte någon skyldighet att ingå ett säkerhetsskyddsavtal. Denna skyldighet gäller nämligen bara om det i upphandlingen förekommer uppgifter i säkerhetsskyddsklassen konfidentiell eller högre, eller upphandlingen i övrigt avser eller ger leverantören tillgång till säkerhetskänslig verksamhet av motsvarande betydelse för Sveriges säkerhet.

Den som har ingått ett säkerhetsskyddsavtal ska anmäla det till Säkerhetspolisen (2 kap. 7 § säkerhetsskyddsförordningen). I Säkerhetspolisens vägledning *Säkerhetsskyddad upphandling – en vägledning* (2019) framhålls att verksamhetsutövaren inte bara är skyldig att ingå säkerhetsskyddsavtal med en huvudleverantör, utan också med eventuella underleverantörer om dessa kan komma att få tillgång till säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen konfidentiell eller högre eller få tillgång till säkerhetskänslig verksamhet där åtkomst kan medföra en inte obetydlig skada för Sveriges säkerhet (s. 7).

6.2.5 Säkerhetsskyddsåtgärder

En verksamhetsutövare som utkontrakterar säkerhetskänslig verksamhet ska ingå ett säkerhetsskyddsavtal med leverantören, där leverantören åläggs att vidta säkerhetsskyddsåtgärder som säkerställer samma nivå av säkerhetsskydd som hade gällt om myndigheten själv bedrivit den utkontrakterade verksamheten. I 2 kap. 2–4 §§ säker-

hetsskyddslagen anges vilka säkerhetsåtgärderna inom säkerhetsskyddet är och vilket syfte de har.

Informationssäkerhet ska förebygga att säkerhetsskyddsklassificerade uppgifter obehörigen röjs, ändras, görs otillgängliga eller förstörs, och förebygga skadlig inverkan i övrigt på uppgifter och informationssystem som gäller säkerhetskänslig verksamhet (2 kap. 2 § säkerhetsskyddslagen). Det innebär att om ett informationssystem ska hantera säkerhetsskyddsklassificerade uppgifter ska informationssystemets säkerhetsfunktioner anpassas för att förebygga att sådana uppgifter obehörigen röjs, ändras, görs otillgängliga eller förstörs. Säkerhetsåtgärderna ska dessutom i förhållande till uppgifter och informationssystem som inte utgör eller innehåller säkerhetsskyddsklassificerade uppgifter, men som har avgörande betydelse för t.ex. styrning, reglering och övervakning av för Sverige viktiga samhällsfunktioner, tillgodose behov av tillgänglighet och riktighet. Med uppgifter och informationssystem avses i sammanhanget såväl uppgifter som de tekniska system som används för att i olika avseenden elektroniskt behandla uppgifter (prop. 2017/18:89, s. 138).

I säkerhetsskyddsförordningen finns en bestämmelse som specifikt tar sikte på situationen då en utkontraktering till utländska leverantörer innefattar hantering av säkerhetsskyddsklassificerade uppgifter. Av bestämmelsen framgår att säkerhetsskyddsklassificerade uppgifter inte får lämnas till en utländsk leverantör om inte Sverige har ingått ett internationellt säkerhetsskyddsåtagande med den andra staten och leverantören har godkänts genom en kontroll enligt den andra statens säkerhetsskyddslagstiftning (3 kap. 9 § andra stycket säkerhetsskyddsförordningen).

Fysisk säkerhet ska förebygga såväl att obehöriga får tillträde till områden, byggnader och andra anläggningar eller objekt där de kan få tillgång till säkerhetsskyddsklassificerade uppgifter eller där säkerhetskänslig verksamhet i övrigt bedrivs, som skadlig inverkan på sådana områden, byggnader, anläggningar eller objekt (2 kap. 3 § säkerhetsskyddslagen).

Personalsäkerhet ska förebygga att personer som inte är pålitliga från säkerhetssynpunkt deltar i en verksamhet där de kan få tillgång till säkerhetsskyddsklassificerade uppgifter eller i en verksamhet som av någon annan anledning är säkerhetskänslig, samt säkerställa att de som deltar i säkerhetskänslig verksamhet har tillräcklig kunskap om säkerhetsskydd (2 kap. 4 § säkerhetsskyddslagen).

6.2.6 Närmare om samrådskravet vid utkontraktering

I 2 kap. 6 § säkerhetsskyddsförordningen finns bestämmelser som tar sikte på statliga myndigheter som avser att genomföra en upphandling som innebär krav på säkerhetsskyddsavtal. Statliga myndigheter måste då under vissa förutsättningar vidta särskilda åtgärder innan ett sådant förfarande inleds.

Om bestämmelserna i 2 kap. 6 § säkerhetsskyddsförordningen är tillämpliga ska myndigheten dels genomföra en särskild säkerhetsskyddsbedömning, dels samråda med Säkerhetspolisen eller Försvarsmakten. De beskrivna skyldigheterna gäller i två fall.

Det ena fallet avser situationer där leverantören kan få tillgång till eller möjlighet att förvara säkerhetsskyddsklassificerade uppgifter utanför myndighetens lokaler. Skyldigheten att göra en särskild säkerhetsbedömning och att samråda med tillsynsmyndighet gäller om uppgifterna hör till säkerhetsskyddsklassen hemlig eller högre. Skyldigheterna gäller alltså bara för uppgifter som hör till de två högsta säkerhetsskyddsklasserna; hemlig och kvalificerat hemlig.

Det är viktigt att ha i åtanke att uppgifter som var för sig bedömts vara begränsat hemliga eller inte hemliga alls kan ha ett högre skyddsvärde sammantagna, vilket medför att skyldigheten att samråda med tillsynsmyndigheten träder in. Enbart det faktum att det är fråga om ett stort antal uppgifter medför dock inte att uppgifterna blir mer känsliga.

Det andra fallet där skyldigheterna enligt paragrafen gäller är om leverantören kan få tillgång till säkerhetskänsliga informationssystem utanför myndighetens lokaler och obehörig åtkomst till systemen kan medföra allvarlig skada för Sveriges säkerhet. Valet av nivån allvarlig skada innebär att skadan motsvarar vad som gäller för placering av uppgifter i den näst högsta säkerhetsskyddsklassen, dvs. hemlig.

Tillsynsmyndigheten får dels förelägga myndigheten att vidta åtgärder enligt säkerhetsskyddslagen och de föreskrifter som har meddelats i anslutning till den lagen, dels besluta att myndigheten inte får genomföra upphandlingen om ett föreläggande inte följs eller om tillsynsmyndigheten bedömer att säkerhetsskyddslagens krav inte kan tillgodoses trots att ytterligare åtgärder vidtas.

6.2.7 Säkerhetsprövning

Den som genom anställning eller på något annat sätt ska delta i säkerhetskänslig verksamhet ska säkerhetsprövas (3 kap. 1 § säkerhetsskyddslagen). Kravet på säkerhetsprövning innebär att en myndighet som avser utkontraktera säkerhetskänslig verksamhet måste genomföra säkerhetsprövning av den personal som ska delta i den säkerhetskänsliga verksamheten.

Säkerhetsprövningen syftar till att klarlägga om en person kan antas vara lojal mot de intressen som skyddas i lagen och i övrigt är pålitlig från säkerhetssynpunkt (3 kap. 2 § säkerhetsskyddslagen). Endast den som har bedömts pålitlig från säkerhetssynpunkt och har tillräckliga kunskaper om säkerhetsskydd, och som behöver uppgifterna eller annan tillgång till verksamheten för att kunna utföra sitt arbete eller på annat sätt delta i den säkerhetskänsliga verksamheten, ska vara behörig att ta del av säkerhetsskyddsklassificerade uppgifter eller i övrigt delta i säkerhetskänslig verksamhet (2 kap. 3 § säkerhetsskyddsförordningen).

Säkerhetsprövningen ska genomföras innan deltagandet i den säkerhetskänsliga verksamheten påbörjas. Prövningen ska innefatta en grundutredning samt registerkontroll och särskild personutredning i viss omfattning (3 kap. 3 § säkerhetsskyddslagen).

Prövningen görs av den som beslutar om anställning eller annat deltagande i den säkerhetskänsliga verksamheten, om inte en myndighet har det bestämmande inflytandet över den prövades lämplighet att delta i säkerhetskänslig verksamhet hos en enskild verksamhetsutövare – då är det myndigheten som gör den slutliga bedömningen (3 kap. 4 § andra stycket säkerhetsskyddslagen).

I 3 kap. 5–12 §§ säkerhetsskyddslagen finns bestämmelser om placering i säkerhetsklass. I 3 kap. 13–18 §§ finns bestämmelser om registerkontroll och särskild personutredning. I 3 kap. 19–21 §§ säkerhetsskyddslagen finns bestämmelser om utlämnande av uppgifter för säkerhetsprövning.

6.2.8 Tystnadsplikt och sekretessbrytande bestämmelse

Säkerhetsskyddslagen innehåller två bestämmelser om tystnadsplikt. I 5 kap. 1 § säkerhetsskyddslagen anges att den som med stöd av lagen har fått del av uppgifter som förekommer i angelägenhet som

avser säkerhetsprövning inte obehörigen får röja eller utnyttja dessa uppgifter. I 5 kap. 2 § säkerhetsskyddslagen anges att den som på grund av anställning eller på annat sätt deltar eller har deltagit i säkerhetskänslig verksamhet inte obehörigen får röja eller utnyttja säkerhetsskyddsklassificerade uppgifter. Vidare anges i förhållande till båda bestämmelserna att i det allmännas verksamhet tillämpas i stället bestämmelserna i OSL.

Utredningen om vissa säkerhetsskyddsfrågor framhöll i sitt betänkande (SOU 2018:82) *Kompletteringar till den nya säkerhetsskyddslagen* att tystnadsplikt enligt säkerhetsskyddslagen i en utkontrakteringssituation inte gäller för leverantörens personal, om inte leverantörens verksamhet som sådan är säkerhetskänslig och därför omfattas av säkerhetsskyddslagen, (s. 126).

Vidare finns i 5 kap. 3 § en sekretessbrytande bestämmelse som ger stöd för att lämna ut uppgifter som omfattas av bestämmelser om sekretess i OSL till en annan stat eller mellanfolklig organisation i ett ärende om underlag för säkerhetsprövning enligt 4 kap. 4 §. Bestämmelsen utgör en sådan föreskrift som anges i 8 kap. 3 § 1 OSL. Kravet på att det står klart att utlämnandet är förenligt med svenska intressen innebär ett hinder mot att lämna ut uppgifter som kommit fram vid en registerkontroll om uppgifterna är olämpliga att delge en utländsk myndighet eller en mellanfolklig organisation (prop. 2017/18:89, s. 156).

6.2.9 Tillsyn

Tillsynen över säkerhetsskyddet regleras i 7 kap. 1 § säkerhetsskyddsförordningen. Tillsyn över säkerhetsskyddet inom Fortifikationsverket, Försvarshögskolan och de myndigheter som hör till Försvarsdepartementet utövas av Försvarsmakten. Säkerhetspolisen utövar tillsyn över säkerhetsskyddet inom övriga myndigheter utom Justitiekanslern samt kommuner och regioner. Tillsyn över enskild verksamhet utövas av länsstyrelserna samt Affärsverket svenska kraftnät, Transportstyrelsen och Post- och telestyrelsen.

Säkerhetspolisen och Försvarsmakten får även utöva tillsyn över leverantörer som har uppdrag för flera verksamhetsutövare om leverantörens samlade uppdrag är av stor betydelse för Sveriges säkerhet (7 kap. 2 § andra stycket säkerhetsskyddsförordningen).

Tillsynsmyndigheterna får inom sitt tillsynsområde utöva tillsyn över säkerhetsskyddet hos leverantörer som omfattas av ett säkerhetsskyddsavtal och över underleverantörer som leverantören har anlitat inom ramen för säkerhetsskyddsavtalet (5 kap. 4 § säkerhetsskyddslagen).

6.2.10 Anmälan av incidenter

Säkerhetsskyddsregelverket innefattar en skyldighet att anmäla vissa typer av incidenter som har betydelse för säkerhetsskyddet. En verksamhetsutövare ska skyndsamt anmäla till Säkerhetspolisen om en säkerhetsskyddsklassificerad uppgift kan ha röjts eller om det inträffat en it-incident i ett informationssystem som verksamhetsutövaren är ansvarig för och som har betydelse för säkerhetskänslig verksamhet och där incidenten allvarligt kan påverka säkerheten i systemet. Anmälningsplikten gäller också om verksamhetsutövaren får kännedom eller misstanke om någon annan för denne allvarlig säkerhetshotande verksamhet (2 kap. 10 § säkerhetsskyddsförordningen).

Om verksamhetsutövaren tillhör Försvarsmaktens tillsynsområde, ska anmälan göras också till Försvarsmakten.

Skyldigheten att anmäla incidenter får förutsättas gälla oavsett om verksamheten som berörs av incidenten bedrivs av verksamhetsutövaren själv eller om den utkontrakterats till en privat tjänsteleverantör. I en utkontrakteringssituation är det av vikt att verksamhetsutövaren säkerställer att tjänsteleverantören har förmåga att upptäcka och informera verksamhetsutövaren om incidenter som inträffat. Detta bör regleras i säkerhetsskyddsavtalet mellan tjänsteleverantören och verksamhetsutövaren.

En verksamhetsutövare som är skyldig att anmäla säkerhetshotande händelser och som tillhandahåller tjänster åt en annan verksamhetsutövare ska i samband med anmälan informera och vid behov samråda med de uppdragsgivare som berörs av incidenten (2 kap. 11 § säkerhetsskyddsförordningen).

6.2.11 Internationella säkerhetsskyddsåtaganden

Det finns särskilda krav för en myndighet som tillämpar säkerhetsskyddsregleringen när myndigheten avser att anlita utländska privata tjänsteleverantörer. Från och med den 1 januari 2022 gäller nämligen att Sverige måste ha ingått ett internationellt säkerhetsskyddsåtagande med ett land för att en verksamhetsutövare ska få lämna ut säkerhetsskyddsklassificerade uppgifter till en utländsk privat tjänsteleverantör i det landet. Leverantören måste också ha godkänts genom en kontroll enligt den andra statens säkerhetsskyddslagstiftning (3 kap. 9 § andra stycket säkerhetsskyddsförordningen och punkt 6 i övergångsbestämmelserna till säkerhetsskyddförordningen).

Ett internationellt säkerhetsskyddsåtagande är en folkrättslig förpliktelse avseende säkerhetsskydd mellan Sverige och ett annat land. Åtagandet utgör juridiskt sett en ömsesidig garanti för att säkerhetsskyddsklassificerade uppgifter hanteras på ett säkert sätt i varje land. Det finns både bi- och multilaterala avtal, t.ex. säkerhetsskyddsavtal med North Atlantic Treaty Organization (NATO) och avtal mellan de nordiska länderna. Varje avtal är unikt beroende på ländernas lagstiftning och behov.

Vissa avtal gäller endast inom militär verksamhet. I dagsläget saknas avtal som gäller för civil verksamhet med bl.a. USA och Kanada, vilket påverkar möjligheterna för myndigheter som tillämpar säkerhetsskyddsregleringen att anlita leverantörer i dessa länder för avtal som löper efter den 1 januari 2022.

Kravet på internationella säkerhetsskyddsåtaganden är något som verksamhetsutövaren särskilt bör beakta vid ingående av kontrakt som löper över den 1 januari 2022. I annat fall finns det en risk att verksamhetsutövaren efter detta datum inte kan tillämpa kontraktet som det ursprungligen var tänkt.

6.2.12 Särskilt om aggregerad och ackumulerad information

En särskild fråga är hur man bör hantera den situationen att en utkontraktering av viss it-drift involverar en stor mängd uppgifter som sedda var för sig är klassificerade som begränsat hemliga, eller som inte är säkerhetsskyddsklassificerade alls, men som sammantagna kan vara betydligt känsligare i förhållande till Sveriges säkerhet. Det kan t.ex. handla om situationer där uppgifter som sammanställts har

bearbetats eller kan bearbetas så att man av sammanställningen kan utvinna en annan och mer känslig information än av uppgifterna var för sig. En annan situation kan vara att den sammanställda informationen visar på exempelvis beroenden mellan olika verksamheter, förmåga, sårbarheter eller andra förhållanden som kan leda till en inte obetydlig skada för Sveriges säkerhet om den röjs.

Det kan av lagmotiven utläsas att sammanställningar av uppgifter från olika källor kan göra att den sammanställda informationen utgör säkerhetsskyddsklassificerade uppgifter även om informationen härrör från öppna källor (prop. 2017/18:89 s. 45). Uppgifterna i en sammanställning kan alltså vara säkerhetsskyddsklassificerade, fastän de i ett annat sammanhang inte är det var och en för sig. Det framgår vidare av lagmotiven att verksamhetsutövarna, vid sin klassificering av uppgifter, måste bedöma om en samling av uppgifter i en viss säkerhetsskyddsklass medför att en högre säkerhetsskyddsklass ska tillämpas. Samtidigt påpekas det att man med hänsyn till behovet av att undvika onödiga administrativa kostnader och ingrepp i enskildas integritet m.m. inte bör göra klassificeringen i större utsträckning och med placering i högre klass än vad som är nödvändigt (prop. 2017/18:89 s. 67).

Utredningen om vissa säkerhetsskyddsfrågor framhöll i sitt slutbetänkande att förarbetsuttalandena kan tolkas så att verksamhetsutövarna i sitt arbete med säkerhetsskyddsklassificering är skyldiga att beakta mängden uppgifter och konsekvenserna av att de sammanställs. Rättsläget kan alltså uppfattas på det sättet att en mängd uppgifter som, sedda var för sig, är att bedöma som begränsat hemliga bör klassificeras som konfidentiella om de finns i en samling och skadan vid röjande skulle bli inte obetydlig (SOU 2018:82, s. 153 f.).

Av Säkerhetspolisens föreskrifter framgår att verksamhetsutövaren vid en särskild säkerhetsskyddsbedömning enligt 3 kap. 1 § säkerhetsskyddsförordningen ska beakta såväl de enskilda säkerhetsskyddsklassificerade uppgifterna som den totala mängden sådana uppgifter som kan komma att behandlas i informationssystemet (4 kap. 6 § i PMFS 2019:2).

Det framgår vidare av Säkerhetspolisens *Vägledning i säkerhetsskydd Informationssäkerhet* (2020) att aggregerade uppgifter betyder att flera olika typer av uppgifter samlas och tillsammans utgör ett nytt skyddsvärde, medan ackumulerade uppgifter betyder en ökad volym av samma typ av uppgifter. Om enskilda uppgifter som saknar

säkerhetsskyddsklass eller är indelade i en av säkerhetsskyddsklasserna begränsat hemlig, konfidentiell eller hemlig samlas, kan det i vissa fall medföra att en högre säkerhetsskyddsklass ska tillämpas på uppgiftssamlingen. Så är fallet om den aggregerade eller ackumulerade informationen gör att en antagonist kan dra andra, helt nya slutsatser av uppgiftssamlingen än av varje enskild uppgift (s. 10).

Detta innebär att en myndighet i sin säkerhetsskyddsanalys kan behöva ta ställning till om en sammanställning av uppgifter, där uppgifterna var för sig inte är säkerhetsskyddsklassificerade, ändå uppnår en nivå av känslighet som medför att säkerhetsskyddsregleringen blir tillämplig eller att uppgifterna i sin sammanställda form hamnar i en högre säkerhetsskyddsklass. En myndighet är dock i en utkontrakteringssituation inte skyldig att bedöma hur skyddsvärdet hos myndighetens uppgifter påverkas av andra verksamhetsutövares uppgifter som hanteras av samma privata tjänsteleverantör. Däremot måste tjänsteleverantören ta ställning till om det samlade uppdraget har betydelse för Sveriges säkerhet.

Det kan exempelvis handla om situationer där tjänsteleverantören tillhandahåller driftstjänster eller infrastrukturlösningar i en omfattning som sammantaget bedöms utgöra en viktig del av den nationella förmågan. Vid större koncentrationer av uppdrag kan detta gälla även om de enskilda uppdragen inte omfattas av säkerhetsskyddsavtal. Säkerhetsskyddslagstiftningen kan i sådana fall bli tillämplig för tjänsteleverantörens verksamhet. Det innebär i sin tur att tjänsteleverantören behöver genomföra en säkerhetsskyddsanalys och med utgångspunkt i analysen vidta relevanta säkerhetsskyddsåtgärder, som kan överskrida de åtgärder som ålagts leverantören i säkerhetsskyddsavtal.

6.2.13 Utkontraktering av säkerhetskänslig verksamhet

Utredningen om vissa säkerhetsskyddsfrågor hade till uppgift att bl.a. kartlägga behovet av att förebygga att säkerhetsskyddsklassificerade uppgifter eller i övrigt säkerhetskänslig verksamhet utsätts för risker i samband med utkontraktering, och föreslå olika förebyggande åtgärder, t.ex. tillståndsprövning. Utredningen lämnade sitt slutbetänkande *Kompletteringar till den nya säkerhetsskyddslagen* (SOU 2018:82) i november 2018.

Utredningen bedömde inledningsvis att det fanns anledning att utöka skyldigheten att ingå säkerhetsskyddsavtal. Utredningen konstaterade i denna del bl.a. följande: Det finns situationer där säkerhetsskyddsklassificerade uppgifter eller i övrigt säkerhetskänslig verksamhet exponeras för utomstående, men där det i dagsläget inte finns någon skyldighet att ingå säkerhetsskyddsavtal. Ett exempel på detta kan vara olika former av samarbeten och samverkan som inte handlar om anskaffning av varor, tjänster eller byggentreprenader. Ett annat exempel kan vara situationer där det är leverantörens och inte beställarens skyddsvärden som behöver skyddas. Det finns också situationer där det är oklart om det gäller krav på säkerhetsskyddsavtal. Om det inte ställs krav på säkerhetsskyddsavtal i alla relevanta situationer där säkerhetsskyddsklassificerade uppgifter eller i övrigt säkerhetskänslig verksamhet kommer att exponeras för utomstående, ökar sannolikheten för att motparten inte vidtar de säkerhetsskyddsåtgärder som behövs.

Utredningen föreslog mot denna bakgrund en utvidgning av skyldigheten att ingå säkerhetsskyddsavtal. Förslaget innebär att den som bedriver säkerhetskänslig verksamhet ska ingå ett säkerhetsskyddsavtal så snart verksamhetsutövaren avser att genomföra en upphandling, ingå ett avtal eller inleda någon annan form av samverkan eller samarbete med en utomstående part, om förfarandet innebär att den utomstående parten kan få tillgång till säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen konfidentiell eller högre, eller i övrigt avser eller kan ge den utomstående parten tillgång till säkerhetskänslig verksamhet av motsvarande betydelse för Sveriges säkerhet.

Utredningens kartläggning av behoven att förebygga att säkerhetsskyddsklassificerade uppgifter eller i övrigt säkerhetskänslig verksamhet utsätts för risker i samband med utkontraktering visade att det finns flera brister i säkerhetsskyddsarbetet som bl.a. yttrar sig vid utkontraktering av säkerhetskänslig verksamhet. Vissa av bristerna gäller säkerhetsskyddet generellt, t.ex. att verksamhetsutövaren inte tillämpar säkerhetsskyddsreglerna eller har bristande kunskap om sina skyddsvärden. Sådana brister accentueras när verksamhetsutövaren utkontrakterar en del av den säkerhetskänsliga verksamheten eller på annat sätt kopplar in utomstående i verksamheten. Andra brister handlar specifikt om olika förfaranden där utomstående involveras i den säkerhetskänsliga verksamheten genom exem-

pelvis utkontraktering. Bristerna handlar om bristfällig eller helt avsaknad av prövning av om utkontraktering är lämplig, eller att det är svårt att pröva lämpligheten. Vidare kan det vara fråga om att säkerhetsskyddsavtal är bristfälliga, bristfällig uppföljning av utkontrakteringen medan den pågår och att det saknas tillräckliga möjligheter för samhället att ingripa mot förfaranden som är olämpliga från säkerhetsskyddssynpunkt.

Med utgångspunkt i kartläggningen av utvecklingsbehovet föreslog utredningen ett antal förebyggande åtgärder som delvis motsvaras av vad som gäller i dagsläget enligt 2 kap. 6 § säkerhetsskyddsförordningen. Utredningens förslag innebär för det första att den som bedriver säkerhetskänslig verksamhet och som avser att genomföra ett förfarande som kräver säkerhetsskyddsavtal innan förfarandet inleds ska identifiera vilka säkerhetsskyddsklassificerade uppgifter eller vilken säkerhetskänslig verksamhet i övrigt som den utomstående parten kan få tillgång till och som kräver säkerhetsskydd (särskild säkerhetsbedömning). Med utgångspunkt i den särskilda säkerhetsbedömningen och övriga omständigheter ska verksamhetsutövaren därefter pröva om det planerade förfarandet är lämpligt från säkerhetsskyddssynpunkt (lämplighetsprövning). Om lämplighetsprövningen leder till bedömningen att det planerade förfarandet är olämpligt från säkerhetsskyddssynpunkt, får det inte inledas.

Utredningens förslag innebär för det andra att verksamhetsutövare som planerar att inleda ett förfarande i vissa fall ska samråda med tillsynsmyndigheten. I förslagen ingår även en möjlighet för tillsynsmyndigheten att förelägga verksamhetsutövaren att vidta åtgärder enligt säkerhetsskyddslagen och de föreskrifter som har meddelats i anslutning till lagen. Om ett föreläggande inte följs eller om tillsynsmyndigheten bedömer att det planerade förfarandet är olämpligt från säkerhetsskyddssynpunkt även om ytterligare åtgärder vidtas, föreslås tillsynsmyndigheten få besluta att verksamhetsutövaren inte får genomföra det planerade förfarandet.

Utredningens förslag innebär för det tredje en möjlighet för tillsynsmyndigheten att genom föreläggande ingripa mot ett pågående förfarande, t.ex. en pågående utkontraktering om ett sådant pågående förfarande som omfattas av ett krav på säkerhetsskyddsavtal är olämpligt från säkerhetsskyddssynpunkt. Föreläggandet kan bl.a. innebära ett krav på att hela eller delar av förfarandet ska upphöra.

Utredningens förslag på utökad skyldighet att teckna säkerhetsskyddsavtal och förslagen på förebyggande åtgärder vid utkontraktering bereds för närvarande i Regeringskansliet.

6.3 Informationssäkerhet

6.3.1 Inledning

Syftet med detta avsnitt är att kartlägga de rättsliga förutsättningarna för myndigheters utkontraktering av it-drift utifrån författningarna som har som huvudsyfte att ställa krav på hur arbetet med myndigheters informationssäkerhet ska bedrivas. Därutöver ställer ett antal författningar krav på hur olika informationsmängder ska skyddas, exempelvis personuppgifter.

För krav på informationssäkerhetsarbetet gäller delvis olika regelverk inom statlig respektive kommunal sektor. För statliga myndigheter gäller förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap. Förordningen innehåller bestämmelser om informationssäkerhet och kompletteras av flera föreskrifter från Myndigheten för samhällsskydd och beredskap (MSB).

Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen (NIS-direktivet) ställer krav på säkerhet i nätverk och informationssystem. Reglerna omfattar leverantörer av samhällsviktiga tjänster och vissa digitala tjänster. Direktivet har genomförts i svensk rätt genom lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster och förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster. MSB har meddelat flera föreskrifter som kompletterar lagen och förordningen.

6.3.2 Statliga myndigheters informationssäkerhet

Förordningen om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap

I förordningen finns bestämmelser som syftar till att statliga myndigheter genom sin verksamhet ska minska sårbarheten i samhället och utveckla en god förmåga att hantera sina uppgifter under fredstida krissituationer och inför, respektive vid, höjd beredskap.

Varje myndighet ansvarar för att egna informationshanteringssystem uppfyller sådana grundläggande och särskilda säkerhetskrav att myndighetens verksamhet kan utföras på ett tillfredsställande sätt, med särskilt beaktande av behovet av säkra ledningssystem (19 §).

It-incidenter som inträffat i statliga myndigheters informationssystem och som allvarligt kan påverka säkerheten i den informationshantering som myndigheten ansvarar för, eller som inträffat i tjänster som myndigheten tillhandahåller åt en annan organisation, ska rapporteras till MSB (20 §). Rapporteringsskyldigheten omfattar inte sådana incidenter som ska anmälas enligt 2 kap. 10 § första stycket 2 säkerhetsskyddsförordningen.

I 21 § finns ett bemyndigande för MSB att meddela föreskrifter om krav på säkerhet för myndigheternas informationshanteringssystem och att meddela föreskrifter rörande rapportering av it-incidenter. MSB har meddelat bestämmelser om sådana säkerhetskrav som avses i 19 § förordningen om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap i två olika föreskrifter, dels i föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS 2020:6), dels i föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter (MSBFS 2020:7).

Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS 2020:6)

Föreskrifterna innehåller bl.a. krav på hur myndigheternas informationssäkerhetsarbete ska utformas och bedrivas, bestämmelser om säkerhetsåtgärder samt bestämmelser om hur uppföljning av informationssäkerhetsarbetet ska ske.

I 6 § finns bestämmelser om hur informationssäkerhetsarbetet ska bedrivas. Där framgår följande. Myndigheten ska säkerställa att informationssäkerhetsarbetet är systematiskt och riskbaserat genom att klassa sin information avseende konfidentialitet, riktighet och tillgänglighet i olika nivåer utifrån vilka konsekvenser ett bristande skydd kan få (informationsklassning). Myndigheten ska vidare identifiera, analysera och värdera risker för sin information (riskbedömning). Myndigheten ska dessutom utifrån genomförd informationsklassning och riskbedömning identifiera behov av och införa ändamålsenliga och proportionella säkerhetsåtgärder, och utvärdera säkerhetsåtgärderna samt vid behov anpassa skyddet av informationen.

I 8 § i föreskrifterna finns en bestämmelse av särskild betydelse vid utkontraktering. Där framgår att myndigheten, innan den låter en extern aktör behandla information, utifrån informationsklassning och riskbedömning, ska hantera de risker en sådan behandling innebär. Myndigheten ska vidare i avtal ställa krav på vilka säkerhetsåtgärder den externa aktören ska vidta och hur myndigheten följer upp dessa krav.

I de allmänna råd som meddelats i anslutning till 8 § i föreskrifterna anges att avtalet mellan myndigheten och den externa aktören bör reglera att den externa aktören ska ha tillräcklig kompetens avseende informationssäkerhet, hur den externa aktören ska överlämna information till myndigheten om misstänkta eller inträffade incidenter, avvikelser och sårbarheter, hur den externa aktören ska följa upp sitt egna och eventuella underleverantörers systematiska och riskbaserade informationssäkerhetsarbete, och hur myndighetens information ska återlämnas när avtalet upphör.

Myndigheten för samhällsskydd och beredskaps föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter (MSBFS 2020:7)

Föreskrifterna innehåller bl.a. bestämmelser om ansvar inom myndigheten, riskbedömning, dokumentation av it-miljön samt bestämmelser med krav kopplade till drift och förvaltning.

Myndigheten ska upprätthålla uppdaterad dokumentation över beroenden mellan olika interna informationssystem respektive beroenden av informationssystem hos externa aktörer (2 kap. 4 §).

I 3 kap. i föreskrifterna finns bestämmelser om bl.a. utkontraktering. Där framgår bl.a. att myndigheten vid utkontraktering ska identifiera vilka krav på säkerhet som ska gälla samt dokumentera vilka säkerhetsåtgärder som valts för att möta respektive krav (3 kap. 1 §).

Myndigheten ska vidare innan driftsättning och inför förändring som kan påverka säkerheten i informationssystemen kontrollera att valda säkerhetsåtgärder är tillräckliga för att möta identifierade krav på säkerhet och verifiera att det finns nödvändig dokumentation för drift och förvaltning. I de fall brister identifieras ska myndigheten vidare riskbedöma och hantera dessa brister innan driftsättning eller inför förändring som kan påverka säkerheten i informationssystemen (3 kap. 2 §).

I de allmänna råden som meddelats i anslutning till dessa bestämmelser anges att nödvändig dokumentation för drift och förvaltning bör omfatta arkitektur, ingående komponenter, konfiguration, dataflöden och övrig relevant systeminformation. Av dokumentationen bör även framgå vem som är systemägare samt om och till vilken extern aktör informationssystemet är utkontrakterat.

Myndigheten för samhällsskydd och beredskaps föreskrifter om rapportering av it-incidenter för statliga myndigheter (MSBFS 2020:8)

Föreskrifterna innehåller bestämmelser om rapportering av it-incidenter enligt 20 § förordningen om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap.

I 8 § i föreskrifterna finns en bestämmelse om incidentrapportering vid utkontraktering. Bestämmelsen innebär att om myndigheten överlåter en del av sin informationshantering till en aktör som inte omfattas av rapporteringsskyldighet ska myndigheten se till att aktören åtar sig att rapportera it-incidenter till myndigheten på ett sådant sätt att myndigheten kan uppfylla kraven i föreskrifterna.

6.3.3 NIS-direktivet och tillhörande nationell lagstiftning

NIS-direktivet syftar enligt artikel 1 till att förbättra den inre marknadens funktion genom att fastställa åtgärder för att uppnå en hög gemensam nivå på säkerhet i nätverks- och informationssystem.

Direktivet innebär bl.a. skyldigheter för vissa leverantörer av samhällsviktiga tjänster, och vissa leverantörer av digitala tjänster, att vidta säkerhetsåtgärder för att hantera risker samt förebygga och hantera incidenter i nätverk och informationssystem som de är beroende av för att tillhandahålla tjänsterna. Regleringen gäller därför, till skillnad från den som avser statliga myndigheter, inte organisationens informationshantering i sin helhet, förutom i de fall där leverantören enbart bedriver samhällsviktiga eller digitala tjänster och att leverantören är beroende av samtliga av sina nätverk och informationssystem för att leverera tjänsten. Bedriver leverantören verksamhet som inte utgörs av en samhällsviktig eller digital tjänst faller den utanför regleringen. Leverantörerna ska också rapportera incidenter som har en betydande eller avsevärd inverkan på kontinuiteten i tjänster.

I direktivet identifieras sju sektorer som tillhandahåller samhällsviktiga tjänster. Dessa är bankverksamhet, digital infrastruktur, energi, finansmarknadsinfrastruktur, hälso- och sjukvård, leverans och distribution av dricksvatten samt transport.

Direktivet har genomförts i svensk rätt genom lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster och förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster. MSB har meddelat föreskrifter om bl.a. anmälan och identifiering av leverantörer av samhällsviktiga tjänster (MSBFS 2018:7), informationssäkerhet för leverantörer av samhällsviktiga tjänster (MSBFS 2018:8), rapportering av incidenter för leverantörer av samhällsviktiga tjänster (MSBFS 2018:9) och rapportering av incidenter för leverantörer av digitala tjänster (MSBFS 2018:10).

Lagen och förordningen om informationssäkerhet för samhällsviktiga och digitala tjänster gäller för de sektorer som anges i direktivet, med tillägg av digitala tjänster. Sådan verksamhet som träffas av regelverket kan bedrivas i såväl enskild som offentlig regi. Hälso- och sjukvård som bedrivs enligt hälso- och sjukvårdslagen (2017:30) kan nämnas som exempel på sådan verksamhet som träffas av regelverket.

Regelverket gäller inte för leverantörer av allmänna kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster och därför omfattas av lagen (2003:389) om elektronisk kommunikation, leverantörer av betrodda tjänster som omfattas av kraven i artikel 19 i Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG, leverantörer av digitala tjänster som är mikroföretag eller små företag enligt definitionen i kommissionens rekommendation 2003/361/EG av den 6 maj 2003 om definitionen av mikroföretag samt små och medelstora företag eller för verksamhet som omfattas av säkerhetsskyddslagen.

Det framgår av 13 § i lagen om informationssäkerhet för samhällsviktiga och digitala tjänster att leverantörer som omfattas av lagen ska vidta ändamålsenliga och proportionella tekniska och organisatoriska åtgärder för att hantera risker som hotar säkerheten i nätverk och informationssystem som de använder för att tillhandahålla samhällsviktiga tjänster. Det framgår vidare att åtgärderna ska säkerställa en nivå på säkerheten i nätverken och informationssystemen som är lämplig i förhållande till risken. Motsvarande skyldigheter gäller för leverantörer av digitala tjänster (15 § lagen om informationssäkerhet för samhällsviktiga och digitala tjänster).

Leverantörerna som träffas av lagen ska vidta lämpliga åtgärder för att förebygga och minimera verkningar av incidenter som påverkar nätverk och informationssystem som de använder för att tillhandahålla samhällsviktiga tjänster, och att åtgärderna ska syfta till att säkerställa kontinuiteten i tjänsterna (14 § lagen om informationssäkerhet för samhällsviktiga och digitala tjänster). Motsvarande skyldigheter gäller för leverantörer av digitala tjänster (16 § lagen om informationssäkerhet för samhällsviktiga och digitala tjänster).

I specialmotiveringen till 13 § i lagen om informationssäkerhet för samhällsviktiga och digitala tjänster förtydligas att säkerhetskraven gäller de nätverk och informationssystem som leverantören använder vid tillhandahållandet av samhällsviktiga tjänster, oavsett om denne sköter underhållet av sina nätverk och informationssystem internt eller har utkontrakterat verksamheten (prop. 2017/18:205, s. 94). Detsamma får antas gälla även i förhållande till de krav som anges i 14, 15 och 16 §§ lagen om informationssäkerhet för samhällsviktiga och digitala tjänster.

Leverantörer av samhällsviktiga tjänster ska utan onödigt dröjsmål rapportera incidenter som har en betydande inverkan på kontinuiteten i den samhällsviktiga tjänst som de tillhandahåller (18 § lagen om informationssäkerhet för samhällsviktiga och digitala tjänster). Leverantörer av digitala tjänster ska inom samma tidsram rapportera incidenter som har en avsevärd inverkan på tillhandahållandet av en digital tjänst som de erbjuder (19 § lagen om informationssäkerhet för samhällsviktiga och digitala tjänster). Incidentrapporten ska enligt 2 kap. 4 § första stycket 4 p. i MSBFS 2018:9 för samhällsviktiga tjänster och enligt 8 § första stycket 4 i MSBFS 2018:10 för digitala tjänster innehålla namn och organisationsnummer till extern aktör dit informationshantering har utkontrakterats i det fall incidenten inträffat hos den externa aktören.

I förordningen om informationssäkerhet för samhällsviktiga och digitala tjänster regleras vilka myndigheter som är tillsynsmyndigheter för leverantörer av samhällsviktiga tjänster enligt lagen om informationssäkerhet för samhällsviktiga och digitala tjänster. Statens energimyndighet är tillsynsmyndighet för energisektorn, Transportstyrelsen för transportsektorn, Finansinspektionen för finansmarknadsinfrastruktursektorn, Inspektionen för vård och omsorg för hälso- och sjukvårdssektorn, Livsmedelsverket är tillsynsmyndighet för den sektor som handhar leverans och distribution av dricksvatten och Post- och telestyrelsen för den sektor som handhar digital infrastruktur (17 § förordningen om informationssäkerhet för samhällsviktiga och digitala tjänster). Post- och telestyrelsen är dessutom tillsynsmyndighet för leverantörer av digitala tjänster (18 § förordningen om informationssäkerhet för samhällsviktiga och digitala tjänster).

Statens energimyndighet, Transportstyrelsen, Finansinspektionen, Livsmedelsverket och Post- och telestyrelsen får meddela föreskrifter om säkerhetsåtgärder för sina respektive tillsynsområden. Socialstyrelsen får meddela sådana föreskrifter för Inspektionen för vård och omsorgs tillsynsområde (8 § förordningen om informationssäkerhet för samhällsviktiga och digitala tjänster). Arbete med sådana föreskrifter pågår.

6.4 Sammanfattning

Reglerna om informationssäkerhet skiljer sig delvis åt mellan statliga myndigheter å ena sidan och kommuner och regioner å den andra.

För statliga myndigheter gäller förordningen om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap och de föreskrifter som MSB meddelat med stöd av förordningen. Av förordningen framgår den grundläggande utgångspunkten att varje myndighet ansvarar för sin egen informationssäkerhet. Det finns ingen myndighet som utövar tillsyn över att dessa regler följs.

Lagen och förordningen om informationssäkerhet för samhällsviktiga och digitala tjänster samt de föreskrifter som MSB meddelat med stöd av lagen och förordningen gäller för sektorerna bankverksamhet, digital infrastruktur, energi, finansmarknadsinfrastruktur, hälso- och sjukvård, leverans och distribution av dricksvatten, transport och digitala tjänster. Tillsynen över regleringen är delad mellan flera myndigheter, som ansvarar för varsin sektor.

Till skillnad från informationssäkerhetsregleringen, som gäller för den totala informationshanteringen inom en verksamhet som träffas av regleringen, så gäller säkerhetsskyddsregleringen för en begränsad del av verksamheten (som är säkerhetskänslig) eller en delmängd uppgifter (för att dessa är säkerhetsskyddsklassificerade). I likhet med vad som gäller enligt informationssäkerhetsregleringen så är det verksamhetsutövaren (eller myndigheten) som ansvarar för att säkerhetsskyddet upprätthålls inom den egna verksamheten. Tillsyn över säkerhetsskydd inom statliga myndigheter, kommuner och regioner utövas av Försvarsmakten och Säkerhetspolisen.

7 Dataskydd

7.1 Inledning

Syftet med detta kapitel är att kartlägga de rättsliga förutsättningarna för myndigheters[1] utkontraktering av it-drift till privata tjänsteleverantörer utifrån dataskyddsregleringen.

Kapitlet inleds med en redogörelse för regleringen av myndigheters behandling av personuppgifter. Därefter följer en genomgång av de regler i dataskyddsförordningen som reglerar det organisatoriska och avtalsmässiga förhållandet mellan en personuppgiftsansvarig och ett personuppgiftsbiträde. Avslutningsvis finns en analys av rättsläget när det gäller överföring av personuppgifter till tredjeland.

7.2 Dataskyddsregleringen

7.2.1 Europakonventionen

Sedan den 1 januari 1995 är den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen) inkorporerad i svensk rätt och gäller som lag.[2] Av 2 kap. 19 § regeringsformen framgår att lag eller annan föreskrift inte får meddelas i strid med Sveriges åtaganden på grund av konventionen.

Enligt artikel 8 i Europakonventionen har var och en rätt till respekt för sitt privat- och familjeliv, sitt hem och sin korrespondens. Offentlig myndighet får inte inskränka åtnjutande av denna rättighet annat än med stöd av lag och om det i ett demokratiskt

[1] Med myndigheter avses i detta kapitel statliga myndigheter, kommuner och regioner om inget annat framgår av sammanhanget.
[2] Lagen (1994:1219) om den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna, prop. 1993/94:117.

samhälle är nödvändigt med hänsyn till statens säkerhet, den allmänna säkerheten, landets ekonomiska välstånd eller till förebyggande av oordning eller brott eller till skydd för hälsa eller moral eller för andra personers fri- och rättigheter.

Behandling av personuppgifter kan falla inom tillämpningsområdet för artikel 8 i Europakonventionen. EU-domstolen har slagit fast att bestämmelserna i artikel 8 i Europakonventionen har viss betydelse vid bedömningen av nationella regler som tillåter behandling av personuppgifter.[3] Vidare har Europadomstolen slagit fast att artikel 8 i Europakonventionen ålägger staten såväl en negativ förpliktelse att avstå från att göra intrång i rätten till respekt för privat- och familjelivet som en positiv förpliktelse att skydda enskilda mot att andra enskilda handlar på ett sätt som innebär integritetsintrång.[4]

7.2.2 Europeiska unionens stadga om de grundläggande friheterna

Vid Europeiska rådets möte i Nice år 2000 antog EU:s medlemsstater Europeiska unionens stadga om de grundläggande rättigheterna (stadgan). Som en följd av Lissabonfördraget, som trädde i kraft år 2009, är stadgan rättsligt bindande för EU-institutionerna och medlemsstaterna när dessa tillämpar unionsrätten.

I artikel 7 i stadgan anges att var och en har rätt till respekt för sitt privatliv och familjeliv, sin bostad och sina kommunikationer. Av artikel 8 i stadgan framgår vidare att var och en har rätt till skydd av de personuppgifter som rör honom eller henne. Dessa uppgifter ska behandlas lagenligt för bestämda ändamål och på grundval av den berörda personens samtycke eller någon annan legitim och lagenlig grund. Var och en har rätt att få tillgång till insamlade uppgifter som rör honom eller henne och att få rättelse av dem. En oberoende myndighet ska kontrollera att dessa regler efterlevs.

[3] Dom av den 20 maj 2003, *Österreichischer Rundfunk m.fl.*, C-465/00, C-138/01 och C-139/01, EU:C:2003:294.
[4] Se t.ex. *Airey mot Irland*, nr 6289/73, dom meddelad den 9 oktober 1979, *X och Y mot Nederländerna*, nr 8978/80, dom meddelad den 26 mars 1985, *K.U. mot Finland*, nr 2872/02, dom meddelad den 2 december 2008 och *Söderman mot Sverige*, nr 5786/08, dom meddelad den 12 november 2013.

7.2.3 Regeringsformen

Svensk grundlag ger ett grundläggande skydd för den personliga integriteten, utöver det som följer av att lag eller annan föreskrift inte får meddelas i strid med Europakonventionen. Enligt målsättningsstadgandet i 1 kap. 2 § första stycket regeringsformen ska den offentliga makten utövas med respekt för den enskilda människans frihet. I fjärde stycket samma paragraf anges att det allmänna ska värna om den enskildes privat- och familjeliv. I 2 kap. 4 och 5 §§ regeringsformen finns bestämmelser om absolut skydd mot allvarliga fysiska integritetsintrång, bl.a. döds- och kroppsstraff. Enligt 2 kap. 6 § första stycket regeringsformen är var och en därutöver skyddad gentemot det allmänna mot bl.a. påtvingade kroppsliga ingrepp.

För att stärka skyddet för den personliga integriteten infördes den 1 januari 2011 ett nytt andra stycke i 2 kap. 6 § regeringsformen. I bestämmelsen anges att var och en gentemot det allmänna är skyddad mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden. Skyddet får enligt 2 kap. 20 och 21 §§ regeringsformen begränsas genom lag, men endast för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle.

7.2.4 Dataskyddsförordningen

Inledning

Den generella regleringen av personuppgiftsbehandling i Sverige och i övriga EU-länder utgörs av Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (dataskyddsförordningen).

Det materiella tillämpningsområdet

Dataskyddsförordningen ska tillämpas på sådan behandling av personuppgifter som helt eller delvis företas på automatisk väg samt på annan behandling än automatisk av personuppgifter som ingår eller kommer att ingå i ett register (artikel 2.1).

Med *personuppgifter* avses varje upplysning som avser en identifierad eller identifierbar fysisk person, varvid en identifierbar fysisk person är en person (*registrerad*) som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet (artikel 4.1).

Uttrycket *behandling* definieras som en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring (artikel 4.2).

Med *register* förstås en strukturerad samling av personuppgifter som är tillgänglig enligt särskilda kriterier, oavsett om samlingen är centraliserad, decentraliserad eller spridd på grundval av funktionella eller geografiska förhållanden (artikel 4.6).

Utgångspunkten är att dataskyddsförordningen är tillämplig på all behandling av personuppgifter som utgör ett led i en verksamhet som omfattas av unionsrätten, med vissa undantag. Dataskyddsförordningen ska inte tillämpas på behandling av personuppgifter som medlemsstater utför när de bedriver verksamhet som omfattas av avdelning V kapitel 2 i EU-fördraget (artikel 2.2 led b), dvs. behandling av personuppgifter som utförs när Sverige bedriver verksamhet som omfattas av den gemensamma utrikes- och säkerhetspolitiken. Dataskyddsförordningen ska inte heller tillämpas för sådan personuppgiftsbehandling som behöriga myndigheter utför i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, i vilket även ingår att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten (artikel 2.2 led d). Sådan personuppgiftsbehandling omfattas i stället av det nya dataskyddsdirektivet.

Att dataskyddsförordningen inte kan tillämpas utanför unionsrätten – i enlighet med vad som framgår av artikel 2.2 led a – följer redan av det förhållandet att EU:s befogenheter att anta bindande rättsakter naturligtvis är begränsad till unionsrätten. Bestämmelsen är alltså en ren upplysningsbestämmelse. I skäl 16 till dataskyddsför-

ordningen anges nationell säkerhet som exempel på en sådan verksamhet som faller utanför unionsrätten.

I artikel 2.2. led c, 2.3 och 2.4 i dataskyddsförordningen finns ytterligare föreskrifter om dataskyddsförordningens materiella tillämpningsområde.

Det territoriella tillämpningsområdet

Dataskyddsförordningen ska tillämpas på behandlingen av personuppgifter inom ramen för den verksamhet som bedrivs av en personuppgiftsansvarig eller ett personuppgiftsbiträde som är etablerad i unionen, oavsett om behandlingen utförs i unionen eller inte (artikel 3.1).

Vidare ska dataskyddsförordningen enligt artikel 3.2 tillämpas på behandling av personuppgifter som avser registrerade som befinner sig i unionen och som utförs av en personuppgiftsansvarig eller ett personuppgiftsbiträde som inte är etablerat i unionen i två situationer, nämligen om behandlingen har anknytning till varor eller tjänster till sådana registrerade i unionen, oavsett om dessa varor eller tjänster erbjuds kostnadsfritt eller inte (led a) eller övervakning av deras beteende så länge beteendet sker inom unionen (led b).

Slutligen ska dataskyddsförordningen tillämpas på behandling av personuppgifter som utförs av en personuppgiftsansvarig som inte är etablerad i unionen, men på en plats där en medlemsstats nationella rätt gäller enligt folkrätten (artikel 3.3). Som exempel på en sådan plats nämns i skäl 25 till förordningen en medlemsstats diplomatiska beskickning eller konsulat.

7.2.5 Dataskyddslagen

Av artikel 288 andra stycket i fördraget om Europeiska unionens funktionssätt följer att en förordning ska ha allmän giltighet och vara till alla delar bindande och direkt tillämplig i varje medlemsstat.

Den omständigheten att den generella unionsrättsakten om dataskydd är en förordning innebär omfattande begränsningar i möjligheten att införa eller behålla nationella bestämmelser om dataskydd. I dataskyddsförordningen finns emellertid många bestämmelser som både medger eller ger utrymme för kompletterande nationella bestäm-

melser av olika slag. I vissa fall t.o.m. förutsätts kompletterande nationella bestämmelser. Detta gäller särskilt för den offentliga sektorn.

Vidare anges i skäl 8 till dataskyddsförordningen att om förordningen föreskriver förtydliganden eller begränsningar av dess bestämmelser genom medlemsstaternas nationella rätt, kan medlemsstaterna, i den utsträckning det är nödvändigt för samstämmigheten och för att göra de nationella bestämmelserna begripliga för de personer de tillämpas på, införliva delar av förordningen i nationell rätt. Det är alltså tillåtet att under vissa förutsättningar genomföra delar av dataskyddsförordningen i den nationella rätten.

De kompletterande bestämmelser som bedömts som lämpliga eller nödvändiga att införa i svensk rätt med anledning av dataskyddsförordningen och som är av generell karaktär, i betydelsen att de rör hela samhället eller flertalet myndigheter och inte endast en sektor, har samlats i lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen).

Dataskyddslagen är inte heltäckande utan endast ett komplement till dataskyddsförordningen (1 kap. 3 §). Det innebär att lagen inte kan tillämpas självständigt. Är dataskyddslagen tillämplig på en viss behandling av personuppgifter som den personuppgiftsansvarige utför kan denna alltså inte nöja sig med att enbart tillämpa bestämmelserna i den lagen. Även bestämmelserna i dataskyddsförordningen måste iakttas.

Dataskyddslagen är subsidiär i förhållande till annan reglering, dvs. om en annan lag eller en förordning innehåller någon bestämmelse som avviker från den lagen, ska den bestämmelsen tillämpas i stället (1 kap. 6 §).

Genom 1 kap. 2 § dataskyddslagen har tillämpningsområdet för dataskyddsförordningen utvidgats. I paragrafen föreskrivs att bestämmelserna i dataskyddsförordningen, i den ursprungliga lydelsen, och denna lag – dvs. dataskyddslagen – ska gälla även vid behandling av personuppgifter som utgör ett led i en verksamhet som inte omfattas av unionsrätten och i verksamhet som omfattas av avdelning V kapitel 2 i EU-fördraget.

7.2.6 Registerförfattningar

Vid sidan om dataskyddsförordningen och dataskyddslagen finns bestämmelser om dataskydd i en mängd s.k. registerförfattningar. I vissa fall finns också bestämmelser om dataskydd insprängda i författningar som i huvudsak reglerar andra frågor.

Registerförfattningarna gäller i regel för en viss myndighet eller grupp av myndigheter. Författningarna innehåller särregler som är anpassade för den verksamhet som myndigheten eller myndigheterna ägnar sig åt. Det följer av att dataskyddslagen är subsidiär i förhållande till annan reglering att registerförfattningarna i förekommande fall ska tillämpas i stället för dataskyddslagen. Det kan i detta sammanhang inflikas att det finns många myndigheter för vilka det inte gäller någon registerförfattning. Sådana myndigheter har att enbart förhålla sig till dataskyddsförordningen och till de kompletterande bestämmelserna i dataskyddslagen.

Som exempel på en registerförfattning kan nämnas domstolsdatalagen (2015:728). Den lagen ska tillämpas när de allmänna domstolarna, de allmänna förvaltningsdomstolarna samt hyres- och arrendenämnderna behandlar personuppgifter dels i den rättskipande och rättsvårdande verksamhet, dels när personuppgifterna vidarebehandlas i den administrativa verksamheten för att lämnas ut efter begäran (2 § första stycket). Det anförda innebär att domstolarna – när de behandlar personuppgifter i andra sammanhang – t.ex. inom ramen för ett personalärende – har att tillämpa dataskyddsförordningen och de kompletterande bestämmelserna i dataskyddslagen.

Det bör understrykas att domstolsdatalagen och andra registerförfattningar endast utgör komplement till dataskyddsförordningen. I författningarna regleras alltså inte alla dataskyddsfrågor. Som exempel kan här nämnas reglerna om överföring av personuppgifter till tredje land som återfinns i artiklarna 44–50 i dataskyddsförordningen. Några särregler om tredjelandsöverföring finns inte i t.ex. domstolsdatalagen. Inte heller innehåller dataskyddslagen några kompletterande regler i detta ämne. En domstol som ska överföra personuppgifter till tredje land har alltså att direkt tillämpa bestämmelserna i dataskyddsförordningen även om den personuppgiftsbehandlingen sker i den rättskipande eller rättsvårdande verksamheten.

7.2.7 Dataskyddsdirektivet

I samband med att dataskyddsförordningen antogs fattades även beslut om ett nytt direktiv för personuppgiftsbehandling inom det brottsbekämpande området: Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF (dataskyddsdirektivet).

Direktivet har i svensk rätt genomförts i huvudsak genom brottsdatalagen (2018:1177).

7.2.8 Brottsdatalagen

Inledning

Brottsdatalagen är en ramlag som gäller vid behandling av personuppgifter som utförs av behöriga myndigheter i syfte att förebygga, förhindra, upptäcka brottslig verksamhet, utreda eller lagföra brott eller verkställa straffrättsliga påföljder (1 kap. 2 §.) Lagen gäller också vid behandling av personuppgifter som en behörig myndighet utför i syfte att upprätthålla allmän ordning och säkerhet. Det ska sägas att grundläggande begrepp som personuppgifter, behandling m.m. vilka förekommer i brottsdatalagen har samma innebörd som motsvarande begrepp i dataskyddsförordningen.

En avgörande skillnad mellan dataskyddsförordningen och brottsdatalagen är att den senare regleringens tillämpningsområde knutits till vilket syfte personuppgiftsbehandlingen har. Ytterligare en förutsättning för att lagen ska vara tillämplig är som sagt att behandlingen utförs av en behörig myndighet. Det förhållandet att brottsdatalagens tillämpningsområde knutits till bl.a. personuppgiftsbehandlingens syfte innebär att personuppgifternas karaktär saknar betydelse för frågan om brottsdatalagen är tillämplig. Personuppgifterna som behandlas måste alltså inte i sig vara hänförliga till de frågor som behandlingen ska syfta till för att lagen ska vara tillämplig.

Brottsdatalagen ska enligt lagmotiven i huvudsak tillämpas av Polismyndigheten, Kustbevakningen, Skatteverket, Tullverket, Åklagarmyndigheten, Ekobrottsmyndigheten, de allmänna domstolarna och Kriminalvården (prop. 2017/18:232, 99 f.).

Brottsdatalagens tillämpningsområde är bredare än det nya dataskyddsdirektivets tillämpningsområde

I likhet med dataskyddsförordningen ska det nya dataskyddsdirektivet inte tillämpas på behandling av personuppgifter som utgör ett led i en verksamhet som inte omfattas av unionsrätten (artikel 2.3 led a). Av skäl 14 till det nya dataskyddsdirektivet framgår att verksamhet som rör nationell säkerhet, verksamhet som utförs av byråer och organ som hanterar nationella säkerhetsfrågor och medlemsstaternas behandling av personuppgifter inom verksamhet som avser den gemensam utrikes- och säkerhetspolitiken inte omfattas av direktivets tillämpningsområde.

Artikel 2.3 a i det nya dataskyddsdirektivet har genomförts genom 1 kap. 4 § brottsdatalagen. Av den bestämmelsen följer att brottsdatalagen inte gäller vid Säkerhetspolisens behandling av personuppgifter som rör nationell säkerhet eller om Polismyndigheten har övertagit en arbetsuppgift som rör nationell säkerhet. Lagen gäller inte heller sådan verksamhet som omfattas av lagen (2007:258) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst.

Det sätt på vilket lagstiftningen utformats innebär att brottsdatalagen däremot ska tillämpas när övriga myndigheter behandlar personuppgifter som ett led i en verksamhet som inte omfattas av unionsrätten (jfr prop. 2017/18:232 s. 104 och 433.). Brottsdatalagen har därmed getts ett bredare tillämpningsområde än det nya dataskyddsdirektivet.

Vid sidan om brottsdatalagen finns olika speciallagar för brottsbekämpande myndigheter. Dessa lagar gäller utöver brottsdatalagen. Som exempel kan nämnas lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område.

7.2.9 Några grunddrag i regleringen

Dataskyddsförordningen

Dataskyddsförordningen bygger på den grundläggande tanken att en personuppgiftsbehandling inte är tillåten med mindre än att det finns en rättslig grund för den. I artikel 6.1 i dataskyddsförordningen listas dessa grunder. Listan är uttömmande.

De rättsliga grunder som myndigheternas personuppgiftsbehandling i allmänhet grundar sig på återfinns i led c och led e. Enligt led c är behandlingen laglig om den är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige. Av led e följer att behandlingen är laglig om den är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning.

När det gäller de rättsliga grunder för behandlingen som följer av led c och led e sägs i första stycket i artikel 6.3 led a och led b att dessa grunder ska fastställas i enlighet med unionsrätten eller en medlemsstats nationella rätt som den personuppgiftsansvarige omfattas av. I lagmotiven till dataskyddslagen görs bedömningen att dessa bestämmelser inte innebär något krav på att själva behandlingen av personuppgifter måste regleras. Det är i stället den rättsliga förpliktelsen, uppgiften av allmänt intresse, eller myndighetsutövningen som ska ha stöd i rättsordningen (prop. 2017/18:105 s. 48 ff.).

I dataskyddslagen har det i 2 kap. 1 och 2 §§ införts bestämmelser som syftar till att tydliggöra vad som följer av artikel 6.1 led c och led e och artikel 6.2 första stycket led a och b i dataskyddsförordningen.

I artikel 5.1 i dataskyddsförordningen listas ett antal principer som alltid måste iakttas när personuppgifter behandlas.

Som exempel kan nämnas att uppgifterna ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål (led b).

Det är som utgångspunkt förbjudet att behandla vissa personuppgifter, så kallade särskilda kategorier av personuppgifter, t.ex. personuppgifter som avslöjar politiska åsikter och personuppgifter som rör fällande domar i brottmål samt lagöverträdelser som innefattar brott (artikel 9 och 10). I vissa situationer gäller undantag från det principiella förbudet (artikel 9.2–4).

I artiklarna 12–23 finns bestämmelser om de registrerades rättigheter. Här kan nämnas rätten till information (artikel 13 och 14), rätten för den registrerade att få sina personuppgifter rättade eller raderade (artikel 16 och 17) samt en rätt att framställa invändningar mot en pågående behandling (artikel 21).

Bestämmelser om personuppgiftsansvarigas ansvar och om personuppgiftsbiträden m.m. finns i artiklarna 24–43.

I artikel 44 finns ett principiellt förbud att överföra personuppgifter som är under behandling eller är avsedda att behandlas efter det att de överförts till ett tredjeland eller en internationell organisation. Undantag från detta förbud föreskrivs i artiklarna 45, 46 och 49.

Slutligen ska nämnas att i artikel 51–99 i dataskyddsförordningen finns bestämmelser om bl.a. tillsynsmyndigheter och sanktioner för dem som inte följer bestämmelserna i förordningen.

Brottsdatalagen

Enligt brottsdatalagen får personuppgifter behandlas om det är nödvändigt för att en behörig myndighet ska utföra sin uppgift att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet (2 kap. 1 § första stycket). I likhet med vad som gäller för dataskyddsförordningen bygger brottsdatalagen på den grundläggande tanken att en personuppgiftsbehandling måste vila på en rättslig grund för att den ska vara laglig.

Liksom när det gäller behandling av personuppgifter enligt dataskyddsförordningen gäller att personuppgifter bara får behandlas för särskilda, uttryckligt angivna och berättigade ändamål (2 kap. 3 § första stycket).

Vissa särregler gäller för känsliga personuppgifter (1 kap. 11–14 §§). Vidare har de registrerade i vissa fall rätt till rättelse och radering av personuppgifter (1 kap. 15 och 16 §§).

I övrigt innehåller lagen bestämmelser om de personuppgiftsansvarigas skyldigheter (3 kap.), enskildas rättigheter (4 kap.), tillsyn (5 kap.), administrativa sanktionsavgifter (6 kap.), skadestånd och överklagande (7 kap.) och överföring av personuppgifter till tredjeland och internationella organisationer (8 kap.).

7.3 Det organisatoriska och avtalsmässiga förhållandet mellan den ansvarige och ett biträde

7.3.1 Roller vid behandling av personuppgifter

Den *personuppgiftsansvarige* är en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter (artikel 4.7). Om ändamålen och medlen för behandlingen bestäms av unionsrätten eller medlemsstaternas nationella rätt kan den personuppgiftsansvarige eller de särskilda kriterierna för hur denne ska utses föreskrivas i unionsrätten eller i medlemsstaternas nationella rätt (artikel 4.7 och skäl 45).

En förutsättning för dataskyddets upprätthållande är att det finns någon som är ansvarig för att reglerna följs. EU-domstolen har därför gett begreppet personuppgiftsansvarig en vid definition och en innebörd som bidrar till att säkerställa ett effektivt och komplett skydd för de personer vars uppgifter behandlas.[5]

Ett *personuppgiftsbiträde* är enligt dataskyddsförordningen en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning (artikel 4.8).

Den som behandlar personuppgifter på ett sätt som omfattas av dataskyddsförordningen utför alltid behandlingen i egenskap av antingen personuppgiftsansvarig eller personuppgiftsbiträde. Några andra roller vid personuppgiftsbehandling finns inte. En annan sak är att det enligt dataskyddsförordningen är möjligt att vara *mottagare* av personuppgifter, dvs. den som får personuppgifter utlämnade till sig, eller *tredje part* (artikel 4.9–10). En mottagare eller tredje part som utför en personuppgiftsbehandling för vilken dataskyddsförordningen tillämpas gör det i egenskap av antingen personuppgiftsansvarig eller personuppgiftsbiträde.

[5] Se bl.a. EU-domstolens dom av den 13 maj 2014, *Google Spain och Google*, C-131/12, ECLI:EU:C:2014:317, p. 34. Se även EU-domstolens dom av den 5 juni 2018, *Wirtschaftsakademie Schleswig-Holstein*, C-210/16, ECLI:EU:C:2018:388, p. 42, där domstolen gjorde bedömningen att, utifrån de omständigheter som var för handen i målet, ett gemensamt ansvar för behandlingen av personuppgifter bidrog till ett mer komplett skydd för de registrerade.

7.3.2 Myndigheters personuppgiftsansvar

Som vi nämner i avsnitt 7.2.6 ovan finns flera registerförfattningar som kompletterar dataskyddsförordningen och dataskyddslagen. Ibland följer det av registerförfattningen vilken myndighet som är personuppgiftsansvarig. Om en personuppgiftsbehandling omfattas av en registerförfattning och personuppgiftsansvaret regleras i registerförfattningen, ansvarar den myndighet som där utpekas som personuppgiftsansvarig för behandlingen av personuppgifter som regleras av registerförfattningen. Omfattas behandlingen av personuppgifter inte av registerförfattningen eller dess bestämmelse om personuppgiftsansvar så avgörs ansvaret utifrån den allmänna definitionen i dataskyddsförordningen.

I de fall personuppgiftsansvaret inte definieras i nationell rätt men där en myndighets verksamhet eller uppgifter regleras av nationell lagstiftning bör personuppgiftsansvaret härledas från nationell rätt genom den uppgift som ålagts den myndigheten.[6] Den myndighet som behandlar personuppgifter som ett led i att uppfylla en rättslig förpliktelse, för att utföra en uppgift av allmänt intresse eller som ett led i myndighetsutövning bör därmed som regel vara att anse som personuppgiftsansvarig för den personuppgiftsbehandlingen, mot bakgrund av kravet på att den rättsliga grunden för sådan behandling ska vara fastställd i enlighet med nationell rätt.

Beroende på om det finns en tillämplig registerförfattning och hur denna är utformad kan bestämmelser om personuppgiftsansvar i en registerförfattning omfatta handhavandet av it-drift. I vissa fall bör personuppgiftsansvaret kunna härledas från nationell rätt genom de uppgifter som ålagts myndigheten. I de fall det saknas tillämpliga bestämmelser om personuppgiftsansvar ska ansvaret bestämmas utifrån den allmänna definitionen.

Myndigheter bestämmer som utgångspunkt över mål och medel för den personuppgiftsbehandling som sker inom ramen för sin egen it-drift på ett sådant sätt att de som utgångspunkt bör vara att betrakta som personuppgiftsansvariga för den behandlingen. En särskild fråga som uppstår är hur personuppgiftsansvaret förhåller sig

[6] Se Artikel 29-gruppens vägledning *Opinion 1/2010 on the concepts of "controller" and "processor" (WP 169)*, antagen den 16 februari 2010. Som exempel nämns uppgiften att administrera socialförsäkring, som medför att personuppgifter måste behandlas för att denna uppgift ska kunna uppfyllas. I ett sådant fall härleds enligt artikel 29-gruppens vägledning personuppgiftsansvaret från nationell rätt genom den uppgift som ålagts den myndighet som administrerar socialförsäkringen.

när flera myndigheter samordnar sin it-drift. Vi avser att återkomma till den frågan i slutbetänkandet.

7.3.3 Personuppgiftsansvarets innebörd vid anlitande av ett personuppgiftsbiträde

Personuppgiftsansvaret innebär ett ansvar både för att efterleva dataskyddsförordningen och de nationella regler som meddelats med stöd av den, och att dokumentera de överväganden som görs och åtgärder som vidtas på ett sådant sätt att efterlevnaden kan påvisas. Detta följer av ansvarsskyldigheten (artikel 5.2).

Ansvarsskyldigheten innebär mer precist att den personuppgiftsansvarige med beaktande av behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter ska genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen utförs i enlighet med förordningen. De åtgärder som vidtas ska ses över och uppdateras vid behov (artikel 24.1). Ett sätt för den personuppgiftsansvarige att visa att denne fullgör sina skyldigheter är att tillämpa godkända uppförandekoder eller godkända certifieringsmekanismer (artikel 24.3).

När en personuppgiftsansvarig anlitar ett personuppgiftsbiträde ska det ske i enlighet med de regler som uppställs i dataskyddsförordningen. Det finns med utgångspunkt i ansvarsprincipen även anledning att dokumentera de överväganden som görs, avseende exempelvis val av biträde, på lämpligt sätt.

När det gäller val av biträde framgår det av dataskyddsförordningen att om en behandling ska genomföras för en personuppgiftsansvarigs räkning ska den personuppgiftsansvarige endast anlita personuppgiftsbiträden som ger tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i förordningen och säkerställer att den registrerades rättigheter skyddas (artikel 28.1). Av skäl 81 framgår att tillräckliga garantier ska ges i synnerhet i fråga om sakkunskap, tillförlitlighet och resurser.

Den personuppgiftsansvarige har med andra ord en omsorgsplikt vid val av biträde, som innefattar att göra en riskbedömning. Omsorgsplikten innebär att den personuppgiftsansvarige behöver utreda vilka förutsättningar personuppgiftsbiträdet har att efterleva sina

skyldigheter enligt dataskyddsregelverket. Eventuella skyldigheter som personuppgiftsbiträdet omfattas av enligt tredjelands lagstiftning att lämna ut personuppgifter till det landets myndigheter i strid med bestämmelserna om tredjelandsöverföring bör enligt vår uppfattning kunna tas i beaktande vid bedömningen av om personuppgiftsbiträdet kan ge tillräckliga garantier.

Ett personuppgiftsbiträde kan visa att sådana tillräckliga garantier tillhandahålls genom att ha anslutit sig till en godkänd uppförandekod eller en godkänd certifieringsmekanism (artikel 28.5).

7.3.4 Personuppgiftsbehandling för den ansvariges räkning

Det som är avgörande för att den som behandlar personuppgifter gör det i egenskap av personuppgiftsbiträde är att denne behandlar personuppgifter ”för den personuppgiftsansvariges räkning”. Det förekommer situationer där rollfördelningen i förhållande till en personuppgiftsbehandling framstår som oklar.

Europeiska dataskyddsstyrelsen, EDPB, har tagit fram en vägledning rörande begreppen personuppgiftsansvarig och personuppgiftsbiträde. I vägledningen framhålls att bedömningen av om det är fråga om ett biträdesförhållande beror på vilka konkreta aktiviteter som vidtas med personuppgifter i en specifik kontext. Bedömningen ska utgå från den tjänst som erbjuds. När tjänsten som erbjuds inte är specifikt inriktad på behandling av personuppgifter, eller där personuppgiftsbehandlingen inte utgör ett kärnelement i den tjänst som erbjuds, så kan tjänsteleverantören vara personuppgiftsansvarig för den personuppgiftsbehandling som tjänsteleverantören utför, beroende på att det då är mer troligt att det är tjänsteleverantören själv som bestämmer ändamål och medel för personuppgiftsbehandlingen.[7]

Tillhandahållande av it-drift kan innefatta många olika former av personuppgiftsbehandling. Oavsett vilken personuppgiftsbehandling som aktualiseras så innebär själva kärnan i uppdraget någon form av hantering av uppgifter för den personuppgiftsansvariga myndighetens räkning, genom exempelvis lagring. Tjänsteleverantören bör därför som utgångspunkt i förhållande till personuppgiftsbehandling som utförs som ett led i att tillhandahålla it-drift vara person-

[7] EDPB, *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*, version 1.0, beslutad den 02 september 2020, s. 25.

uppgiftsbiträde åt uppdragsgivande myndighet, som är personuppgiftsansvarig.

7.3.5 Personuppgiftsbiträdesavtalets form och innehåll

Av dataskyddsförordningen framgår att när uppgifter behandlas av ett personuppgiftsbiträde ska hanteringen regleras genom ett avtal eller en annan rättsakt enligt unionsrätten eller enligt medlemsstaternas nationella rätt som är bindande för personuppgiftsbiträdet med avseende på den personuppgiftsansvarige (artikel 28.3).

Det finns varken inom svensk rätt eller unionsrätten någon rättsakt med det innehåll som framgår av dataskyddsförordningen avseende förhållandet mellan den personuppgiftsansvarige och ett personuppgiftsbiträde som är tillämplig vid utkontraktering av it-drift. En myndighet som anlitar en privat tjänsteleverantör måste därför ingå ett personuppgiftsbiträdesavtal med tjänsteleverantören avseende personuppgiftsbehandlingen som denne kommer att utföra för myndighetens räkning. I det följande refereras mot denna bakgrund enbart till avtal mellan den personuppgiftsansvarige och personuppgiftsbiträdet.

Personuppgiftsbiträdesavtalet ska vara skriftligt (artikel 28.9) och kan helt eller delvis baseras på sådana standardavtalsklausuler som beslutas av kommissionen eller en tillsynsmyndighet (artikel 28.6–8).

I personuppgiftsbiträdesavtalet ska föremålet för behandlingen, behandlingens varaktighet, art och ändamål, typen av personuppgifter och kategorier av registrerade, samt den personuppgiftsansvariges skyldigheter och rättigheter anges (artikel 28.3). I dataskyddsförordningen föreskrivs dessutom följande rörande avtalets innehåll.

Det ska framgå att biträdet endast får behandla personuppgifter på dokumenterade instruktioner från den personuppgiftsansvarige, inbegripet när det gäller överföringar av personuppgifter till ett tredjeland eller en internationell organisation (artikel 28.3, led a).

Avtalet ska till sitt innehåll säkerställa att personer med behörighet att behandla personuppgifterna har åtagit sig att iaktta konfidentialitet eller omfattas av en lämplig lagstadgad tystnadsplikt (artikel 28.3, led b).

Det ska framgå av avtalet att personuppgiftsbiträdet ska vidta alla de tekniska och organisatoriska åtgärder som krävs enligt dataskyddsförordningen för att säkerställa en lämplig säkerhetsnivå (artikel 28.3 led c och artikel 32).

Personuppgiftsbiträdet ska vidare i avtalet åta sig att respektera de villkor som uppställs i avtalet för anlitande av ett annat personuppgiftsbiträde (underbiträde) (artikel 28.3, led d).

I avtalet ska biträdet även åläggas att hjälpa den personuppgiftsansvarige, genom lämpliga tekniska och organisatoriska åtgärder och om detta är möjligt, så att den personuppgiftsansvarige kan fullgöra sin skyldighet att svara på begäran om utövande av den registrerades rättigheter (artikel 28.3, led e).

Det ska av avtalet framgå att personuppgiftsbiträdet ska bistå den personuppgiftsansvarige med att se till att vissa i förordningen angivna skyldigheter avseende bl.a. säkerhet uppfylls (artikel 28, led f).

Avtalet ska reglera hanteringen av personuppgifter när biträdets uppdrag att behandla personuppgifter upphört (artikel 28, led g).

Personuppgiftsbiträdet ska dessutom i avtalet åläggas att ge den personuppgiftsansvarige tillgång till all information som krävs för att visa att de skyldigheter som fastställs i denna artikel har fullgjorts samt möjliggöra och bidra till granskningar, inbegripet inspektioner, som genomförs av den personuppgiftsansvarige eller av en annan revisor som bemyndigats av den personuppgiftsansvarige (artikel 28, led h).

7.3.6 Personuppgiftsbiträdets skyldigheter och ansvar

Personuppgiftsbiträdets uppgift är att behandla personuppgifter enligt den personuppgiftsansvariges instruktioner (artikel 29). Sådan personuppgiftsbehandling som går utöver den ansvariges instruktioner är inte tillåten. I personuppgiftsbiträdesavtalet regleras ytterligare skyldigheter för biträdet gentemot den ansvarige.

Utöver skyldigheten att enbart behandla personuppgifter enligt den ansvariges instruktioner och de skyldigheter som framgår av biträdesavtalet så innehåller dataskyddsförordningen vissa skyldigheter som direkt åligger personuppgiftsbiträdet.

Personuppgiftsbiträdet ska föra ett register över alla kategorier av behandling som utförts för den personuppgiftsansvariges räkning (artikel 30). Personuppgiftsbiträdet ska vidare på begäran samarbeta

med tillsynsmyndigheten vid utförandet av dennes uppgifter (artikel 31). Personuppgiftsbiträdet har ett självständigt ansvar för att vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken (artikel 32). Personuppgiftsbiträdet ska underrätta den personuppgiftsansvarige utan onödigt dröjsmål efter att ha fått vetskap om en personuppgiftsincident (artikel 33.2). Personuppgiftsbiträdet ska också under vissa omständigheter utse ett dataskyddsombud (artikel 37). Avslutningsvis innehåller dataskyddsförordningen bestämmelser som gäller när personuppgiftsbiträdet anlitar ett underbiträde (artikel 28.2 och 4).

Om personuppgiftsbiträdet inte uppfyller sina skyldigheter enligt dataskyddsförordningen kan biträdet bli föremål för administrativa sanktionsavgifter (artikel 83). Det finns även möjlighet för en registrerad att väcka talan mot ett personuppgiftsbiträde (artikel 79). Den registrerade har också rätt till ersättning från personuppgiftsbiträdet när skada inträffar som en följd av överträdelse av förordningens bestämmelser (artikel 83).

Personuppgiftsbiträden ska avslutningsvis i vissa fall utse en företrädare inom unionen (artikel 27.1).

7.3.7 Underbiträden

Ett personuppgiftsbiträde får inte anlita ett annat personuppgiftsbiträde (underbiträde) utan att ett särskilt eller allmänt skriftligt förhandstillstånd har erhållits av den personuppgiftsansvarige. Om ett allmänt skriftligt tillstånd har erhållits, ska personuppgiftsbiträdet informera den personuppgiftsansvarige om eventuella planer på att anlita nya personuppgiftsbiträden eller ersätta personuppgiftsbiträden, så att den personuppgiftsansvarige har möjlighet att göra invändningar mot sådana förändringar (artikel 28.2).

I de fall där ett personuppgiftsbiträde anlitar ett underbiträde för utförande av specifik behandling på den personuppgiftsansvariges vägnar ska underbiträdet genom ett avtal eller en annan rättsakt enligt unionsrätten eller enligt medlemsstaternas nationella rätt, åläggas samma skyldigheter i fråga om dataskydd som de som fastställs i avtalet eller den andra rättsakten mellan den personuppgiftsansvarige och personuppgiftsbiträdet, och framför allt att ge tillräck-

liga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i denna förordning. Om underbiträdet inte fullgör sina skyldigheter i fråga om dataskydd ska det ursprungliga personuppgiftsbiträdet vara fullt ansvarig gentemot den personuppgiftsansvarige för utförandet av det andra personuppgiftsbiträdets skyldigheter (artikel 28.4).

7.3.8 Behandlingar som går utöver den ansvariges instruktioner

Om ett personuppgiftsbiträde fastställer ändamålen med och medlen för behandlingen innebär det en överträdelse av dataskyddsförordningen och att personuppgiftsbiträdet blir personuppgiftsansvarig för den behandlingen (artikel 28.10).

Frågan är hur behandlingar som går utöver *den ansvariges instruktioner* förhåller sig till behandlingar för vilka *personuppgiftsbiträdet fastställer ändamål och medel* för personuppgiftsbehandlingen.

Den personuppgiftsansvarige får endast behandla personuppgifter som är adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas (artikel 5.1, led c). Det är inte otänkbart att en personuppgiftsbehandling som personuppgiftsbiträdet utför som går utöver den ansvariges instruktioner, men inte sker för ändamål som biträdet själv fastställt, ryms inom de tillåtna ramarna inom vilka den ansvarige får behandla personuppgifter. Så länge behandlingen inte sker för ändamål som biträdet själv fastställt, bör behandlingen inte kunna anses ske i strid med bestämmelsen i artikel 28.10. En sådan behandling skulle dock stå i strid med artikel 29. Den skulle dessutom ske i strid med villkoren i personuppgiftsbiträdesavtalet.

En behandling som innebär att personuppgiftsbiträdet behandlar uppgifter för ändamål som biträdet själv fastställt innebär att biträdet själv blir ansvarig för behandlingen, och kan därmed bli skyldig att betala sanktionsavgifter enbart på den grunden att det skett en överträdelse av artikel 28.10.

7.3.9 Reglering av inbördes ansvar och sanktioner

Inledning

Både tillsynsmyndighetens sanktionsmöjligheter och den registrerades ställning har stärkts genom dataskyddsförordningen. När det gäller relationen mellan den personuppgiftsansvarige och personuppgiftsbiträdet så innehåller dataskyddsförordningen väldigt få bestämmelser om vad som gäller när personuppgiftsbiträdet inte uppfyller sina skyldigheter i förhållande till den personuppgiftsansvarige. Detta får förutsättas regleras på avtalsmässig väg i relationen mellan de båda. Det finns dock anledning att beröra några regler som är av betydelse för relationen mellan den ansvarige och biträdet när biträdet inte uppfyller sina skyldigheter enligt dataskyddsförordningen i förhållande till den ansvarige.

Skadestånd

En personuppgiftsansvarig som behandlat personuppgifter på ett sätt som strider mot dataskyddsförordningen och därigenom orsakar skada ansvarar för skadan. Ett personuppgiftsbiträde ansvarar för skada uppkommen till följd av behandlingen endast om denne inte har fullgjort de skyldigheter enligt dataskyddsförordningen som specifikt riktar sig till personuppgiftsbiträden eller agerat utanför eller i strid med den personuppgiftsansvariges lagenliga anvisningar (artikel 82.2).

Den personuppgiftsansvarige ska lämna biträdet instruktioner för personuppgiftsbehandlingen (jfr artikel 28.3). Om personuppgiftsbiträdet anser att en instruktion strider mot dataskyddsförordningen eller mot andra av unionens eller medlemsstaternas dataskyddsbestämmelser ska biträdet omedelbart informera den ansvarige om detta (artikel 28.3). En sådan underrättelse bör rimligen kunna påverka personuppgiftsbiträdets ansvar för personuppgiftsbehandling som sker i strid med dataskyddsförordningen.

Personuppgiftsbiträdet är skyldigt att följa den ansvariges instruktioner. Detta förhållande skulle även kunna uttryckas som att den personuppgiftsansvarige har en ensidig rätt att lämna, och ändra redan lämnade, instruktioner. En annan sak är att en ändring av instruk-

tionerna kan påverka prissättningen för den tjänst som biträdet tillhandahåller den ansvarige.

Det går att tänka sig en situation där den personuppgiftsansvarige lämnar en instruktion som innebär att exempelvis tredjelandsöverföring av personuppgifter inte är tillåten. Om personuppgiftsbiträdet ändå genomför en tredjelandsöverföring så innebär detta att biträdet handlar i strid med den ansvariges instruktioner och personuppgiftsbiträdets bör då kunna hållas ansvarig för skada som drabbar den registrerade genom att tredjelandsöverföringen sker utan stöd i dataskyddsförordningen.

Om den ansvarige har vetskap om eller skäl att misstänka att personuppgiftsbiträdet överför personuppgifter till tredjeland i strid med den ansvariges instruktioner bör dock den ansvarige inte kunna undkomma i alla fall visst ansvar. Detta eftersom den personuppgiftsansvarige eller personuppgiftsbiträdet ska undgå ansvar endast om den visar att den inte på något sätt är ansvarig för den händelse som orsakade skadan (artikel 28.3).

En personuppgiftsansvarig och ett personuppgiftsbiträde som har medverkat vid samma behandling och som är ansvariga för eventuell skada som behandlingen orsakat är solidariskt ansvariga (artikel 82.4). Den av den ansvarige och biträdet som då har betalat full ersättning för skadan har rätt att från den andre som medverkat vid samma behandling återkräva den del av ersättningen som motsvarar dennes del av ansvaret för skadan (artikel 82.5).

Den ansvarige har sammanfattningsvis möjlighet att få ersättning för utlägg som den ansvarige gör för skador som personuppgiftsbiträdet orsakar när behandling av personuppgifter sker i strid med den personuppgiftsansvariges instruktioner.

Administrativa sanktionsavgifter

Tillsynsmyndigheten får påföra administrativa sanktionsavgifter vid överträdelser av dataskyddsförordningen (artikel 58.2 led i och artikel 83). Denna befogenhet finns både i förhållande till den personuppgiftsansvarige och personuppgiftsbiträdet, när biträdet inte uppfyller de skyldigheter i dataskyddsförordningen som riktar sig direkt till personuppgiftsbiträdet. Som exempel på när sanktionsavgifter kan utdömas gentemot ett personuppgiftsbiträde kan nämnas den

situationen då personuppgiftsbiträdet behandlat personuppgifter på något annat sätt än enligt den personuppgiftsansvariges instruktioner (artikel 83.4 led a som innehåller en hänvisning till artikel 29).

Det ska i sammanhanget framhållas att det i Sverige finns en beloppsmässig begränsning för sanktionsavgifter som utdöms i förhållande till myndigheter, som är väsentligt lägre än vad som gäller i förhållande till privata aktörer. Det finns en möjlighet för medlemsstaterna att fastställa regler om sanktionsavgifter för myndigheter (artikel 58.7). Sådana regler finns i dataskyddslagen, där det framgår att i förhållande till myndigheter får sanktionsavgifter bestämmas upp till 10 miljoner kronor (6 kap. 2 §). För ett personuppgiftsbiträde som inte omfattas av beloppsbegränsningen gäller att sanktionsavgifterna kan uppgå till 10 000 000 EUR eller på upp till 2 procent av ett företags totala globala årsomsättningen under föregående budgetår (artikel 58.4). I lagmotiven anges bl.a. följande som skäl för införandet av den beloppsmässiga begränsningen. Inom den privata sektorn kan en överträdelse av dataskyddsregleringen, förutom att kränka enskildas personliga integritet, medföra otillbörliga konkurrensfördelar som snedvrider den inre marknaden. Någon sådan ekonomisk vinning, på bekostnad av andra aktörer på marknaden, kan myndigheter inte dra. Dessutom lyfts att när det gäller institutionernas egen behandling av personuppgifter så gäller en beloppsgräns som är betydligt lägre än vad som gäller enligt dataskyddsförordningen (prop. 2017/18:105, s. 141).

Det förekommer avtalsklausuler som innebär att den personuppgiftsansvarige ska vara skyldig att ersätta personuppgiftsbiträdet när personuppgiftsbiträdet drabbats av en sanktionsavgift, där maxbeloppet är satt högre än de 10 miljoner kronor som gäller enligt dataskyddslagen. Det kan finnas anledning för en myndighet att överväga om det är lämpligt att godta sådana avtalsklausuler, mot bakgrund av att den svenska lagstiftaren gjort bedömningen att sanktionsavgifter som kan utdömas gentemot myndigheter ska uppgå till max 10 miljoner kronor.

7.4 Tredjelandsöverföring enligt dataskyddsförordningen

7.4.1 Inledning

Det ingår i vårt uppdrag att analysera de rättsliga förutsättningarna för utkontraktering av it-drift till privata tjänsteleverantörer med särskild uppmärksamhet på frågor som rör överföring av personuppgifter till tredjeland. Vi ska också redogöra för lagstiftning som hindrar eller försvårar för statliga myndigheter, kommuner och regioner att utkontraktera it-drift till privata leverantörer med bibehållen säkerhet.

Detta avsnitt innehåller en analys av de rättsliga förutsättningarna för överföring av personuppgifter till tredjeland, i ljuset av EU-domstolens senaste praxis avseende överföringar av personuppgifter till tredjeland.

Det bör inledningsvis poängteras att det är den personuppgiftsansvarige, och i vissa fall personuppgiftsbiträdet, som ska säkerställa att dataskyddsregleringen efterlevs. Det innebär att det är den personuppgiftsansvarige, dvs. myndigheten, som ska tolka regelverket och utifrån sin tolkning ta ställning till vilka åtgärder som lagligen kan vidtas med personuppgifter. Detta gäller även för överföringar av personuppgifter till tredjeland.

De nationella dataskyddsmyndigheterna kan gemensamt genom EDPB lämna råd, riktlinjer och rekommendationer avseende tolkningen och tillämpningen av reglerna i dataskyddsförordningen (artikel 70.1 led e). I slutändan är det dock EU-domstolen som avgör hur dataskyddsförordningens bestämmelser ska tolkas.

Det kan konstateras att dataskyddsförordningens regler om tredjelandsöverföring försvårar, och i vissa fall förhindrar, vissa former av utkontraktering, inte minst efter EU-domstolens avgörande i *Facebook Ireland och Schrems*. Det är dock enligt vår mening inte fråga om ett omotiverat förhindrande av utkontraktering. Vi ser inte heller att det är möjligt att vidta några författningsåtgärder på nationell nivå i fråga om tredjelandsöverföringar vid utkontraktering av it-drift till privata leverantörer eftersom dataskyddsförordningens regler inte lämnar något utrymme för nationell lagstiftning i dessa situationer.

7.4.2 Överföring av personuppgifter till tredjeland är bara tillåten i vissa fall

Det är enligt dataskyddsförordningen som utgångspunkt förbjudet att överföra personuppgifter till tredjeland, dvs. länder utanför EU och EES, och till internationella organisationer. Överföring av personuppgifter till tredjeland får bara ske om villkoren i dataskyddsförordningen för när sådan överföring är tillåten är uppfyllda (artikel 44).

Dataskyddsregelverket syftar till att skydda de registrerades personuppgifter. Ett fritt flöde av personuppgifter över gränserna till länder med endast ett svagt eller obefintligt skydd för enskildas fri- och rättigheter vid behandling av personuppgifter skulle urholka det skydd som dataskyddsförordningen är avsedd att ge.

Den som överför personuppgifter har inte bara att förhålla sig till bestämmelserna i femte kapitlet. Alla andra bestämmelser i dataskyddsförordningen måste också följas. Det innebär bl.a. att det måste finnas en rättslig grund för den personuppgiftsbehandlingen enligt artikel 6.

Det följer av förordningstexten att förbudet även gäller för vidare överföring av personuppgifter från det tredje landet eller den internationella organisationen till ett annat tredjeland eller en annan internationell organisation.

7.4.3 Vad avses med en tredjelandsöverföring av personuppgifter?

Utredningens bedömning: Det utgör en överföring av personuppgifter till tredjeland när en personuppgiftsansvarig eller ett personuppgiftsbiträde behandlar personuppgifter genom användning av utrustning som finns i tredjeland. Det saknar betydelse hur lång eller kort tid som utrustningen används och om uppgifterna är krypterade eller pseudonymiserade – det är alltjämt fråga om personuppgifter och en överföring av sådana uppgifter.

Allmänt

Vad som närmare ska förstås med att personuppgifter överförs till tredjeland är inte reglerat i dataskyddsförordningen. I skälen till förordningen anges att ”[d]et är viktigt att den skyddsnivå som fysiska personer säkerställs inom unionen genom denna förordning inte undergrävs när personuppgifter överförs från unionen till personuppgiftsansvariga, personuppgiftsbiträden eller andra mottagare i tredjeland […] vilket inbegriper vidarebefordran av personuppgifter från tredjelandet […] till personuppgiftsansvariga, personuppgiftsbiträden i samma eller ett annat tredjeland” (skäl 101).

Skrivningen tyder på att det inte bara är när personuppgifter överförs från en personuppgiftsansvarig eller ett personuppgiftsbiträde inom EU ochEES eller i ett tredjeland till en mottagare i ett annat tredjeland som det är fråga om en tredjelandsöverföring, utan även när en personuppgiftsansvarig eller ett personuppgiftsbiträde som finns i ett tredjeland för över personuppgifter till en mottagare i samma tredjeland.

Praxis från EU-domstolen avseende innebörden av tredjelandsöverföring

EU-domstolen har i sin praxis uttalat att åtgärden att låta överföra personuppgifter från en medlemsstat till ett tredjeland i sig utgör en behandling av personuppgifter (dom av den 6 oktober 2015, *Schrems*, C-362/14, EU:C:2015:650, punkt 45).

EU-domstolen har i övrigt i sin praxis mest utförligt behandlat innebörden av en tredjelandsöverföring i målet *Lindqvist* (dom av den 6 november 2003, C-101/01, EU:C:2003:596) där frågan gällde om en internetpublicering innebar att personuppgifter överfördes till tredjeland i den meningen som avsågs i artikel 25 i 1995 års dataskyddsdirektiv.[8]

I sitt svar på dessa frågor angav EG-domstolen att det inte föreligger någon ”överföring av … uppgifter till tredje land” i den mening som avses i artikel 25 i direktiv 95/46 när en person som befinner sig i en medlemsstat lägger ut personuppgifter som är lagrade på en

[8] Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter.

webbsida som i sin tur är lagrad hos en webbhotelleverantör som är etablerad i samma medlemsstat eller i en annan medlemsstat, varvid uppgifterna blir åtkomliga för alla som kopplar upp sig på Internet, inklusive personer i tredje land (p. 4 i domslutet).

EG-domstolen underströk särskilt att prövningen hade begränsats till frågan om Bodil Lindqvists åtgärder utgjorde en överföring av personuppgifter till tredjeland (p. 62). Det ska även noteras att domstolen i själva domslutet talade om en person som befinner sig i en medlemsstat (p. 4). Domstolen besvarade alltså endast frågan hur åtgärder som vidtas av en enskild individ och som leder till en internetpublicering sker ska bedömas. Domstolen tog uttryckligen inte ställning till frågan om webbhotelleverantörens åtgärder var att betrakta som en överföring.

Vår bedömning av innebörden av tredjelandsöverföring

En strikt läsning av domen i *Lindqvist* ger vid handen att internetpublicering inte utgör någon överföring av personuppgifter till tredjeland i den mening som avses i artikel 25 i 1995 års dataskyddsdirektiv givet att det är en enskild individ som publicerar uppgifterna, att den enskilda individen befinner sig i en medlemsstat och att webbhotelleverantören är etablerad i en medlemsstat.

Som vi bedömer saken måste det dock betraktas som en överföring av personuppgifter till tredjeland att en personuppgiftsansvarig eller ett personuppgiftsbiträde behandlar personuppgifter genom användning av utrustning som finns i tredjeland. Det saknar betydelse hur lång eller kort tid som utrustningen används. Inte heller har det någon betydelse i sammanhanget att uppgifterna är krypterade eller pseudonymiserade. Det är alltjämt fråga om personuppgifter och en överföring av sådana uppgifter. Av detta följer att det inte krävs – för att det ska vara fråga om en överföring – att uppgifterna lämnas ut till tredje part.[9]

Även om personuppgifterna hela tiden är under den personuppgiftsansvariges kontroll är det alltså fråga om en överföring när de förs över till tredjeland eller en internationell organisation.

[9] Jfr Sören Öman, Dataskyddsförordningen, artikel 44, Nordstedts Juridik (JUNO).

Det är också vår bedömning att det inte är fråga om en tredjelandsöverföring när personuppgifter behandlas uteslutande inom EU, även om den personuppgiftsansvarige eller personuppgiftsbiträdet som behandlar personuppgifterna är bunden av tredjelands lagstiftning som innebär att denne kan åläggas att lämna ut uppgifter direkt till ett tredjelands myndigheter. Tredjelandsöverföringen sker först i samband med att uppgifterna överförs till myndigheter eller annan mottagare i tredjeland. Däremot kan förekomsten av nämnda skyldigheter enligt vår uppfattning ha betydelse utifrån omsorgsplikten vid val av personuppgiftsbiträde (se avsnitt 7.3.3).

7.4.4 Överföring på grundval av ett beslut om adekvat skyddsnivå

Personuppgifter får överföras till tredjeland eller en internationell organisation om kommissionen har beslutat att tredjelandet, ett territorium eller en eller flera specificerade sektorer i tredjelandet, eller den internationella organisationen i fråga säkerställer en adekvat skyddsnivå (artikel 45.1). En överföring som sker på denna grund kräver inget särskilt tillstånd. Ett beslut om adekvat skyddsnivå fattas av kommissionen enligt artikel 45.3.

I artikel 45.2 finns regler om vilka faktorer som kommissionen ska beakta när den bedömer om det finns en adekvat skyddsnivå. Bestämmelsen innehåller tre led med en uppräkning av olika omständigheter som kommissionen ska ta hänsyn till i sin bedömning. Det första ledet (led a) tar sikte på respekten för rättsstatsprincipen och mänskliga rättigheter och grundläggande friheter liksom förekomsten av relevant lagstiftning och regler samt faktiska och verkställbara rättigheter för registrerade, inbegripet tillgång till effektiv administrativ och rättslig prövning för de registrerade vars personuppgifter överförs. Det andra ledet (led b) avser förekomsten av en eller flera effektivt fungerande oberoende tillsynsmyndigheter i det tredjelandet som har ansvar för att säkerställa och kontrollera att dataskyddsregler följs, och lämpliga verkställighetsbefogenheter. Det tredje ledet (led c) avser bl.a. förekomsten av internationella åtaganden som det berörda tredjelandet gjort.

Kommissionen har med stöd av motsvarande regler i 1995 års dataskyddsdirektiv fattat tolv beslut om adekvat skyddsnivå. Dessa beslut avser USA, Andorra, Argentina, Bailiwick of Guernsey, dvs.

öarna Guernsey, Alderney, Sark, Herm, Jethou, Brecqou och Lihou samt Färöarna, Isle of Man, Israel, Jersey, Kanada, Nya Zeeland, Schweiz och Uruguay. Av artikel 45.9 i dataskyddsförordningen följer att dessa beslut ska förbli i kraft tills de ändras, ersätts eller upphävs.

Hittills har kommissionen fattat ett beslut om adekvat skyddsnivå med stöd av artikel 45.3 i dataskyddsförordningen. Detta beslut avser Japan.

När det gäller USA antog kommissionen ett beslut redan år 2000 om adekvat skyddsnivå genom de s.k. Safe Harbor-principerna.[10] Beslutet innebar att det var tillåtet att överföra personuppgifter till organisationer i USA som anslutit sig till principerna och fanns upptagna i en särskild förteckning som offentliggjordes och förvaltades av USA:s handelsministerium. Beslutet innebar alltså ingen generell möjlighet att överföra personuppgifter till USA. Den 6 oktober 2015 ogiltigförklarades beslutet av EU-domstolen i *Schrems*.

Efter intensiva förhandlingar mellan kommissionen och USA antogs i juli 2016 ett nytt beslut om adekvat skyddsnivå genom den så kallade skölden för privatlivet.[11] Det senare av dessa beslut var i allt väsentligt konstruerat på samma sätt som det tidigare beslutet om adekvat skyddsnivå genom Safe Harbor-principerna. Även 2016 års beslut om adekvat skyddsnivå genom skölden för privatlivet ogiltigförklarades av EU-domstolen (dom av den 16 juli 2020, *Facebook Ireland och Schrems*, C-311/18, EU:C:2020:559).

7.4.5 Överföring som omfattas av lämpliga skyddsåtgärder

Utredningens bedömning: Standardavtalsklausuler är en lämplig skyddsåtgärd som kan läggas till grund för överföring av personuppgifter till tredjeland om det i mottagarens land finns ett grundläggande rättighetsskydd och en möjlighet att göra detta skydd gällande inför domstol eller annan oberoende instans.

[10] Kommissionens beslut av den 26 juli 2000 enligt Europaparlamentets och rådets direktiv 95/46/EG om huruvida ett adekvat skydd säkerställs genom de principer om integritetsskydd (Safe Harbor Privacy Principles) i kombination med frågor och svar som Förenta staternas handelsministerium utfärdat (2000/520/EG).

[11] Kommissionens genomförandebeslut (EU) 2016/1250 av den 12 juli 2016 enligt Europaparlamentets och rådets direktiv 95/46/EG om huruvida ett adekvat skydd säkerställs genom skölden för skydd av privatlivet i EU och Förenta staterna.

Allmänt

Om det inte finns något beslut om adekvat skyddsnivå kan överföring av personuppgifter till tredjeland eller en internationell organisation ske efter att den personuppgiftsansvarige eller personuppgiftsbiträdet som har för avsikt att överföra personuppgifter har vidtagit lämpliga skyddsåtgärder och på villkor att lagstadgade rättigheter för registrerade och effektiva rättsmedel för registrerade finns att tillgå (artikel 46.1).

I artikel 46.2 i dataskyddsförordningen finns en lista på lämpliga skyddsåtgärder som inte kräver något särskilt tillstånd av en tillsynsmyndighet för att användas. I listan nämns rättsligt bindande och verkställbara instrument mellan myndigheter (led a), bindande företagsbestämmelser (led b), standardiserade dataskyddsbestämmelser som antas av kommissionen eller av en tillsynsmyndighet, s.k. standardavtalsklausuler (led c och d), samt en godkänd uppförandekod eller en godkänd certifieringsmekanism tillsammans med rättsligt bindande och verkställbara åtaganden för den personuppgiftsansvarige eller personuppgiftsbiträdet i tredjelandet att tillämpa lämpliga skyddsåtgärder, även när det gäller registrerades rättigheter (led e och f).

I artikel 46.3 nämns ytterligare två skyddsåtgärder. Till skillnad från de skyddsåtgärder som listas i artikel 46.2 kräver dessa särskilt tillstånd av tillsynsmyndighet. Dessa skyddsåtgärder är avtalsklausuler mellan den personuppgiftsansvarige eller personuppgiftsbiträdet och den personuppgiftsansvarige, personuppgiftsbiträdet eller mottagaren av personuppgifterna i det tredjelandet eller den internationella organisationen (led a) eller bestämmelser som ska införas i administrativa överenskommelser mellan offentliga myndigheter eller organ vilka inbegriper verkställbara och faktiska rättigheter för registrerade (led b).

EDPB har gett ut riktlinjer när det gäller sådana skyddsåtgärder som avses i artikel 46.2 led a och artikel 46.3 led a.[12] Dessa skyddsåtgärder tar sikte på överföringar mellan myndigheter eller motsvarande. En myndighet som vill överföra personuppgifter till en tjänsteleverantör i tredjeland kan alltså inte använda dessa skyddsåtgärder.

[12] EDPB, *Guidelines 2/2020 on articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies*, antagna den 18 januari 2020.

Kommissionen har tidigare fattat beslut om standardavtalsklausuler.[13] Kommissionen publicerade den 12 november 2020 ett utkast till nya standardavtalsklausuler på sin webbplats.[14] De nya standardavtalsklausulerna får antas efter ett granskningsförfarande i en kommitté där medlemsstaterna finns representerade (artikel 46.2 led c som hänvisar till artikel 93.2, där det föreskrivs att granskningsförfarandet i artikel 5 i Europaparlamentets och rådets förordning /EU/ nr 182/2011 av den 16 februari 2011 om fastställande av allmänna regler och principer för medlemsstaternas kontroll av kommissionens utövande av sina genomförandebefogenheter ska tillämpas för beslutet).

I artikel 40, 42 och 47 finns detaljerade bestämmelser om bindande företagsbestämmelser, godkända uppförandekoder och certifieringsmekanismer. Den förstnämnda av dessa skyddsåtgärder tar sikte på överföring av personuppgifter inom en internationell koncern eller en internationell grupp av företag. Skyddsåtgärden kan alltså inte användas av en myndighet som vill överföra personuppgifter till en privat tjänsteleverantör i tredjeland. Det finns såvitt vi känner till ännu inte några godkända uppförandekoder eller certifieringsmekanismer som svenska myndigheter kan använda sig av för att föra över personuppgifter till länder utanför EU eller EES.

Den grund i artikel 46 som är tillämplig för svenska myndigheters överföring av personuppgifter till tredjeland är sammanfattningsvis standardavtalsklausuler enligt artikel 46.2 led c och d.

När är standardavtalsklausuler en lämplig skyddsåtgärd?

Det följer av förordningstexten i artikel 46.1 att det inte räcker att den personuppgiftsansvarige eller personuppgiftsbiträdet som har för avsikt att överföra personuppgifter till tredje land har vidtagit lämpliga skyddsåtgärder. Överföringen får bara ske på villkor ”att

[13] Kommissionens beslut 2001/497/EG av den 15 juni 2001 om standardavtalsklausuler för överföring av personuppgifter till tredje land enligt direktiv 95/46/EG, kommissionens beslut 2010/87/EU av den 5 februari 2010 om standardavtalsklausuler för överföring av personuppgifter till registerförare etablerade i tredjeland i enlighet med Europaparlamentets och rådets direktiv 95/46/EG och kommissionens genomförandebeslut (EU) 2016/2297 av den 16 december 2016 om ändring av beslut 2001/497/EG och 2010/87/EU rörande standardavtalsklausuler för överföring av personuppgifter till tredjeländer och till registerförare etablerade i tredjeländer i enlighet med Europaparlamentets och rådets direktiv 95/46/EG.

[14] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Commission-Implementing-Decision-on-standard-contractual-clauses-for-the-transfer-of-personal-data-to-third-countries, besökt 2020-11-23.

lagstadgade rättigheter för registrerade och effektiva rättsmedel för registrerade finns tillgängliga". Det förefaller alltså krävas att det i mottagarlandet finns ett grundläggande rättighetsskydd och en möjlighet att göra detta skydd gällande inför domstol, för att en tredjelandsöverföring med stöd av standardavtalsklausuler ska kunna komma i fråga. Denna tolkning vinner enligt vår mening stöd av EU-domstolens uttalanden som redovisas i det följande.

När det gäller frågan om vilken nivå av skydd som krävs för de tre kriterierna "lämpliga skyddsåtgärder", "lagstadgade rättigheter" och "effektiva rättsmedel" så uttalade EU-domstolen följande i rättsfallet *Facebook Ireland och Schrems*. Det krävs samma nivå av skydd för fysiska personer oavsett vilken grund enligt dataskyddsförordningen som åberopas för överföringen av personuppgifter (p. 92). Kravet på skyddsnivå är alltså detsamma när kommissionen fattar ett beslut om adekvat skyddsnivå enligt artikel 45.3 som när en personuppgiftsansvarige eller ett personuppgiftsbiträde för över personuppgifter med stöd av lämpliga skyddsåtgärder enligt artikel 46.

Vidare konstaterar domstolen att när det gäller kravet på "adekvat skyddsnivå", det inte krävs att det berörda tredjelandet säkerställer en skyddsnivå som är identisk med den som garanteras i unionens rättsordning. Kravet på adekvat skyddsnivå ska förstås som att tredjelandet, genom sin interna lagstiftning eller på grund av de internationella förpliktelser som åligger landet, de facto säkerställer en nivå för skyddet av grundläggande fri- och rättigheter som är *väsentligen likvärdig* med den skyddsnivå som garanteras inom unionen enligt förordningen, jämförd med stadgan (p. 94). Detsamma gäller vid användande av standardavtalsklausuler som grund för överföring till tredjeland (p. 96).

Skyddsnivån ska fastställas utifrån dataskyddsförordningen, jämförd med de grundläggande rättigheter som garanteras i stadgan (p. 101). När det gäller frågan om vilka omständigheter som ska beaktas i bedömningen av skyddsnivån så ska, utöver avtalsvillkoren, hänsyn tas till "de relevanta delarna av rättssystemet i det tredjelandet såvitt avser den åtkomst som myndigheterna i det tredjelandet eventuellt har till överförda personuppgifter". Ledning för denna bedömning kan hämtas i artikel 45.2 (se avsnitt 7.4.3) (p. 104). EDPB ger också i rekommendationer som beslutades den 10 november 2020 vägledning avseende hur bedömningen av om övervakning av bl.a.

datatrafik i tredjeland innebär ett godtagbart ingripande i skyddet för fysiska personers rättigheter vid behandling av personuppgifter.[15]

Vi drar slutsatsen av domstolens uttalanden i *Facebook Ireland och Schrems* att standardavtalsklausuler är en lämplig skyddsåtgärd som kan läggas till grund för överföring av personuppgifter endast när rättssystemet i det berörda tredjelandet erbjuder en viss nivå av skydd för de registrerade som berörs av tredjelandsöverföringen. Denna slutsats stöds av domstolens uttalande att det finns situationer i vilka standardavtalsklausuler inte kan vara ett tillräckligt medel för att i praktiken säkerställa ett effektivt skydd av de personuppgifter som överförs till det berörda tredjelandet, exempelvis beroende på att lagstiftningen i det tredjelandet tillåter att myndigheterna i detta tredjeland gör ingrepp i de registrerade personernas rättigheter avseende dessa uppgifter (p. 126).

Domstolen konstaterar avslutningsvis att samtliga skyddsåtgärder enligt artikel 46.2 inte nödvändigtvis måste föreskrivas i ett beslut av kommissionen, såsom beslutet om standardavtalsklausuler (p. 128). Eftersom de standardiserade dataskyddsbestämmelserna inte kan leda till skyddsåtgärder som går utöver en avtalsenlig skyldighet att säkerställa att den skyddsnivå som krävs enligt unionsrätten iakttas, kan det vara nödvändigt, beroende på den situation som råder i ett visst tredjeland, för den personuppgiftsansvarige att vidta ytterligare åtgärder för att säkerställa att skyddsnivån iakttas (p. 133).

EDPB:s rekommendationer om ytterligare skyddsåtgärder

EU-domstolen uttalar, som konstaterats ovan, i *Facebook Ireland och Schrems* att det kan krävas ytterligare skyddsåtgärder som kompletterar standardavtalsklausulerna för att uppnå rätt skyddsnivå (p. 133–134). EDPB har lämnat rekommendationer om sådana ytterligare skyddsåtgärder.[16]

EDPB:s rekommendationer synes utgå från att det kan finnas situationer då det är tillräckligt att den personuppgiftsansvarige eller personuppgiftsbiträdet vidtar ytterligare skyddsåtgärder som komplement till standardavtalsklausulerna, oavsett vilken nivå av grundläggande rättighetsskydd och tillgång till rättslig prövning som finns i

[15] EDPB, *Recommendations 02/2020 on the European Essential Guarantees for surveillance measures*.
[16] EDPB, *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*.

det berörda tredjelandet. På sidan 15 i rekommendationerna anges exempelvis att vid överföringar som berörs av sektion 702 i Foreign Intelligence Surveillance Act (FISA) i USA eller liknande övervakningsprogram så kan tredjelandsöverföringen vara tillåten om ytterligare skyddsåtgärder vidtas som gör försök att få obehörig åtkomst till personuppgifterna verkningslösa.

Vi anser dock att det följer av såväl förordningstexten som av EU-domstolens uttalanden i *Facebook Ireland och Schrems* att det krävs att det i mottagarlandet finns ett grundläggande rättighetsskydd och en möjlighet att göra detta skydd gällande inför domstol eller annan oberoende instans, för att en tredjelandsöverföring med stöd av standardavtalsklausuler ska kunna komma i fråga. Domstolen uttalar särskilt att ytterligare skyddsåtgärder inte kan säkerställa den skyddsnivå som krävs när lagstiftningen i det tredjelandet ålägger mottagaren av personuppgifterna skyldigheter som strider mot standardavtalsklausulerna. Orsaken är att sådana skyldigheter kan äventyra den avtalsenliga garantin om adekvat skydd mot att offentliga myndigheter i det berörda tredjelandet får åtkomst till dessa uppgifter (p. 135).

I bilaga 2 till EDPB:s rekommendationer finns exempel på ytterligare skyddsåtgärder i form av tekniska, avtalsmässiga och organisatoriska åtgärder. Användningsfall sex på sidan 26 i rekommendationerna gäller överföring till molntjänstleverantörer eller andra personuppgiftsbiträden som kräver behandling av uppgifter i läsbart format för att kunna utföra sitt uppdrag. Om tredjelandets myndigheters rätt till tillgång till uppgifterna som överförs går utöver vad som är nödvändigt och proportionerligt i ett demokratiskt samhälle så anser EDPB att det saknas tillgång till tekniska åtgärder som kan ge ett tillräckligt skydd för registrerades rättigheter. Detta, framhåller EDPB, gäller även om kryptering tillämpas både under transport och vid lagring.

Vi tolkar detta användningsfall som att det är avsett att omfatta alla tjänster som kräver behandling av okrypterade personuppgifter, dvs. inte bara sådana tjänster där mottagarens personal aktivt behöver ta del av personuppgifter (t.ex. vid support) för att kunna utföra sitt uppdrag. Det innebär i så fall att EDPB anser att det inte finns några ytterligare tekniska skyddsåtgärder som kan bidra till ett adekvat skydd vid användning av sådana tjänster som träffas av användningsfallet, när tredjelandets myndigheters rätt till tillgång till

uppgifterna som överförs går utöver vad som är nödvändigt och proportionerligt i ett demokratiskt samhälle.

I användningsfall tre behandlar EDPB situationen då uppgifter som är destinerade till ett tredjeland som omfattas av ett kommissionsbeslut om adekvat skyddsnivå överförs via internet och dirigeras via tredjeländer som inte omfattas av sådana kommissionsbeslut. Under vissa förutsättningar anser EDPB att kryptering kan vara en ytterligare skyddsåtgärd som är tillräcklig för att överföringen ska kunna ske i enlighet med dataskyddsförordningen. En fråga som infinner sig är om EDPB:s rekommendationer ska förstås som att det alltid krävs att tekniska skyddsåtgärder vidtas när uppgifter överförs via internet, eftersom det aldrig vid sändningstillfället med säkerhet går att förutse hur uppgifterna kommer att dirigeras under överföringen till mottagaren.

7.4.6 Överföringar och utlämnanden som inte är tillåtna enligt unionsrätten

Av artikel 48 följer att domstolsbeslut eller beslut från myndigheter i tredjeland där det krävs att en personuppgiftsansvarig eller ett personuppgiftsbiträde överför eller lämnar ut personuppgifter får erkännas eller genomföras på något som helst sätt endast om det grundar sig på en internationell överenskommelse, såsom ett avtal om ömsesidig rättslig hjälp, som gäller mellan det begärande tredjelandet och unionen eller en medlemsstat, utan att detta påverkar andra grunder för överföring enligt detta kapitel.

En begäran om utlämnande av uppgifter från en domstol eller en myndighet i ett tredjeland kan alltså inte åberopas som en grund för att överföra personuppgifter till tredjeland. Artikeln innebär dock inget förbud mot ett sådant utlämnande om det kan ske med stöd av någon av bestämmelserna i kapitlet (jfr skäl 115 sista meningen).

7.4.7 Undantag i särskilda situationer

Om det inte finns något beslut om adekvat skyddsnivå och om en överföring av personuppgifter till tredjeland eller en internationell organisation inte heller kan grundas på förekomsten av lämpliga skyddsåtgärder får en överföring eller en uppsättning av överföringar

ske till ett tredjeland eller en internationell organisation enligt första stycket i artikel 49.1 på följande villkor:

- Den registrerade har uttryckligen samtyckt till att uppgifterna får överföras, efter att först ha blivit informerade om de eventuella riskerna med sådana överföringar för den registrerade (led a).
- Överföringen är nödvändig för att fullgöra ett avtal mellan den registrerade och den personuppgiftsansvarige eller för att genomföra åtgärder som föregår ett sådant avtal på den registrerades begäran (led b).
- Överföringen är nödvändig för att ingå eller fullgöra ett avtal mellan den personuppgiftsansvarige och en annan fysisk eller juridisk person i den registrerades intresse (led c).
- Överföringen är nödvändig av viktiga skäl som rör allmänintresset (led d).
- Överföringen är nödvändig för att kunna fastställa, göra gällande eller försvara rättsliga anspråk (led e).
- Överföringen är nödvändig för att kunna skydda den registrerades eller andra personers grundläggande intressen, när den registrerade är fysiskt eller rättsligt förhindrad att ge sitt samtycke (led f).
- Överföringen görs från ett register som enligt unionsrätten eller medlemsstaternas nationella rätt är avsett att ge allmänheten information och som är tillgängligt antingen för allmänheten eller för var och en som kan styrka ett berättigat intresse, men endast i den utsträckning som de i unionsrätten eller medlemsstaternas nationella rätt angivna villkoren för tillgänglighet uppfylls i det enskilda fallet (led g).

Av andra stycket i artikel 49.1 följer att när en överföring inte skulle kunna grundas på en bestämmelse i artikel 45 eller 46 och inget av undantagen för en särskild situation som avses i första stycket i samma punkt är tillämpligt, får en överföring till ett tredjeland eller en internationell organisation äga rum endast om överföringen inte är repetitiv, endast gäller ett begränsat antal registrerade, är nödvändig för ändamål som rör den personuppgiftsansvariges tvingande berättigade intressen och den registrerades intressen eller rättigheter och friheter inte väger tyngre, och den personuppgiftsansvarige har

bedömt samtliga omständigheter kring överföringen av uppgifter och på grundval av denna bedömning vidtagit lämpliga skyddsåtgärder för att skydda personuppgifter.

En överföring enligt första stycket artikel 49.1 led g får inte omfatta alla personuppgifter eller hela kategorier av personuppgifter som finns i registret (artikel 49.2).

Undantagsbestämmelserna i artikel 49.1 led a, b och c samt andra stycket får inte användas av offentliga myndigheter när de vidtar åtgärder som ett led i deras myndighetsutövning (artikel 49.3).

Det allmänintresse som avses i artikel 49.1 led d ska vara erkänt i unionsrätten eller i den nationella rätt som den personuppgiftsansvarige omfattas av (artikel 49.4).

Artikel 49 reglerar undantag från förbudet mot överföring av personuppgifter till tredjeland i *särskilda situationer*, och det anges särskilt i artikeln att de särskilda undantagen är avsedda att användas när det inte är möjligt att överföra uppgifterna på grundval av artikel 45 eller artikel 46. Tillämpning av artikel 49 är alltså avsedd endast i undantagsfall. Enligt EU-domstolens praxis ska undantag från och begränsningar av skyddet för personuppgifter inskränkas till vad som är strängt nödvändigt.[17]

Avslutningsvis får medlemsstaterna, om det saknas beslut om adekvat skyddsnivå, i sin nationella rätt med hänsyn till viktiga allmänintressen, uttryckligen fastställa gränser för överföringen av specifika kategorier av personuppgifter till ett tredjeland eller en internationell organisation. Medlemsstaterna ska underrätta kommissionen om sådana bestämmelser (artikel 49.5).

[17] Se bl.a. dom av den 16 december 2008, *Satakunnan Markkinapörssi och Satamedia*, C-73/07, EU:C:2008:727, p. 56; dom av den 9 november 2010, *Volker und Markus Schecke och Eifert*, C-92/09 och C-93/09, EU:C:2010:662, p. 77; dom av den 8 april 2014, *Digital Rights Ireland och Seitlinger m.fl.*, C-293/12, EU:C:2014:238, p. 52; *Schrems*, p. 92; och dom av den 21 december 2016, *Tele2 Sverige*, C-203/15, EU:C:2016:970, p. 96).

7.4.8 Rättsläget avseende överföringar av personuppgifter till USA

Utredningens bedömning: EU-domstolens konstateranden i *Facebook Ireland och Schrems* avseende rättsläget i USA vad gäller inskränkningar av grundläggande rättigheter och tillgången till rättsmedel och oberoende prövning äger giltighet även i förhållande till övriga grunder för överföring av personuppgifter till USA enligt dataskyddsförordningen, eftersom kravet på skyddsnivå är detsamma oavsett vilken grund för överföringen som tillämpas. Vi har mot denna bakgrund svårt att se att det i en situation som gäller tredjelandsöverföring vid utkontraktering av it-drift finns några ytterligare skyddsåtgärder som kan vidtas som läker de brister som EU-domstolen i *Facebook Ireland och Schrems* bedömer finns i amerikansk lagstiftning.

EU-domstolen har bedömt att det inte finns en adekvat skyddsnivå för personuppgifter i USA

Som vi beskriver i avsnitt 7.4.3 så ogiltigförklarade EU-domstolen 2016 års beslut om adekvat skydd genom skölden för privatlivet i *Facebook Ireland och Schrems*. Sedan EU-domstolen ogiltigförklarat beslutet är det inte längre möjligt att föra över personuppgifter till USA på den grunden.

EU-domstolens bedömning av skyddsnivån i USA får betydelse även för andra grunder för överföring

Mot bakgrund av ovanstående återstår möjligheten att föra av personuppgifter med stöd av lämpliga skyddsåtgärder enligt artikel 46 eller att tillämpa de undantag för särskilda situationer som regleras i artikel 49.

När det gäller möjligheten att använda sig av standardavtalsklausuler och undantaget i artikel 49 som grund för överföring av personuppgifter till USA kan följande konstateras utifrån EU-domstolen uttalanden i *Facebook Ireland och Schrems*.

För det första konstaterar domstolen att bedömningen av giltigheten av beslut om adekvat skydd genom skölden för privatlivet har relevans även för bedömningen av de skyldigheter som åligger den personuppgiftsansvarige och mottagaren av personuppgifter med stöd av de standardiserade dataskyddsbestämmelserna (p. 154). Detta konstaterande får förstås i ljuset av att domstolen i domskälen även uttalar att den skyddsnivå som krävs för att en överföring av personuppgifter till tredjeland ska vara tillåten är densamma oavsett på vilken grund för överföringen som tillämpas (se ovan avsnitt 7.4.4). Domstolens bedömning av giltigheten av beslutet om adekvat skydd genom skölden för privatlivet har därför betydelse även för möjligheten att föra över personuppgifter till USA på andra grunder i dataskyddsförordningen.

För det andra gör domstolen bedömningen att de inskränkningar av grundläggande rättigheter som vissa övervakningsprogram som tillämpas av amerikanska myndigheter innebär inte är begränsade till vad som är strikt nödvändigt, eftersom de interna bestämmelser som övervakningsprogrammen grundar sig på inte motsvarar de minimikrav som i unionsrätten gäller enligt proportionalitetsprincipen (p. 184). Därför är de begränsningar av skyddet av personuppgifter som överförts till USA inte reglerade på ett sådant sätt att de uppfyller krav som är väsentligen likvärdiga med dem som uppställs i unionsrätten (p. 185).

För det tredje konstaterar domstolen att det saknas tillgång till ett sådant rättsmedel som kan användas inför ett organ som ger personer vars uppgifter överförs till USA garantier som är väsentligen likvärdiga med dem som krävs enligt unionsrätten (p. 197).

Det grundläggande rättsskyddet i USA ger med andra ord inte en sådan nivå av skydd som krävs enligt dataskyddsförordningen. EU-domstolen ogiltigförklarar därför beslutet om skölden för privatlivet (p. 201).

Vår bedömning är att domstolens konstateranden avseende rättsläget i USA vad gäller inskränkningar av grundläggande rättigheter och tillgången till rättsmedel och oberoende prövning äger giltighet även i förhållande till övriga grunder för överföring av personuppgifter till USA enligt dataskyddsförordningen, eftersom kravet på skyddsnivå är densamma oavsett vilken grund som tillämpas. Vi har mot denna bakgrund svårt att se att det i en situation som gäller tredjelandsöverföring vid utkontraktering av it-drift finns några ytter-

ligare skyddsåtgärder som kan vidtas som läker de brister som EU-domstolen i *Facebook Ireland och Schrems* bedömer finns i amerikansk lagstiftning.

7.5 Tredjelandsöverföringar enligt brottsdatalagen

Bestämmelser om överföring av personuppgifter till tredjeland och internationella organisationer finns i 8 kap. brottsdatalagen.

En behörig myndighet får under vissa förutsättningar överföra personuppgifter till ett tredjeland eller en internationell organisation, om personuppgifterna behandlas i Sverige eller är avsedda att behandlas i ett tredjeland eller av en internationell organisation (1 § första stycket). För att överföringen ska vara tillåten krävs *för det första* att den är nödvändig för att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet (1 § första stycket p. 1). Överföringen måste alltså vara nödvändig för ett syfte som omfattas av lagens tillämpningsområde. *För det andra* krävs att överföringen riktas till en behörig myndighet i ett tredjeland eller till en internationell organisation som är en behörig myndighet (1 § första stycket p. 2). Slutligen och *för det tredje* krävs att överföring omfattas av ett beslut om adekvat skyddsnivå, tillräckliga skyddsåtgärder och ett undantag för särskilda situationer (1 § första stycket p. 3 a–c).

Vad som närmare ska förstås med ett beslut om adekvat skyddsnivå, tillräckliga skyddsåtgärder och undantag för särskilda situationer regleras i 3–5 §§. Dessa regler är i huvudsak uppbyggda på samma sätt som motsvarande regler i dataskyddsförordningen.

I 2 § regleras den situationen att en svensk myndighet har fått personuppgifter från en annan medlemsstat. Sådana personuppgifter får överföras till tredjeland eller en internationell organisation endast om den myndighet som har lämnat uppgifterna till en svensk myndighet har medgett att de överförs (första stycket). Om medgivande på grund av tidsbrist inte kan inhämtas i förväg får personuppgifterna ändå överföras om det är nödvändigt för att avvärja en omedelbar och allvarlig fara för allmän säkerhet. Detsamma gäller om det är nödvändigt för att avvärja en omedelbar och allvarlig fara

för andra väsentliga intressen för Sverige eller någon annan medlemsstat (andra stycket).

I 6 och 7 §§ finns regler om vad som gäller för vidareöverföring av sådana personuppgifter som avses i 2 §.

Av 8 § första stycket följer att en behörig myndighet i Sverige i vissa undantagsfall får överföra personuppgifter till andra än behöriga myndigheter. En sådan överföring får ske bl.a. om det är absolut nödvändigt för att den svenska myndigheten ska kunna utföra en uppgift enligt 1 kap. 2 § som den har ansvar för.

7.6 Sammanfattning och våra samlade bedömningar

Det här kapitlet innehåller en genomgång av de delar av dataskyddsregelverket som i våra direktiv utpekas som särskilt centrala vid utkontraktering av it-drift. En viktig utgångspunkt för tillämpningen av reglerna är att det är den personuppgiftsansvarige som har ansvaret för att de personuppgifter som behandlas under dennes ansvar hanteras i enlighet med dataskyddsregleringen.

När den ansvarige uppdrar åt ett personuppgiftsbiträde att behandla personuppgifter å den ansvariges vägnar så är det den ansvarige som ska lämna biträdet instruktioner för behandlingen. Detta är enligt vår mening en central utgångspunkt i relationen mellan den personuppgiftsansvarige och personuppgiftsbiträdet.

Överföring av personuppgifter till tredjeland är en behandling av personuppgifter som bara är tillåten i de fall som anges i dataskyddsförordningens femte kapitel.

Vår bedömning är att det utgör en överföring av personuppgifter till tredjeland när en personuppgiftsansvarig eller ett personuppgiftsbiträde behandlar personuppgifter genom användning av utrustning som finns i tredjeland. Det saknar betydelse hur lång eller kort tid som utrustningen används, och om uppgifterna är krypterade eller pseudonymiserade – det är alltjämt fråga om personuppgifter och en överföring av sådana uppgifter.

Standardavtalsklausuler är en lämplig skyddsåtgärd som kan läggas till grund för överföring av personuppgifter till tredjeland om det i mottagarens land finns ett grundläggande rättighetsskydd och en möjlighet att göra detta skydd gällande inför domstol eller annan oberoende instans.

EU-domstolens konstateranden i *Facebook Ireland och Schrems* avseende rättsläget i USA vad gäller inskränkningar av grundläggande rättigheter och tillgången till rättsmedel och oberoende prövning äger enligt vår mening giltighet även i förhållande till övriga grunder för överföring av personuppgifter till USA enligt dataskyddsförordningen, eftersom kravet på skyddsnivå är detsamma oavsett vilken grund för överföringen som tillämpas. Vi har mot denna bakgrund svårt att se att det i en situation som gäller tredjelandsöverföring vid utkontraktering av it-drift finns några ytterligare skyddsåtgärder som kan vidtas som läker de brister som EU-domstolen i *Facebook Ireland och Schrems* bedömer finns i amerikansk lagstiftning.

8 Offentlighet, sekretess och tystnadsplikt

8.1 Inledning

Vi ska enligt direktiven bl.a. kartlägga de rättsliga förutsättningarna för myndigheter[1] att utkontraktera it-drift. En central fråga i det sammanhanget är om de uppgifter som omfattas av en utkontraktering ska betraktas som röjda enligt offentlighets- och sekretesslagen (2009:400) OSL.

Det är inte möjligt att besvara denna fråga utan att dessförinnan analysera röjandebegreppets innebörd. I det följande gör vi inledningsvis en översiktlig genomgång av reglerna om offentlighet, sekretess och tystnadsplikt (avsnitt 8.2–8.8). Därefter följer en analys av röjandebegreppet i OSL med utgångspunkt i lagtext, lagmotiv, praxis och litteratur (avsnitt 8.9).

8.2 Allmänna handlingar

Var och en har enligt 2 kap. 1 § tryckfrihetsförordningen (TF) rätt att ta del av allmänna handlingar. En handling är enligt 2 kap. 4 § TF allmän om den förvaras hos en myndighet och enligt 9 § eller 10 § är att anse som inkommen till eller upprättad hos myndigheten. En upptagning, t.ex. en elektronisk handling, anses enligt 2 kap. 6 § TF vara förvarad hos myndigheten, om upptagningen är tillgänglig för myndigheten med tekniskt hjälpmedel som myndigheten själv utnyttjar för överföring i sådan form att den kan läsas, avlyssnas eller uppfattas på annat sätt.

[1] Med myndigheter avses i detta kapitel statliga myndigheter, kommuner och regioner om inget annat framgår av sammanhanget.

En handling anses ha kommit in till en myndighet, när den har anlänt till myndigheten eller kommit behörig befattningshavare till handa (2 kap. 9 § första stycket TF). I fråga om upptagning gäller i stället att den anses ha kommit in till myndigheten när någon annan har gjort den tillgänglig för myndigheten med tekniskt hjälpmedel som myndigheten själv utnyttjar för överföring i sådan form att den kan läsas eller avlyssnas eller uppfattas på annat sätt (2 kap. 6 § TF). En handling anses upprättad hos en myndighet när den har expedierats, eller om den inte har expedierats, när det ärende som den hänför sig till har slutbehandlats hos myndigheten eller, om handlingen inte hänför sig till visst ärende, när den har justerats av myndigheten eller färdigställts på annat sätt (2 kap. 10 § TF).

Från bestämmelsen om när en handling anses inkommen görs undantag i 2 kap. 9 § tredje stycket TF. En åtgärd som någon vidtar endast som ett led i en teknisk bearbetning eller teknisk lagring av en handling som en myndighet har tillhandahållit ska inte anses leda till att handlingen har kommit in till myndigheten. Bestämmelsen reglerar alltså den situationen att en icke allmän handling, som någon har bearbetat eller lagrat tekniskt, återkommer till den myndighet som tillhandahöll den. Handlingen ska vid återkomsten inte anses vara inkommen. Syftet med detta är att förhindra att en handling endast på grund av att den skickats för teknisk bearbetning eller teknisk lagring ändrar karaktär och blir allmän, dvs. bestämmelsen avser att bevara handlingens status, inte att ändra den. Handlingens status hos en mottagande myndighet regleras av en annan bestämmelse i TF nämligen 2 kap. 13 § första stycket TF (jfr HFD 2019 ref. 24 p. 23).

En handling som förvaras hos en myndighet endast som ett led i en teknisk bearbetning eller teknisk lagring för någon annans räkning anses inte som allmän handling hos den myndigheten (2 kap. 13 § första stycket TF).

Rätten att ta del av allmänna handlingar får begränsas bara om det är nödvändigt med hänsyn till vissa, särskilt angivna, intressen (2 kap. 2 § första stycket TF). En sådan begränsning ska anges noga i en bestämmelse i en särskild lag eller, om det i ett visst fall anses lämpligare, i en annan lag som den förstnämnda lagen hänvisar till (2 kap. 2 § andra stycket TF). Den särskilda lag som avses är OSL.

8.3 Några definitioner

I 3 kap. § OSL definieras några i lagen förekommande centrala begrepp.

Sekretess definieras som ett förbud mot att röja en uppgift, vare sig det sker muntligen, genom utlämnande av en allmän handling eller på något annat sätt. Med *sekretessreglerad uppgift* avses en uppgift för vilken det finns en bestämmelse om sekretess. Med *sekretessbelagd uppgift* förstås en sekretessreglerad uppgift för vilken sekretess gäller i ett enskilt fall. En *sekretessbrytande bestämmelse* är en bestämmelse som innebär att en sekretessbelagd uppgift får lämnas ut under vissa förutsättningar. En *primär sekretessbestämmelse* är en bestämmelse om sekretess som en myndighet ska tillämpa på grund av att bestämmelsen riktar sig direkt till myndigheten eller omfattar en viss verksamhetstyp eller en viss ärendetyp som hanteras hos myndigheten eller omfattar vissa uppgifter som finns hos myndigheten. En *bestämmelse om överföring av sekretess* är en bestämmelse som innebär att en sekretessbestämmelse som är tillämplig på en uppgift hos en myndighet, ska tillämpas på uppgiften även av en myndighet som uppgiften lämnas till eller som har elektronisk tillgång till uppgiften hos den förstnämnda myndigheten. Slutligen ska med *sekundär sekretessbestämmelse* förstås en bestämmelse om sekretess som en myndighet ska tillämpa på grund av en bestämmelse om överföring av sekretess.

8.4 Vad innebär sekretess?

Som vi konstaterar ovan innebär sekretess ett förbud att röja en uppgift, oavsett om det görs muntligen, genom utlämnande av allmän handling eller på något annat sätt (3 kap. 1 § OSL). Förbudet att röja uppgifter träffar alltså varje form av röjande. Sekretess innebär således både handlingssekretess och tystnadsplikt och gäller inte bara för uppgifter i allmänna handlingar, utan även för uppgifter som finns hos en myndighet i sådana handlingar som ännu inte blivit allmänna. Otillåtet röjande av en sekretessbelagd uppgift är straffsanktionerat som brott mot tystnadsplikt (20 kap. 3 § brottsbalken).

Sekretess gäller som huvudregel inte bara i förhållande till enskilda (dvs. privatpersoner, företag etc.) utan också mellan myndigheter samt inom en myndighet, om det finns olika verksamhets-

grenar där som är att betrakta som självständiga i förhållande till varandra (8 kap. 1 och 2 §§ OSL).

En uppgift för vilken sekretess gäller får röjas för en utländsk myndighet eller mellanfolklig organisation under vissa förutsättningar (8 kap. 3 § OSL) Ett utlämnande får ske antingen i enlighet med en särskild föreskrift i lag eller förordning eller om uppgifterna i motsvarande fall skulle få lämnas ut till en svensk myndighet och det enligt den utlämnande myndigheten står klart att det är förenligt med svenska intressen att uppgiften lämnas.

8.5 Offentlighet- och sekretesslagens tillämpningsområde

Enligt 2 kap. 1 § första stycket OSL gäller lagens förbud mot att röja eller utnyttja en uppgift för myndigheter. Av övriga bestämmelser i kapitlet och bilagan till OSL följer att vissa organ som inte är myndigheter ska jämställas med sådana vid tillämpningen av 2 kap. TF och OSL.

I bestämmelsens andra stycke anges att lagens förbud mot att röja eller utnyttja en uppgift också gäller för en person som fått kännedom om uppgiften genom att för det allmännas räkning delta i en myndighets verksamhet på grund av anställning eller uppdrag hos myndigheten, på grund av tjänsteplikt, eller på annan liknande grund.

Röjandeförbudet enligt lagen gäller alltså inte bara för myndighetens anställda, utan också för sådana personer som på grund av uppdrag hos myndigheten eller på annan liknande grund deltar i myndighetens verksamhet.

8.6 Sekretessbestämmelsers uppbyggnad

En sekretessbestämmelse består i regel av tre huvudsakliga rekvisit, dvs. förutsättningar för bestämmelsens tillämplighet. Dessa rekvisit anger sekretessens föremål, dess räckvidd och dess styrka.

Sekretessens föremål är den information som kan hemlighållas och anges i lagen genom ordet *uppgift* tillsammans med en mer eller mindre långtgående precisering av uppgiftens art, exempelvis uppgift om enskilds personliga förhållanden.

En sekretessbestämmelses räckvidd bestäms normalt genom att det i bestämmelsen preciseras att sekretessen för de angivna uppgifterna bara gäller i en viss typ av ärende, i en viss typ av verksamhet eller hos en viss myndighet. Några få sekretessbestämmelser gäller utan att räckvidden är begränsad. Uppgiften kan då hemlighållas oavsett i vilket ärende, i vilken verksamhet eller hos vilken myndighet den förekommer.

Sekretessens styrka bestäms i regel med hjälp av s.k. skaderekvisit. Man skiljer i detta sammanhang mellan raka och omvända skaderekvisit. Vid rakt skaderekvisit är utgångspunkten att uppgiften är offentlig och att sekretess gäller bara om det kan antas att en viss skada uppstår om uppgiften lämnas ut. Vid ett omvänt skaderekvisit är utgångspunkten den motsatta, dvs. att uppgiften är sekretessbelagd. Uppgiften får då lämnas ut endast om det står klart att den kan röjas utan att viss skada uppstår. Sekretessen kan även vara absolut, vilket innebär att de uppgifter som omfattas av bestämmelsen ska hemlighållas utan någon skadeprövning, om uppgifterna begärs ut.

8.7 Sekretessbrytande bestämmelser

Som vi konstaterar ovan gäller sekretess inte bara i förhållande till enskilda utan också gentemot andra svenska myndigheter, utländska myndigheter och mellanfolkliga organisationer, samt mellan olika självständiga verksamhetsgrenar inom en myndighet. I vissa fall måste dock myndigheter kunna lämna ut uppgifter för att kunna utföra sina uppgifter. Vidare kan enskilda i vissa fall ha ett berättigat behov av att få ta del av uppgifter som annars omfattas av sekretess. Sekretessregleringen innehåller därför särskilda sekretessbrytande bestämmelser. Dessa har utformats efter en intresseavvägning mellan myndigheternas eller enskildas behov av att ta del av uppgifterna och de intressen som aktuella sekretessbestämmelser ska skydda.

8.8 Överföring av sekretess och tystnadsplikt

8.8.1 Överlämnande till annan myndighet

Som huvudregel gäller att sekretess inte följer med en uppgift när den lämnas till en annan myndighet. Det beror bl.a. på att behovet av och styrkan i en sekretess inte kan bestämmas enbart med hänsyn till sekretessintresset. Offentlighetsintresset kan kräva att uppgifter som behandlas som hemliga hos en myndighet är offentliga hos en annan myndighet.

Vissa bestämmelser om överföring av sekretess med begränsade tillämpningsområden har dock införts. Sådana bestämmelser innebär att en primär sekretessbestämmelse som är tillämplig hos en myndighet ska tillämpas på uppgiften även av en myndighet som uppgiften har lämnats till eller som har elektronisk tillgång till uppgiften hos den förstnämnda myndigheten (s.k. direktåtkomst). En och samma sekretessbestämmelse kan således vara en primär sekretessbestämmelse hos den utlämnande myndigheten och en sekundär sekretessbestämmelse hos den mottagande myndigheten.

Om en sekretessreglerad uppgift lämnas från en myndighet till en annan gäller sekretess för uppgiften hos den mottagande myndigheten antingen om sekretess följer av en primär sekretessbestämmelse som är tillämplig hos den mottagande myndigheten eller om sekretess följer av en bestämmelse om överföring av sekretess. Om ingen av dessa förutsättningar är uppfyllda blir uppgiften offentlig hos den mottagande myndigheten.

8.8.2 Överlämnande till privata subjekt

Gällande rätt

OSL innehåller ingen allmän bestämmelse om tystnadsplikt för en utomstående fysisk eller juridisk person som har tagit del av en sekretessbelagd uppgift. I enskilda fall kan dock tystnadsplikt enligt OSL ändå gälla, nämligen då uppgiften lämnats ut med förbehåll enligt 10 kap. 14 § OSL som inskränker den enskildes rätt att lämna uppgiften vidare eller utnyttja den.

I vissa andra fall av utlämnande till privata subjekt träder tystnadsplikt enligt andra författningar in, såsom den tystnadsplikt som gäller för advokater enligt 8 kap. rättegångsbalken eller inom enskilt bedriven hälso- och sjukvård enligt 6 kap. 12 § patientsäkerhetslagen (2010:659).

Tystnadsplikt för privata tjänsteleverantörer

Den 1 januari 2021 trädde lagen (2020:914) om tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter i kraft (tystnadspliktslagen).

Tystnadspliktslagen ska tillämpas när en myndighet uppdrar åt ett företag eller en annan enskild (tjänsteleverantör) att endast tekniskt bearbeta eller tekniskt lagra uppgifter (1 §) Vid tillämpning av lagen jämställs med myndigheter associationer som avses i 2 kap. 3 § OSL, organ som anges i bilagan till OSL och vissa yrkesmässigt bedrivna enskilda verksamheter som till någon del är offentligt finansierade (2 §). Med tjänsteleverantör jämställs en underleverantör som medverkar till att fullgöra tjänsteleverantörens uppdrag (3 §). Den som på grund av anställning eller på något annat sätt har deltagit i en tjänsteleverantörs verksamhet att på uppdrag av en myndighet endast tekniskt bearbeta eller lagra uppgifter får inte obehörigen röja eller utnyttja dessa uppgifter (4 §).

8.9 Röjandebegreppet

8.9.1 Lagtexten

Utredningens bedömning: Det följer av lagtexten i offentlighets- och sekretesslagen (2009:400) att ett utlämnande är en form av röjande, att uttrycket röja är ett neutralt begrepp i den meningen att det kan vara såväl tillåtet som otillåtet och att det inte krävs att mottagaren av uppgiften ska ha tagit del av den för att den ska betraktas som röjd.

Definitionen av sekretess

Som följer av det föregående definieras uttrycket sekretess som ett förbud att röja en uppgift, vare sig det sker muntligen, genom utlämnande av en allmän handling eller på något annat sätt (3 kap. 1 § OSL).

Uttrycket *röja* definieras inte i lagtexten. Att utlämna en allmän handling eller muntligen förmedla uppgiften nämns däremot som exempel på hur ett röjande av en uppgift kan gå till. Anledningen till att dessa exempel lyfts fram i lagtexten är att de anknyter till grundlagsskyddade rättigheter; handlingsoffentligheten enligt TF och yttrandefriheten enligt regeringsformen. Med formuleringen *eller på något annat sätt* markeras att lagstiftaren föreställt sig att uppgifter också kan röjas på andra sätt än de som uttryckligen nämns i lagtexten.

Av lagtexten framgår således att ett utlämnande av en uppgift utgör en form av röjande. En uppgift som har lämnats ut är därmed röjd. En uppgift kan alltså inte vara utlämnad utan att samtidigt vara röjd.

Vi har i våra kontakter med myndigheter under arbetets gång fått veta att den uppfattningen förekommer att uttrycket röja endast tar sikte på ett utlämnande i strid med en sekretessbestämmelse förekommer. Som konstateras i det föregående definieras uttrycket sekretess som ett *förbud* mot att röja en uppgift. Det är självfallet inte alltid förbjudet att röja uppgifter. Om en myndighet exempelvis efter en skadeprövning finner att en uppgift kan lämnas ut och i enlighet med detta lämnar ut uppgiften så röjer myndigheten uppgiften utan att det finns ett förbud mot det. Som följer av lagtexten är ju ett utlämnande en form av röjande. Det är i ett sådant fall fråga om ett tillåtet röjande. Myndigheten röjer förstås uppgiften även i det fallet att den lämnar ut uppgiften i strid med en sekretessbestämmelse. Det är i ett sådant fall fråga om ett otillåtet röjande. Uttrycket röja är således neutralt i den meningen att ett röjande kan vara såväl tillåtet som otillåtet.

Uppfattningen att uttrycket röja endast tar sikte på ett utlämnande i strid med en sekretessbestämmelse strider mot lagtexten och måste därmed betecknas som felaktig.

Att röja en uppgift

Uttrycket *röja* i olika varianter förekommer förutom i definitionen av uttrycket sekretess på ett flertal ställen i OSL. Enligt 2 kap. 1 § första stycket OSL – som handlar om lagens tillämpningsområde – gäller förbud att *röja* en uppgift för myndigheter. Skaderekvisiten i OSL – såväl de raka som de omvända – utgår från uttrycket röja. I 18 kap. 7 § OSL sägs exempelvis att sekretess gäller för uppgift som hänför sig till verksamhet som avser särskilt personsäkerhetsarbete enligt 2 a § polislagen (1984:387), om det inte står klart att uppgiften kan *röjas* utan fara för att verksamheten skadas.

Det är enligt OSL alltid uppgifter som röjs. Ingenstans i OSL heter det att en handling röjs. Detta är naturligt eftersom OSL – om vi bortser från 4–6 kap. – inte innehåller några regler om handlingar. Som vi redan varit inne på definieras uttrycket sekretess som ett förbud att röja en *uppgift*. Det är uppgifter som står i fokus enligt OSL och de uppgifter som finns i handlingar är bara en delmängd av alla uppgifter som omfattas av regleringen.

Att lämna ut en handling eller en uppgift

I vissa bestämmelser i OSL används uttrycket *lämna ut* i olika varianter. I några av dessa bestämmelser – t.ex. i definitionen av uttrycket sekretess – talas om utlämnande av *allmän handling*. Som nämns i avsnitt 8.2 följer av 2 kap. 19 § andra stycket TF att det i en särskild lag ska anges hur ett beslut om att avslå en begäran om att utfå en allmän handling ska överklagas. Den lag som här avses är OSL och i linje med detta föreskrivs i 6 kap. 7 § första stycket p. 1 OSL att en enskild får överklaga ett beslut av en myndighet att inte *lämna ut en handling* till den enskilde.

I de flesta bestämmelser i OSL där uttrycket lämna ut förekommer heter det att *en uppgift lämnas ut*. En sekretessbrytande bestämmelse sägs exempelvis vara en bestämmelse som innebär att en sekretessbelagd *uppgift får lämnas ut* under vissa förutsättningar (3 kap. 1 § OSL). I 5 kap. 5 § första stycket första meningen OSL sägs att om det kan antas att *en uppgift i en allmän handling inte får lämnas ut* på grund av en bestämmelse om sekretess, får myndigheten markera detta genom att en särskild anteckning (sekretessmarkering) görs på handlingen eller, om handlingen är elektronisk, införs i handlingen

eller i det datasystem där den elektroniska handlingen hanteras. Ett annat exempel på detta finns i 10 kap. 2 § OSL där det sägs att sekretess inte hindrar att *en uppgift lämnas* till en enskild eller till en annan myndighet, om det är nödvändigt för att den utlämnande myndigheten ska kunna fullgöra sin verksamhet.

Att lämna ut en handling eller en uppgift – vad är det för skillnad?

I OSL talas det alltså i vissa fall om att en *handling* lämnas ut och i andra fall om att en *uppgift* lämnas ut. Frågan inställer sig hur dessa formuleringar förhåller sig till varandra.

Det kan konstateras att uttrycket handling i OSL anknyter till TF:s terminologi. Med handling avses en framställning i skrift eller bild samt en upptagning som endast med tekniska hjälpmedel kan läsas eller avlyssnas eller uppfattas på annat sätt (2 kap. 3 § TF). Denna definition träffar såväl traditionella pappershandlingar som elektroniska handlingar. En uppgift kan vara dokumenterad i en handling. Det är sådana uppgifter som är av intresse i sammanhanget, inte handlingen i sig. Att lämna ut en handling innebär att uppgifter i handlingen lämnas ut. Den som lämnar ut en handling lämnar alltså ut uppgifter.

Mot denna bakgrund måste saken uppfattas på det sättet att när det i OSL sägs att en handling lämnas ut avses den form av uppgiftsutlämnande som sker genom att en handling lämnas ut. När det däremot heter att en uppgift lämnas ut så avses dels det fallet att uppgiften lämnas ut genom att en handling lämnas ut, dels det fallet att uppgifterna lämnas ut på något annat sätt. Saken bör kunna uttryckas så att uppgifter alltid lämnas ut när en handling lämnas ut men en handling lämnas inte alltid ut när uppgifter lämnas ut.

En uppgift är röjd även om någon inte tar del av den

Enligt Svenska Akademiens ordlista ska med uttrycket röja förstås avslöja, förråda; visa, lägga i dagen. I en rent språklig mening framstår det som tveksamt om en uppgift kan sägas vara avslöjad – som alltså är en synonym till röjd – med mindre än att en utomstående tagit del av uppgiften. En tolkning i enlighet med detta skulle alltså

innebära att en uppgift inte kan betraktas som röjd med mindre än att någon utomstående *tagit del av* uppgiften.

Det ligger i sakens natur att när det i OSL sägs att en uppgift lämnas ut, detta inte tar sikte på annat än att uppgiften lämnas ut från myndigheten. Man skulle kunna uttrycka det som att en uppgift måste passera en gräns – sekretessgränsen – för att den ska kunna betraktas som utlämnad. Om exempelvis en myndighetsanställd lämnar en handling till sin kollega på myndigheten har uppgifterna i handlingen inte lämnats ut. (Här bortses ifrån det fallet att sekretess gäller inom en myndighet, se 8 kap. 2 § OSL.)

En uppgift måste kunna betraktas som utlämnad även om mottagaren av uppgiften inte har tagit del av den. Antag att en myndighet på begäran av en journalist skickar ett e-postmeddelande med en handling bifogad. Uppgifterna i handlingen är förstås utlämnade oavsett om journalisten tagit del av dem eller inte.

Med utgångspunkt i röjandebegreppets allmänspråkliga betydelse skulle man kunna argumentera för att frågan om en uppgift är utlämnad respektive frågan om en uppgift är röjd ska bedömas separat och att en uppgift som har lämnats ut – dvs. passerat sekretessgränsen – inte ska ses som röjd om inte någon som befinner sig på andra sidan gränsen har tagit del av uppgiften. Uppgiften skulle alltså kunna betraktas som utlämnad men inte röjd.

Av definitionen av sekretess följer dock att en uppgift som har lämnats ut har röjts. En argumentation som går ut på att en uppgift skulle kunna betraktas som utlämnad men inte som röjd kan alltså inte vara riktig. Som nyss konstaterats måste en uppgift kunna betraktas som utlämnad även om mottagaren av uppgiften inte tagit del av den. Härav följer att det inte krävs att mottagaren har tagit del av uppgiften för att den ska kunna betraktas som röjd.

Att lämna ut och att röja – finns det någon skillnad?

Man kan mot denna bakgrund ställa sig frågan om det i OSL görs någon skillnad mellan att lämna ut en uppgift och att röja en uppgift.

Som vi tolkar det används i OSL uttrycket *lämna ut uppgifter* i de fall åtgärden – dvs. att låta uppgifterna passera sekretessgränsen – föregås av ett beslut från myndighetens sida. Det framstår som naturligt att t.ex. hävda att en myndighet som med stöd av en sekretess-

brytande bestämmelse beslutar att en sekretessbelagd uppgift ska passera sekretessgränsen lämnar ut uppgiften. Med den tolkningen framstår det som logiskt att det i t.ex. definitionen av sekretessbrytande bestämmelse heter att uppgifter får lämnas ut.

En annan sak är att sådana beslut som innebär att myndigheten låter uppgifter passera sekretessgränsen i vissa fall kan fattas formlöst t.ex. när en enskild tar del av uppgifter om sig själv på ”Mina sidor” genom att logga in på myndighetens webbsida med hjälp av e-legitimation.

I vissa fall förefaller det inte korrekt att beskriva ett skeende som att en myndighet har lämnat ut uppgifter. Om exempelvis en enskild myndighetsanställd, utan att agera på myndighetens vägnar, muntligen förmedlar uppgifterna framstår det som naturligare att i stället hävda att uppgifterna röjts.

Som vi redan varit inne på utgör ett utlämnande av en uppgift en form av röjande. När det i lagtexten heter att en uppgift lämnas ut – som t.ex. i 10 kap. 2 § OSL – avses just den formen av röjande. När det heter att uppgifter röjs träffas däremot alla situationer då en uppgift passerar sekretessgränsen. Med den tolkningen framstår det som logiskt att det i definitionen av sekretess i 3 kap. 1 § OSL talas om ett förbud att röja en uppgift. Avsikten är naturligtvis att alla situationer då en uppgift passerar sekretessgränsen ska träffas av förbudet och inte endast när det sker genom att en uppgift lämnas ut.

I det följande används uttrycken lämna ut respektive röja omväxlande utifrån vad som framstår naturligt i sammanhanget.

8.9.2 Lagmotiven

Utredningens bedömning: Lagmotiven till sekretesslagstiftningen ger ingen närmare vägledning när det gäller frågan hur röjandebegreppet i offentlighets- och sekretesslagen (2009:400) ska tolkas. Det finns i lagmotiven till straffbestämmelsen om brott mot tystnadsplikt i 20 kap. 3 brottsbalken stöd för att en uppgift ska betraktas som röjd så snart den lämnats ut.

Inledning

Syftet med detta avsnitt är att undersöka om det i lagmotiven till OSL och dess föregångare sekretesslagen (1980:100) samt straffbestämmelsen om brott mot tystnadsplikt i 20 kap. 3 § brottsbalken finns någon vägledning när det gäller frågan hur röjandebegreppet i OSL ska tolkas.

Lagmotiven till offentlighets- och sekretesslagen

Den 30 juni 2009 ersattes 1980 års sekretesslag med OSL. Med endast en språklig justering överfördes definitionen av uttrycket sekretess i 1980 års sekretesslag till den nya definitionskatalogen 3 kap. 1 § OSL. Några materiella ändringar gjordes alltså inte och inte heller gjordes i lagstiftningsärendet några uttalanden om hur röjandebegreppet ska tolkas (prop. 2008/09:150 s. 297 ff. och 364). Vägledande uttalanden får därför sökas i lagmotiven till 1980-års sekretesslag.

Lagmotiven till 1980 års sekretesslag

Promemorians förslag

Till grund för 1980 års sekretesslag låg ett förslag som presenterades i den inom Justitiedepartementet upprättade promemorian (Ds Ju 1977:1 och 11) *Handlingssekretess och tystnadsplikt*.

I det första kapitlet i promemorians förslag till sekretesslag hade vissa grundläggande bestämmelser tagits in. I 2 § reglerades i två punkter vad sekretess innebar (s. 24). Enligt den första punkten innebar sekretess en begränsning i rätten enligt 2 kap. TF att ta del av allmän handling, i den mån sekretessbelagd uppgift röjs genom att handlingen lämnas ut. I den andra punkten i samma paragraf föreskrevs att sekretess innebar – när inte annat följde av bestämmelse som upptogs i lagen eller som hade stöd i denna – ett förbud att genom utlämnande av handling, muntligen eller på annat sätt röja sekretessbelagd uppgift utanför den särskilda verksamhet för det allmännas räkning vari den har inhämtats eller att utnyttja uppgiften utanför denna verksamhet.

I specialmotiveringen till 2 § 2 angavs följande (s. 225).

> Sålunda förbjuds genom bestämmelsen varje form av röjande av sekretessbelagd uppgift. Det är likgiltigt om röjande sker genom att en allmän handling företes, genom att någon får ta del av en handling som inte är allmän, genom att befattningshavare meddelar uppgifter i ett brev eller genom att han lämnar information muntligen. Också andra former för röjande av uppgift kan tänkas, exempelvis att någon förevisar ett hemligt föremål för annan. Det är utan betydelse om uppgiften före röjandet är dokumenterad eller inte. Inte heller spelar det någon roll om uppgift lämnas ut på begäran av utomstående eller efter initiativ av den som har uppgiften om hand.

Lagrådsremissen

I den lagrådsremiss som utarbetades sedan promemorian hade remissbehandlats gavs den föreslagna lagens första kapitel som – i likhet med lagförslaget i promemorian innehöll vissa grundläggande bestämmelser – en annorlunda utformning (prop. 1979/80:2 Del A s. 407 f.).

Till skillnad från förslaget i promemorian fanns i lagrådsremissens lagförslag ingen klar definition av uttrycket sekretess. I stället hette det i 2 § att – om sekretess gäller enligt denna lag för uppgift – uppgiften inte får lämnas till enskild, vare sig det sker genom att allmän handling lämnas ut eller det sker muntligen eller på annat sätt. I 3 § sades att – om sekretess gäller enligt denna lag för uppgift som förekommer hos viss myndighet – uppgiften inte får lämnas till annan myndighet eller till annan verksamhetsgren inom samma myndighet.

I specialmotiveringen till 2 § angavs följande (s. 119).

> Genom bestämmelsen i 2 §, som i likhet med 3 § ger uttryck åt den för lagens konstruktion grundläggande tanken om en enhetlig reglering av sekretessen, förbjuds varje form av röjande av sekretessbelagd uppgift för enskild. I lagtexten uttrycks detta så att uppgift inte får lämnas ut till enskild. Det saknar betydelse på vilket sätt röjande sker. I första hand nämns förbud mot att röja uppgift genom att lämna ut allmän handling. Vad som menas med allmän handling framgår av TF (jfr prop. 1975/76:160 s. 119). Uppgift får inte heller röjas genom att en befattningshavare lämnar ut information muntligen eller på annat sätt. Innebörden härav är att befattningshavaren inte får låta någon ta del av hemlig uppgift vare sig detta sker genom att allmän handling företes eller att någon får ta del av handling som inte är allmän eller att uppgiften meddelas i brev. Också andra former för röjande av en uppgift kan tänkas, exempelvis att någon förevisar ett hemligt föremål för annan. Bestämmelsen avser alltså varje form av röjande. Det är också utan

> betydelse om uppgiften före röjandet är dokumenterad eller inte. Inte heller spelar det någon roll om uppgift lämnas ut på begäran av utomstående eller efter initiativ av den som har uppgiften om hand.

Lagrådet

I sin granskning påpekade lagrådet att det förhållandet att uttrycket sekretess saknade en klar definition ledde till vissa komplikationer (s. 454). Som en följd av detta ansåg lagrådet att det skulle ges en förklaring av den speciella innebörd begreppet sekretess avsågs ha i lagen. Lagrådet föreslog därför att det i den föreslagna lagens första paragraf – som i övrigt föreslogs innehålla en beskrivning av lagens innehåll – i ett andra stycke skulle införas en bestämmelse med följande innehåll (s. 489).

> Bestämmelserna avser förbud att röja uppgift, vare sig det sker muntligen eller genom att allmän handling lämnas ut eller det sker på annat sätt (*sekretess*).

Lagrådets förslag i denna del godtogs och lagtexten kom att få den utformning som lagrådet hade förordat (s. 494).

Lagmotiven ger inte någon vägledning

I både specialmotiveringen till det lagförslag som lämnades i promemorian och i specialmotiveringen till det lagförslag som lämnades i lagrådsremissen talas det om någon får *ta del av* en uppgift etc. Det går att argumentera för att dessa formuleringar och de exempel på röjande som lämnas i texterna tyder på att man föreställde sig att det endast kunde vara fråga om ett röjande i de fall mottagaren hade tagit del av uppgifterna. I viss utsträckning grumlas dock bilden av att det i båda texterna även talas om att uppgifter lämnas ut. Att en uppgift har lämnats ut säger någonting om huruvida mottagaren tagit del av uppgiften. I detta sammanhang finns även skäl att göra den allmänna reflektionen att om tanken hade varit att mottagaren måste ha tagit del av uppgifterna för att de ska betraktas som röjda, det hade varit på sin plats att tydligt påpeka detta. Det ligger nära till hands att tolka frånvaron av ett sådant påpekande som att lagstiftaren inte hade någon sådan avsikt eller kanske inte ens reflekterade över frågeställningen.

Som vi redogör för ovan arbetades lagförslaget i lagrådsremissen om på inrådan av lagrådet. I lagrådsremissens specialmotivering kommenteras bestämmelsen såsom den utformats i remissen och inte bestämmelsen såsom den slutligen kom att utformas.

I den bestämmelse som specialmotiveringen i lagrådsremissen behandlar används inte uttrycket röja utan endast att *en uppgift lämnas ut*. Något tydligt stöd för tesen att det var lagstiftarens avsikt att ett röjande skulle förutsätta att mottagaren tar del av uppgiften finns inte i den kommenterade bestämmelsens ordalydelse eller i lagrådets motivering av sitt förslag.

Med hänsyn till detta bedömer vi att lagmotiven inte kan anses ge någon egentlig vägledning när det gäller frågan om det krävs att någon tagit del av en uppgift för att en uppgift ska betraktas som röjd.

Lagmotiven till bestämmelsen om brott mot tystnadsplikt

Brott mot tystnadsplikt

För brott mot tystnadsplikt döms den – enligt 20 kap. 3 § första stycket brottsbalken – som röjer uppgift, som han är pliktig att hemlighålla enligt lag eller annan författning eller enligt förordnande eller förbehåll som har meddelats med stöd av lag eller annan författning, eller olovligen utnyttjar sådan hemlighet. I andra stycket i samma bestämmelse föreskrivs ansvar även för oaktsamma gärningar. I ringa fall ska inte dömas till ansvar.

Som framgår av lagtexten träffas alltså – trots brottsbeteckningen brott mot tystnadsplikt – alla former av röjande av straffbestämmelsen.

Det bör noteras att bestämmelsen är subsidiär i förhållande till andra bestämmelser, dvs. den ska endast tillämpas om inte någon annan bestämmelse är tillämplig. Man kan tänka sig gärningar som faller in såväl under någon straffbestämmelse i exempelvis 19 kap. brottsbalken som under aktuell straffbestämmelse. I ett sådant fall ska alltså den första av dessa bestämmelser tillämpas.

När det gäller uppsåtliga brott ska – såvitt framgår av lagmotiven – det subjektiva rekvisitet, dvs. kravet på uppsåt eller oaktsamhet, omfatta också det förhållandet att den röjda uppgiften inte får *lämnas ut* i det aktuella fallet (prop. 1979/80:2, Del A, s. 404). En offentlig funktionär som av oaktsamhet misstar sig på sekretessregleringens

innehåll ska alltså fällas till ansvar för endast oaktsamt brott, om denne röjer en sekretessbelagd uppgift. Oaktsamma brott som är ringa ska vara fria från ansvar. I lagmotiven sägs vidare att frågan om ett oaktsamt brott är ringa får avgöras med hänsyn till samtliga omständigheter i det konkreta fallet. En faktor som kan vara av betydelse – förutom vilken uppgift som röjts och vilken skada det lett till – är vilka krav som rimligen kan ställas på den offentliga funktionären med hänsyn till dennes möjligheter att bedöma den rättsliga situationen.

Närmare om lagmotiven

Innan 1980 års sekretesslag trädde i kraft den 1 januari 1981 fanns bestämmelser om förbud att lämna ut allmänna handlingar i lagen (1937:249) om inskränkningar i rätten att utbekomma allmänna handlingar medan regler om tystnadsplikt i det allmännas verksamhet fanns spridda i ett stort antal författningar.

I linje med den uppdelning som gjordes i lagstiftningen mellan handlingssekretess och tystnadsplikt träffade bestämmelsen i 20 kap. 3 § brottsbalken – enligt sin ordalydelse – endast den som muntligen förmedlade (yppade) eller olovligen utnyttjade hemlig uppgift. Vidare fanns i 41 § i 1937 års sekretesslag bestämmelser om straff för den som i strid med den lagen eller föreskrift som meddelats enligt lagen utlämnade allmän handling eller bröt mot förbehåll som gjorts vid handlingens utlämnande.

Till grund för den lagrådsremiss som utarbetades på grundval av den tidigare omnämnda promemorian föreslog regeringen att 1937 års sekretesslag och därmed även 41 § i den lagen skulle upphävas, att en ny sekretesslag skulle införas (1980 års sekretesslag) samt att bestämmelsen om brott mot tystnadsplikt skulle justeras på det sättet att den skulle omfatta den som röjde någon uppgift som han till följd av lag eller annan författning var pliktig att hemlighålla eller om han olovligen utnyttjade sådan hemlighet (prop. 1979/80:2, Del A, s. 444).

I specialmotiveringen till förslaget resonerade departementschefen kring innebörden av 20 kap. 3 § brottsbalken enligt den lydelse som gällde då (s. 402). Med hänvisning till rättsfallet NJA 1953 s. 654 menade han att det kunde betraktas som brott mot tystnadsplikt att någon röjer något, som han ska hemlighålla, genom att förete en icke

allmän handling eller genom att visa upp en hemlig allmän handling trots att ordet yppa användes i bestämmelsen. Departementschefens slutsats var därför att det fanns goda skäl för att hävda att också *utlämnande av allmän handling* i strid med föreskrifterna i 1937 års sekretesslag eller mot förbud som har meddelats enligt den lagen skulle betraktas som ett brott mot tystnadsplikt. Han var också av den uppfattningen – med hänvisning till prop. 1975:76:160 s. 266 och 1975/76:204 s. 171 – att även den som bröt mot förbehåll som har gjorts vid utlämnande av handling kunde tänkas bli straffad för brott mot tystnadsplikt och att 41 § i 1937 års sekretesslag därmed inte längre hade någon självständig betydelse.

I sin granskning av förslaget förordade lagrådet – för att det skulle bli helt klart att straffbestämmelsen inte endast avsåg tystnadsplikt som föreskrivs direkt i lag eller annan författning utan även sådan som följer av förordnande eller förbehåll – att första stycket i paragrafen skulle anges avse, att någon röjer uppgift som han är pliktig att hemlighålla enligt lag eller annan författning eller enligt förordnande eller förbehåll, som meddelats med stöd av lag eller annan författning, eller att han olovligen utnyttjar sådan hemlighet. (s. 488).

När det gäller frågan om bestämmelsen i 20 kap. 3 § kunde tillämpas på gärningar som inte omfattades av lydelsen påpekade lagrådet med hänvisning till litteraturen (Beckman m.fl., Kommentar till brottsbalken II, 4 uppl. 1978, s. 401) att den i remissprotokollet redovisade uppfattningen om gällande rätt inte var oomtvistad.

Slutligen ska sägas att lagrådet förordade brottsbeteckningen sekretessbrott i stället för brott mot tystnadsplikt. Enligt lagrådet byggde tydligen förslaget på sekretesslag på uppfattningen att brott mot tystnadsplikt skulle omfatta inte endast *röjande* som skedde genom muntligt eller skriftligt meddelande utan också *det blotta utlämnandet av sekretessbelagd allmän handling*. Lagrådet menade att redan det förhållande att det rådde tveksamhet om gällande rätts innebörd medförde att det inte kunde anses vara lämpligt – om man avser att innesluta även *det blotta utlämnandet av handling* – att använda beteckningen brott mot tystnadsplikt.

I slutprotokollet godtog departementschefen den av lagrådet föreslagna lydelsen (s. 504). Däremot vidhöll han den uppfattningen att beteckningen brott mot tystnadsplikt skulle användas, dock utan att invända mot den tolkning av uttrycket röja som lagrådet gav uttryck för.

Det finns fog för tolkningen att en uppgift är röjd så snart den lämnats ut

Det finns i de ovan omtalade lagmotiven stöd för att lagstiftaren tänkte sig att ett röjande sker så snart en handling lämnas ut. Det som avses här är förstås att den uppgift som finns dokumenterad i handlingen röjs. Att lagrådet vid sin uttolkning av innebörden i lagförslaget skriver att ett röjande ska kunna ske genom *blotta* utlämnandet av en handling måste rimligen tolkas som att det enligt lagrådet inte uppställs något krav på att uppgiften i handlingen måste avslöjas för att den ska röjas.

De aktuella uttalandena avser uttrycket röja i 20 kap. 3 § brottsbalken och inte uttrycket röja i OSL. Bestämmelsen om brott mot tystnadsplikt innebär dock att det uppställs en straffsanktion för den som uppsåtligen eller av oaktsamhet röjer uppgifter i strid med OSL. Mot den bakgrunden framstår det som ologiskt att tänka sig att uttrycket röja i 20 kap. 3 § brottsbalken skulle ha en annan innebörd än i OSL. Vår slutsats blir därmed att uttrycken i de olika lagstiftningarna bör tolkas på samma sätt.

Det ska för ordningens skull nämnas att det på ett ställe i lagmotiven framhålls att det för tjänstemän som har att tillämpa sekretesslagen finns en viss marginal som följer av rekvisitens utformning och området där ansvar för sekretessbrott [brott mot tystnadsplikt] inträder (prop. 1979:/80, Del A, s. 85). Vi uppfattar att detta uttalande inte tar sikte på annat än det förhållandet att det för att ansvar för brott mot tystnadsplikt ska komma i fråga inte är tillräckligt att ett röjande skett. Därutöver krävs ju att det subjektiva rekvisitet är uppfyllt. Det som avses är med andra ord att ett röjande i strid med sekretesslagen (i dag OSL) inte nödvändigtvis innebär att någon gjort sig skyldig till brott mot tystnadsplikt. Detta uttalande kan alltså inte åberopas som stöd för att uttrycket röja i 20 kap. 3 § brottsbalken skulle ha en annan innebörd än i OSL.

Eftersom uttrycket röja i OSL således bör tolkas på samma sätt som motsvarande uttryck i 20 kap. 3 § brottsbalken finns alltså fog för att hävda att ett röjande enligt OSL sker så snart en handling lämnas ut.

8.9.3 Rättspraxis

Det saknas rättspraxis som uttryckligen behandlar frågan om när en uppgift ska betraktas som röjd enligt OSL.

8.9.4 Litteratur

Kommentaren till offentlighets- och sekretesslagen

I kommentaren till OSL sägs att rättsfallet NJA 1991 s. 103 kan vara vägledande också vid tillämpningen av OSL och när det gäller brott mot tystnadsplikt.[2] Vilka skäl denna slutsats grundas på redovisas inte.

Vi återkommer till detta rättsfall i kapitel 9 och 10.

Brottsbalkskommentaren

I kommentaren till straffbestämmelsen om brott mot tystnadsplikt i 20 kap. 3 § brottsbalken sägs att när det i OSL talas om röjande, ligger däri inte mer än att gärningen ska bestå i att uppgift eller allmän handling lämnas ut i fall som omfattas av sekretess. Något krav på att ett avslöjande ska ha skett ska däremot inte läggas in i ordet röja.[3] Enligt kommentaren bör vidare – med hänvisning till prop. 1979/80:2 Del A s. 402 ff., s. 488 och s. 504 – samma innebörd kunna ges ordet röja också i 20 kap. 3 § brottsbalken.

8.10 Våra samlade bedömningar

Av bl.a. definitionen av sekretess i 3 kap. 1 § OSL framgår att ett utlämnande är en form av röjande. Av samma bestämmelse följer att uttrycket röja är neutralt i den meningen att det kan vara såväl tillåtet som otillåtet.

---

[2] Se Lenberg E. m.fl., *Offentlighets- och sekretesslag /2009:400/* 3 kap. 1 §, Nordstedts Juridik /JUNO/ /, Ahlström K., *Offentlighets- och sekretesslag /2009:400/* 3 kap. 1 §, Lexino /JUNO/ / och Corell H. mf.l. *Sekretesslagen, Kommentar till 1980 års lag med ändringar*, Norstedts juridik, tredje uppl., Stockholm, 1991, s. 64.

[3] Se Johansson S. m.fl. *Brottsbalken m.m.*, 20 kap. 3 §, Norstedts Juridik /JUNO/ /, se även Roos A-M., 20 kap. 3 § *brottsbalken*, Karnov /JUNO/ /och jfr samma författare, 20 kap. 3 §, Lexino /JUNO/ /.

En uppgift kan vara utlämnad utan att någon har tagit del av den. Ett resonemang som går ut på att en uppgift inte skulle kunna betraktas som röjd med mindre än att någon tar del av den förutsätter därmed det betraktelsesättet att uppgifter skulle kunna vara utlämnade utan att vara röjda. Av definitionen av sekretess följer dock att ett utlämnande är en form av röjande. Som vi konstaterar ovan måste en uppgift kunna betraktas som utlämnad även om mottagaren av uppgiften inte har tagit del av den. Härav följer att det inte krävs att mottagaren har tagit del av uppgiften för att den ska kunna betraktas som röjd.

Lagmotiven till sekretesslagstiftningen ger ingen närmare vägledning när det gäller frågan hur röjandebegreppet i OSL ska tolkas. Däremot finns det i lagmotiven till straffbestämmelsen om brott mot tystnadsplikt i 20 kap. 3 brottsbalken stöd för att en uppgift ska betraktas som röjd så snart den lämnats ut.

9 Tidigare utredningar

9.1 Inledning

Frågan hur myndigheternas[1] utkontraktering av it-drift förhåller sig till uttrycket röja i offentlighets- och sekretesslagen (2009:400) (OSL) är inte ny. Ämnet har varit föremål för behandling i flera statliga utredningar, i myndighetsrapporter, debattartiklar och liknande.

Syftet med detta avsnitt är att teckna en översiktlig bild av några av de analyser som redan har gjorts (avsnitt 9.4–9.7) och bemöta några av de argument som har framförts (avsnitt 9.8). Framställningen är inte heltäckande i den meningen att vi redogör för allt som hittills har skrivits i ämnet. Ett urval har gjorts.

Rättsfallet NJA 1991 s. 103 och ett beslut den 9 september 2014 (dnr 3032-2011) från Riksdagens ombudsmän (JO) har haft betydelse för de analyser som gjorts. I syfte att underlätta förståelsen av de aktuella analyserna inleder vi med att sammanfatta nämnda rättsfall och beslut (avsnitt 9.2 och 9.3).

I avsnitt 9.9 behandlar vi frågan när en uppgift – enligt NJA 1991 s. 103 – ska anses röjd i den mening som avses i straffbestämmelsen om vårdslöshet med hemlig uppgift. Frågan om de i rättsfallet uppställda riktlinjerna kan användas för att avgöra om en utkontraktering innebär att uppgifter som omfattas av utkontrakteringen röjs enligt OSL behandlas däremot i kapitel 10.

[1] Med myndigheter avses i detta kapitel statliga myndigheter, kommuner och regioner om inget annat framgår av sammanhanget.

9.2 NJA 1991 s. 103

9.2.1 Vårdslöshet med hemlig uppgift

Rättsfallet NJA 1991 s. 103 handlar om brottet vårdslöshet med hemlig uppgift. I det följande lämnas därför en kort beskrivning av straffbestämmelsen.

Brottsbalkens 19 kap. har rubriken *Om brott mot Sveriges säkerhet*. Den som av grov oaktsamhet befordrar, lämnar eller röjer sådan uppgift som avses i bestämmelsen om obehörig befattning med hemlig uppgift (7 §) – dvs. uppgift om försvarsverk, vapen, förråd, import, export, tillverkningssätt, underhandlingar, beslut eller något förhållande i övrigt vars uppenbarande för främmande makt kan medföra men för Sveriges säkerhet, vare sig uppgiften är riktig eller inte, om uppgiften rör något förhållande av hemlig natur – döms enligt 9 § för *vårdslöshet med hemlig uppgift*.

9.2.2 Närmare om rättsfallet

Omständigheterna kan sammanfattas enligt följande.

Ett bolag skulle enligt avtal med en försvarsmyndighet förvara två pärmar med handlingar som innehöll uppgifter som var hemliga i den mening som avses i 19 kap. 9 § brottsbalken. Pärmarna förvarades i ett säkerhetsskåp. Reservnycklarna till säkerhetsskåpet förvarades – i strid med gällande säkerhetsföreskrifter – i ett låst jalusiskåp av trä. Vid ett inbrott i bolagets lokaler bröt gärningsmannen upp jalusiskåpet och beredde sig därefter med hjälp av reservnycklarna tillträde till säkerhetsskåpet där pärmarna förvarades. Gärningsmannen hade tagit en kamera, vapen och ammunition som fanns i skåpet men det var inte klarlagt om han hade tagit del av handlingarnas innehåll.

Två personer som ansvarade för säkerheten hos bolaget åtalades för vårdslöshet med hemlig uppgift. Såväl tingsrätten som hovrätten fann dem skyldiga till den åtalade gärningen och de dömdes för vårdslöshet med hemlig uppgift.

De åtalade överklagade till Högsta domstolen och anförde bl.a. att de inte kunde anses ha röjt uppgifterna eftersom det inte var visat att deras åsidosättande av säkerhetsföreskrifterna hade lett till att någon obehörig hade tagit del av handlingarnas innehåll.

Högsta domstolen ogillade åtalet och anförde i domskälen följande.

> När det gäller frågan huruvida [de tilltalade] genom sitt förfarande kan anses ha röjt uppgifter ur de i säkerhetsskåpet förvarade handlingarna är följande att beakta. Uttrycket ”röjer uppgift” i bestämmelsen innebär enligt vanligt språkbruk att en uppgift avslöjas eller uppenbaras. Detta förutsätter att det finns någon person, för vilken uppgiften görs tillgänglig. Det torde dock inte alltid kunna krävas att denne faktiskt har fått kännedom om uppgiften. Det bör sålunda som regel vara tillräckligt att en handling med hemliga uppgifter har kommit i någon obehörigs besittning. Även vissa andra, närliggande situationer bör omfattas. Däremot kan inte varje möjlighet att ta del av en uppgift, som har beretts någon obehörig, medföra att uppgiften skall anses ha röjts; en sådan ordning skulle i realiteten innebära att det oaktsamma handlandet i sig ofta skulle medföra straffansvar. Avgörande för straffansvar bör främst vara om uppgiften har blivit tillgänglig för någon obehörig under sådana omständigheter, att man måste räkna med att den obehörige kommer att ta del av uppgiften.
>
> Det bör inte komma i fråga att på grund av uttalanden i lagförarbetena vidga bestämmelsens tillämpningsområde till situationer som ligger helt vid sidan av vad som sålunda kan anses följa av ordalydelsen. Varken de motivuttalanden vartill hänvisas i TR:ns och HovR:ns domar eller andra uttalanden i förarbetena till bestämmelsen eller dess tidigare motsvarighet ger för övrigt stöd för en sådan vidgad tillämpning.
>
> I målet är upplyst att vid inbrottet tillgripits, förutom en i lokalen befintlig kamera, två kulsprutepistoler jämte ammunition som förvarades i säkerhetsskåpet. Det har däremot inte kunnat klarläggas huruvida gärningsmannen tagit någon befattning med de i säkerhetsskåpet förvarade hemliga handlingarna. Omständigheterna är inte heller sådana att de hemliga uppgifterna likväl kan anses ha röjts. Åtalet skall därför ogillas.

9.3 Beslutet från JO

Två vårdgivare hade ingått avtal med ett företag om hjälp med journalföring av patientuppgifter. Enligt avtalen agerade företaget som personuppgiftsbiträde i förhållande till vårdgivaren (som var personuppgiftsansvarig). Avtalen innebar att vårdgivaren tillät att läkarsekreterare som var anställda hos företaget på distans lyssnade av inlästa diktat och skrev in uppgifterna i patientens journal. Hanteringen var helt elektronisk och uppgifter lagrades aldrig utanför regionens it-system.

Det råder enligt 25 kap. 1 § OSL, stark sekretess till skydd för uppgifter om patienter inom den allmänna hälso- och sjukvården. JO konstaterade att frågan om en vårdgivare kan lämna ut sekretessbelagda uppgifter till ett personuppgiftsbiträde eller till personal hos biträdet ska prövas på vanligt sätt enligt OSL.

Läkarsekreterarna hos företaget omfattades inte av den tystnadsplikt som enligt OSL gällde för vårdgivarens egen personal. Frågan om uppgifterna i patientjournalerna kunde göras tillgängliga för läkarsekreterarna var därför enligt JO i första hand beroende av om ett utlämnande kunde ske utan att det innebar men (dvs. skada) för den som skyddas av sekretessen. Läkarsekreterarna hade en avtalsreglerad tystnadsplikt i förhållande till arbetsgivaren (dvs. företaget). Vidare följer av regelverket om behandling av personuppgifter en sorts tystnadsplikt för den som behandlar uppgifterna. Enligt JO var dessa ”alternativa” tystnadsplikter för läkarsekreterarna inte tillräckliga för att anse att ett utlämnande kunde ske utan att det innebar men (skada) för den som skyddas av sekretessen. Mot bakgrund av att de uppgifter som behandlades enligt avtalen var av mycket integritetskänsligt slag lades vid bedömningen vikt bl.a. vid att vårdgivarens egen personal kan dömas för brott mot tystnadsplikt om en sekretessbelagd uppgift felaktigt röjs, medan så inte var fallet när det gällde läkarsekreterare som var anställda i företaget. Ett utlämnande hade enligt JO inte heller haft stöd i någon av de sekretessbrytande bestämmelser som finns i 10 kap. OSL eller i en lag eller förordning som OSL hänvisar till.

JO:s slutsats blev att vårdgivarna inte hade haft rättsligt stöd för att på det sätt som skett lämna ut sekretessbelagda uppgifter om patienter för journalföring av företagets läkarsekreterare. Enligt JO var det anmärkningsvärt att vårdgivarna inte hade ägnat sekretessaspekterna större uppmärksamhet i samband med att avtalen ingicks. Vårdgivarna fick allvarlig kritik för att de hade ingått avtal som innebar att regionen lämnade ut patientuppgifter för journalföring av anställda vid ett företag, trots att detta inte var förenligt med regelverket om sekretess.

9.4 E-delegationen

Fram till år 2015 avlämnade E-delegationen en rad betänkanden med förslag som syftade till att underlätta statsförvaltningens digitalisering.

Mot bakgrund av det ovan nämnda beslutet från JO beslutade E-delegationen att inleda en förstudie i syfte att klarlägga rättsläget rörande i vad mån sekretess utgjorde hinder för utkontraktering och skapa underlag för en bedömning av om det fanns anledning för delegationen att överväga författningsåtgärder inom området (Fi 2009:01/2015/4, 2015-03-09). I sitt slutbetänkande (SOU 2015:66) *En förvaltning som håller ihop* analyserade E-delegationen frågan om utkontraktering och sekretess med utgångspunkt i nämnda förstudie (s. 45 ff.).

Enligt den uppfattning som E-delegationen framförde borde en myndighet – vid den skadeprövning som ska göras inför ett utlämnande av sekretessreglerade uppgifter – inte endast beakta om mottagaren träffas av en straffsanktionerad tystnadsplikt i traditionell mening. Enligt delegationen borde en avtalsreglerad tystnadsplikt vara tillfyllest i många fall. Vidare argumenterades för att det röjande som en utkontraktering i många fall innebär skulle kunna betraktas som ett nödvändigt utlämnande enligt 10 kap. 2 § OSL.

Som vi uppfattar saken var det emellertid E-delegationens uppfattning att en utkontraktering inte måste innebära att uppgifterna röjs. Enligt delegationens uppfattning röjdes inte uppgifterna om de hade gjorts *tillgängliga* för en utomstående på ett sådant sätt att det föreföll osannolikt att mottagaren tog del av uppgifterna. Delegationen hänvisade i detta sammanhang till Högsta domstolens tolkning av uttrycket *röjer uppgift* i straffbestämmelsen om vårdslöshet med hemlig uppgift i 19 kap. 9 § brottsbalken [NJA 1991 s. 103]. Delegationen underströk att det som enligt Högsta domstolen är avgörande för straffansvar enligt 19 kap. 9 § brottsbalken är att uppgiften har blivit tillgänglig för någon obehörig under sådana omständigheter att man måste räkna med att den obehörige kommer att ta del av uppgiften. Även om rättsfallet rörde gränsen för det straffrättsliga ansvaret torde – enligt delegationen – ett liknande resonemang kunna föras i fråga om den närmare innebörden av röjandebegreppet i OSL.

Slutligen bör nämnas att det enligt E-delegationen – trots vissa oklarheter – inte fanns tillräckliga skäl att föreslå någon författningsändring på området.

9.5 Esamverkansprogrammet

9.5.1 Rättsliga uttalanden och vägledningar under åren 2015–2016

Sedan E-delegationen slutfört sitt uppdrag år 2015 bildades eSamverkansprogrammet (eSam) på initiativ av de generaldirektörer som hade ingått i E-delegationen. Syftet var att åstadkomma ett fortsatt samarbete kring digital utveckling på frivillig väg.

Den 17 december 2015 publicerade eSam det rättsliga uttalandet *Röjandebegreppet enligt offentlighets- och sekretesslagen* (VER 2015-190). I uttalandet sades att om uppgifter görs tekniskt tillgängliga för en privat tjänsteleverantör som enligt avtal inte får ta del av eller vidarebefordra uppgifterna och omständigheterna i övrigt medför att det är osannolikt att detta ändå sker, uppgifterna inte ska anses röjda i OSL:s mening.

Som skäl för sin ståndpunkt anförde eSam att innebörden av röjandeförbudet i lagmotiven till 1980 års sekretesslag beskrivs på ett sätt som indikerar att ett röjande också förutsätter att mottagaren kommer att ta del av uppgiften i fråga eller åtminstone har rätt att göra det. Slutligen påpekades att avsikten med att uppgifter görs tillgängliga för en privat tjänsteleverantör vid utkontraktering av itdrift inte är att denne ska tillgodogöra sig informationsinnehållet. Syftet är i stället att tjänsteleverantören enbart ska tekniskt bearbeta eller lagra själva informationsmassan.

I skriften *Outsourcing – en vägledning om sekretess och persondataskydd* som publicerades i januari 2016 kommenterade eSam det rättsliga uttalandet (s. 16 ff.). I skriften hänvisas till bl.a. rättsfallet NJA 1991 s. 103 som – enligt eSam – borde kunna tjäna till vägledning vid tolkningen av röjandebegreppet i OSL.

9.5.2 Rättsliga uttalanden, vägledningar och kompletteringar under åren 2018–2019

Den 23 oktober 2018 publicerade eSam det rättsliga uttalandet *Rättsligt uttalande om röjande och molntjänster* (VER 2018:57). I uttalandet sägs att om sekretessreglerade uppgifter görs tekniskt tillgängliga för en privat tjänsteleverantör som till följd av ägarförhållanden eller annars är bunden av regler i ett annat land, enligt vilka tjänsteleverantören kan bli skyldig att överlämna information utan att internationell rättshjälp anlitats eller annan laglig grund finns enligt svensk rätt, får uppgifterna anses vara röjda. Anledningen är att det inte längre är osannolikt att uppgifterna kan komma att lämnas till utomstående. Detsamma får – enligt uttalandet – anses gälla om redan ägarförhållanden eller geografisk placering av en privat tjänsteleverantörs tekniska hjälpmedel ger anledning att befara att mänskliga rättigheter (t.ex. skyddet för privatlivet) eller det allmännas intressen (t.ex. rikets säkerhet) inte skulle säkerställas om svenska myndigheters data hade tillgängliggjorts.

Inledningsvis slår eSam fast att det rättsliga uttalandet från den 17 december 2015 inte tog sikte på sådana molntjänster som erbjuds av företag som har servrar i olika länder så att informationen kan finnas sparad (speglad) i flera länder och snabbt kan flyttas mellan olika jurisdiktioner samt vara åtkomlig via nät.

Slutligen anför eSam att en annan bedömning inte kan uteslutas för det fall att ett röjande hindras genom kryptering av tillräcklig – och när så krävs – godkänd kvalitet eller av andra åtgärder med samma verkan.

Den 20 september 2019 publicerade eSam promemorian *Kompletterande information om molntjänster.* Syftet med promemorian var att komplettera det rättsliga uttalandet som gjorts i oktober 2018.

Under rubriken *Information* klargörs att det som sägs i det rättsliga uttalandet från december 2015 om röjandebegreppet enligt OSL förutsatte två saker. För det första att tjänsteleverantören enligt avtal med uppdragsgivaren inte får ta del av eller vidarebefordra de uppgifter som görs tekniskt tillgängliga för tjänsteleverantören och för det andra att omständigheterna i övrigt inte får medföra att det var osannolikt att det ändå skulle ske. Enligt eSam räcker det alltså inte med att göra en sannolikhetsbedömning. En sådan bedömning blir

aktuell att göra först sedan det konstaterats att den rättsliga regleringen av parternas mellanhavanden har utformats på ett hållbart sätt.

Vi tolkar eSam som att man ger uttryck för att en myndighet röjer en uppgift som omfattas av sekretess om myndigheten lämnar ut uppgiften till en privat tjänsteleverantör som enligt den lag denne har att följa kan bli tvungen att lämna ut uppgiften till en utländsk myndighet utan att sekretessprövning först gjorts av en svensk myndighet.

I skriften *Outsourcing 2.0 En vägledning om sekretess och dataskydd* som publicerades i december 2019 kommenterar eSam det resonemang som förs i promemorian. Det framgår tydligt av denna vägledning att den utländska lagstiftning som eSam åsyftar är den år 2018 antagna amerikanska lagstiftningen Clarifying Lawful Overseas Use of Data Act (US CLOUD Act). Enligt eSam innebär denna lagstiftning att amerikanska myndigheter under vissa förutsättningar kan begära att privata tjänsteleverantörer som är underkastade amerikansk jurisdiktion, ska bevara eller lämna ut uppgifter som är under tjänsteleverantörens kontroll utan att gå vägen via internationell rättshjälp.

9.5.3 Kritik mot eSam:s ställningstaganden

De ställningstaganden som eSam gjort under åren 2018 till 2019 har kritiserats i olika sammanhang.

Representanter från Sveriges kommuner och regioner (SKR) har bl.a. – trots att organisationen ingår i eSam – gett uttryck för uppfattningen att US CLOUD Act inte behöver innebära några ökade risker för offentlig sektors molninvesteringar. Även Microsoft har gett uttryck för en liknande uppfattning.[2]

Kritik har också riktats mot eSam från advokathåll.[3] Kritiken som har haft molntjänster i fokus kan sägas ha legat på två plan. Kritikerna menar – för det första – att det saknas rättsligt stöd för att kräva annat än att myndigheterna inför en förestående utkontraktering ska genomföra den av eSam förordade sannolikhetsbedömningen. För det andra menar kritikerna att den faktiska sannolik-

[2] Voister, *Esam om Cloud Act kritik* (2019) och Microsoft, *Molntjänster och säkerhet* (2018).
[3] Cirio Advokatbyrå AB, *Molntjänster, offentlighet- och sekretess i offentlig sektor. Utredning om och förslag till lagstiftning rörande offentlig sektors möjligheter att använda publika molntjänster* (2020).

heten för att uppgifter som lagras hos molntjänster skulle lämnas ut till amerikanska myndigheter med stöd av US CLOUD Act är låg.[4]

9.6 Digitaliseringsrättsutredningen

Digitaliseringsrättsutredningen analyserade frågan hur utkontraktering av it-drift förhåller sig till röjandebegreppet i OSL.

Utredningen konstaterade att det är omtvistat om det finns rättsliga förutsättningar för att under vissa omständigheter lämna ut sekretessbelagda uppgifter utan att ett röjande av uppgifterna faktiskt sker (s. 349). Utredningen tog inte uttrycklig ställning till frågan men pekade ändå på ett par omständigheter som enligt utredningen talade mot att så skulle vara fallet oavsett om det endast är ett s.k. tekniskt tillgängliggörande av uppgifter och att den privata tjänsteleverantörens personal har förbjudits i avtal ta del av eller vidarebefordra informationen (s. 351 f.).

Utredningen påtalade att det av kommentaren till brottsbalken följer att det alltid är ett röjande att göra en uppgift tillgänglig för någon annan, oavsett om det sker ett faktiskt avslöjande av informationen. Vidare gav utredningen uttryck för uppfattningen att viss försiktighet bör iakttas när det gäller att hämta ledning i Högsta domstolens resonemang i rättsfallet NJA 1991 s. 103 eftersom resonemanget där avser gränsdragningen för straffansvar.

Slutligen ska sägas att utredningen även uppmärksammade att Transportstyrelsen i rapporten *Kartlägga hanteringen av vissa uppgifter* som författades på regeringens uppdrag med anledning av den s.k. Transportstyrelseskandalen år 2017 funnit att uppgifter som varit tillgängliga för obehöriga var att betrakta som i formell mening röjda även om det inte fanns några indikationer på att uppgifterna kommit i orätta händer.

[4] Kritiken har bemötts av eSam och en av Esams kritiker har replikerat, se eSam, *Kommentar till kritisk rapport om molntjänster i offentlig sektor* (2020) och Computer Sweden, *Varför bemöter inte Esam och Försäkringskassan huvudpunkterna i vår kritik?* (2020).

9.7 Några myndighetsrapporter

9.7.1 Statens servicecenter

I februari 2015 publicerade Statens servicecenter (SSC) skriften *En förvaltningsgemensam tjänst för e-arkiv – delrapport*. I bilaga 4 till rapporten som har titeln *Offentlighet och sekretess inom en förvaltningsgemensam e-arkivtjänst* analyseras hur outsourcing (av oss benämnt utkontraktering) av it-drift förhåller sig till röjandebegreppet i OSL i ljuset av det ovan nämnda beslutet från JO.

Utan att ta uttrycklig ställning förs i bilagan ett resonemang om vilka möjligheter som finns för myndigheter att – utan en sekretessbrytande bestämmelse – utkontraktera it-drift till privata tjänsteleverantörer när de uppgifter som omfattas av utkontrakteringen är sekretessreglerade. Bland omständigheter som skulle kunna vägas in vid en skadeprövning enligt OSL nämns det förhållandet att avtal träffats som begränsar tjänsteleverantörens rättsliga möjligheter att ta del av det sakliga innehållet i uppgiftssamlingarna eller förekomsten av tekniska åtgärder som exempelvis kryptering. I de fall utkontrakteringen avser uppgifter som omfattas av absolut sekretess sägs att kryptering torde vara nödvändigt och att en sådan möjligen skulle kunna få den följden att uppgifterna inte kan anses ha röjts enligt OSL. Det understryks att argumentationen är vansklig inte minst mot bakgrund av det aktuella beslutet från JO.

En annan sak som i detta sammanhang är värt att lyfta fram är att det i bilagan ges uttryck för uppfattningen att det förefaller ha utvecklats en praxis som innebär att ett utlämnande av handlingar som sker endast för teknisk bearbetning och teknisk lagring utanför myndigheten inte skulle utgöra ett röjande i den mening som avses i OSL. I bilagan sägs att denna praxis möjligen grundar sig på det förhållandet att ett sådant utlämnande inte utgör någon expediering i tryckfrihetsförordningens (TF) mening. Vidare hänvisas till ett uttalande i lagmotiven (prop. 1975/76:160 s. 137) där det sägs att det är naturligt att se saken så att upptagningen [vid teknisk bearbetning och teknisk lagring utanför myndigheten] aldrig har befunnit sig utanför myndigheten.

9.7.2 Pensionsmyndigheten

I rapporten *Molntjänster i staten En ny generation av outsourcing* från Pensionsmyndigheten (se avsnitt 3.1) sägs bl.a. att om en myndighet anlitar en molntjänstleverantör och den information som myndigheten har för avsikt att lämna ut till den aktuella molntjänstleverantören är sekretessreglerad, har myndigheten att ta ställning till om sekretess utgör ett hinder för utlämnande (s. 39).

Av allt att döma var det således Pensionsmyndighetens utgångspunkt att en myndighet röjer uppgifter i den mening som avses i OSL om den lämnar ut uppgifter till en molntjänstleverantör. Med hänvisning till E-delegationens förstudie (se ovan) konstateras emellertid i rapporten att det förekommer diskussioner om det är möjligt att lämna ut sekretessbelagda uppgifter till externa it-leverantörer under förutsättning att uppgifterna inte röjs för leverantören (s. 40). Enligt den bedömning Pensionsmyndigheten gjorde i rapporten ligger det nära till hands att uppgifterna inte kan anses röjda om myndigheten krypterar informationen innan den överlämnas till molntjänstleverantören och att frågan om sekretess hindrar ett utlämnande därmed faller. Detta ansågs dock förutsätta att myndigheten behåller krypteringsnyckeln, att leverantören inte har någon möjlighet att ta del av uppgifterna i läsbart format eller uppfatta de sekretessbelagda uppgifterna på annat sätt, att uppgifterna är krypteringsskyddade på samma sätt hos eventuella underleverantörer, att lämpliga avtalsvillkor upprättas mellan parterna för att förhindra att leverantören tar del av uppgifterna om en sådan möjlighet trots allt skulle uppstå och att myndigheten har tillgång till konkreta verktyg för att kunna granska leverantörens hantering och kontrollera att denne efterlever avtalsvillkoren.

9.7.3 Kammarkollegiet

I februari 2019 publicerade Kammarkollegiet förstudien *Webbaserat kontorsstöd*.

I studien öppnade Kammarkollegiet upp för synsättet att uppgifter som levererats till en molntjänstleverantör inte nödvändigtvis måste betraktas som röjda i den mening som avses i OSL (s. 33). Detta skulle – enligt Kammarkollegiet – förutsätta att myndigheten i avtalet med molntjänstleverantören tydligt anger att leverantörens

personal inte får ta del av lagrade uppgifter utan myndighetens förhandstillstånd. Enlig Kammarkollegiet möjliggör detta för myndigheten att göra en sekretessprövning i det enskilda fallet.

Kammarkollegiet tog i studien även upp frågan om kryptering eller andra åtgärder med samma verkan kan innebära att sekretessreglerade uppgifter får hanteras av en privat tjänsteleverantör (s. 34). Det framstår som oklart om Kammarkollegiet menade att dessa åtgärder kan ha betydelse för frågan om uppgifterna ska betraktas som röjda enligt OSL eller om åtgärderna endast har betydelse som omständigheter att beakta vid den skadeprövning som myndigheten har att göra inför ett eventuellt röjande.

Slutligen ska sägas att Kammarkollegiet sade sig instämma i den slutsats som eSam gav uttryck för i sitt rättsliga uttalande från oktober 2018 (s. 35). Det som här avsågs var uttalandet om att uppgifter som finns tillgängliga i en utländsk molntjänst bör betraktas som röjda om den privata tjänsteleverantören är bunden av regler i ett annat land, enligt vilka leverantören kan bli skyldig att överlämna information till en myndighet i det landet utan att internationell rättshjälp anlitats eller annan laglig grund finns enligt svensk rätt.

9.7.4 Försäkringskassan

I november 2019 publicerade Försäkringskassan skriften *Vitbok Molntjänster i samhällsbärande verksamhet – risker, lämplighet och vägen framåt.*

I vitboken sade sig Försäkringskassan dela den bedömning som eSam och Kammarkollegiet förordade, nämligen att det måste betraktas som ett röjande enligt OSL, att vid utkontraktering anlita privata tjänsteleverantörer som kan komma att lämna ut uppgifter till ett annat lands myndigheter (s. 30). Enligt Försäkringskassans bedömning kunde inte kryptering lösa normkonflikten. Enligt Försäkringskassan kan det inte heller uteslutas att en myndighet i ett annat land som anser sig behörig att tillgå uppgifter också anser sig ha rätt att tillgå krypteringsnycklar. Vidare framhöll Försäkringskassan att de krypteringsmetoder som skulle försvåra en sådan tillgång skulle medföra att en stor del av tjänsternas funktionalitet kraftigt skulle försämras.

9.8 Några synpunkter på tidigare utredningar m.m.

9.8.1 Inledning

Det är tydligt att det synsätt som eSam förespråkar har fått ett betydande genomslag. Flera myndigheter har åtminstone delvis anammat den argumentation som eSam för (för enkelhetens skull skriver vi i det följande eSam även i det fall uppfattningen delas av flera).

I detta avsnitt redovisar vi vår syn på några av de ställningstagandena som kommit till uttryck i tidigare utredningar. Innan vi närmare går in på våra synpunkter är ett par påpekanden på plats.

Som vi redovisar ovan (avsnitt 8.9) är det vår bedömning att en uppgift som är utlämnad också är röjd oavsett om någon tagit del av uppgiften eller inte. Ett utlämnande är en form av röjande. Av detta följer att en uppgift inte kan vara utlämnad utan att samtidigt vara röjd.

Det har inte gjorts någon närmare analys av hur uttrycken röja och lämna ut förhåller sig till varandra i någon av de tidigare utredningarna. Uttrycket *lämna ut* verkar i vissa fall ha använts i enlighet med den tolkningen vi har gjort. I vissa andra fall har uttrycket använts på ett sätt som indikerar att man inte nödvändigtvis betraktat en utlämnad uppgift som röjd.

När det gäller det ovan redovisade JO-beslutet bör noteras att frågan inte gällde om sekretessreglerade uppgifter hade lämnats ut eller röjts. Det ansågs vara givet att så var fallet eftersom uppgifterna hanterades av personer (läkarsekreterarna) som inte ingick i myndighetens verksamhet (jfr 2 kap. 1 § OSL). Frågan var i stället om de två vårdgivarna hade haft laga grund för att lämna ut sekretessreglerade uppgifter till läkarsekreterarna.

9.8.2 Teknisk bearbetning eller teknisk lagring

Utredningens bedömning: Det förekommer att en privat tjänsteleverantör eller en myndighet endast tekniskt bearbetar eller tekniskt lagrar uppgifter på uppdrag av en myndighet. Det finns inget stöd för antagandet att uppdragsmyndigheten inte röjer uppgifterna i enlighet med offentlighets- och sekretesslagen (2009:400) i en sådan situation.

Inledning

I bilaga 4 till den tidigare redovisade rapporten från SSC sägs att det förefaller ha utvecklats en praxis som innebär att ett utlämnande av handlingar som sker endast för teknisk bearbetning och teknisk lagring utanför myndigheten inte skulle utgöra ett röjande i den mening som avses i OSL. Som vi tidigare nämnt har man i detta sammanhang bl.a. hänvisat till lagmotiven där det sägs att det är naturligt att se saken så att upptagningen [vid teknisk bearbetning och teknisk lagring utanför myndigheten] aldrig har befunnit sig utanför myndigheten.

Syftet med detta avsnitt är att undersöka om det finns grund för antagandet att uppdragsmyndigheten inte röjer uppgifterna i enlighet med OSL i en sådan situation.

Bestämmelserna i TF

Som vi redogjort för ovan följer av 2 kap. 9 § tredje stycket TF att en åtgärd som någon vidtar endast som ett led i en teknisk bearbetning eller teknisk lagring av en handling som en myndighet har tillhandahållit inte ska anses leda till att handlingen har kommit in till myndigheten. Bestämmelsen reglerar alltså den situationen att en icke allmän handling, som någon har bearbetat eller lagrat tekniskt, återkommer till den myndighet som tillhandahöll den. Handlingen ska vid återkomsten inte anses vara inkommen.

En handling som förvaras hos en myndighet endast som ett led i en teknisk bearbetning eller teknisk lagring för någon annans räkning anses inte som allmän handling hos den myndigheten (2 kap. 13 § första stycket TF).

Dessa bestämmelser tillkom år 1978 i samband med att 2 kap. TF ersattes med ett helt nytt kapitel.

I allmänmotiveringen till 2 kap. 10 § TF (nuvarande 2 kap. 13 § första stycket TF) anförde departementschefen bl.a. att offentlighetsprincipen inte krävde att allmänheten skulle ha tillgång till en upptagning hos en myndighet som endast har teknisk befattning med den (prop. 1975/76:160 s. 87). Vidare påtalades att undantagsbestämmelsen inte endast träffade den situationen att en myndighet tekniskt bearbetade eller lagrade upptagningar för annan myndighets räkning utan även när myndigheten agerade på uppdrag av enskild.

I specialmotiveringen tydliggjordes att undantagsbestämmelsen – i likhet med vad som alltjämt gäller – var tillämplig på *handlingar*, dvs. såväl traditionella pappershandlingar som upptagningar (s. 171). Härutöver påpekades att t.ex. en magnetbandsupptagning som förvarades hos en arkivmyndighet normalt inte kunde anses lagrad för annans räkning.

I specialmotiveringen till 2 kap. 6 § andra stycket TF (nuvarande 2 kap. 9 § tredje stycket TF) anfördes som exempel på en situation då bestämmelsen skulle kunna vara tillämplig att en myndighet översände ett maskinskrivet manuskript till en datacentral för överföring av texten till ett magnetband (prop. 1975/76:160 s. 137). Enligt den bedömning som gjordes fick uppenbarligen den omständigheten att magnetbandsupptagningen blev tillgänglig för den uppdragsgivande myndigheten inte medföra att upptagningen ansågs ha inkommit dit. Enligt departementschefen var det i sådana fall naturligt att se saken så att upptagningen aldrig hade befunnit sig utanför myndigheten. För att hålla undan sådana situationer bedömdes det dock som nödvändigt att införa en särskild undantagsbestämmelse.

Liknande situationer som vid teknisk bearbetning kunde – enligt departementschefen – uppkomma vid teknisk lagring för myndighets räkning. Som exempel på detta nämndes sådan lagring som krävde särskilda tekniska anordningar, t.ex. lagring av information i skrivminne eller på magnetband.

Någon särskild bestämmelse om att en handling som en myndighet ställde till förfogande för en annan myndighet endast för teknisk bearbetning eller teknisk lagring inte skulle anses som inkommen till den senare myndigheten föreslogs inte. Skälet för detta angavs vara att en sådan handling enligt 2 kap. 10 § TF över huvud taget inte skulle betraktas som en allmän handling (s. 138).

Bestämmelserna i OSL

En bestämmelse om överföring av sekretess

Får en myndighet i verksamhet för enbart teknisk bearbetning eller teknisk lagring för en annan myndighets räkning en uppgift som hos den senare myndigheten är sekretessreglerad av hänsyn till ett allmänt intresse, blir sekretessbestämmelsen tillämplig även hos den mottagande myndigheten (11 kap. 4 a § OSL).

Av lagmotiven framgår att bestämmelsen är tänkt att tillämpas när en myndighet tillhandahåller digitala tjänster åt en annan myndighet och vid en myndighets utkontraktering av it-drift till en annan myndighet (prop. 2016/17:198 s. 28). Bestämmelsen är även tillämplig på uppgifter som den mottagande myndigheten får av enskilda och andra myndigheter än beställarmyndigheten för den senare myndighetens räkning. En förutsättning för att bestämmelsen ska vara tillämplig är förstås att dessa digitala tjänster och utkontrakteringar har utformats på ett sådant sätt att de avser förvaring av handlingar endast som ett led i en teknisk bearbetning eller teknisk lagring för annans räkning.

Tillämpningsområdet för bestämmelsen är detsamma som för den undantagsbestämmelse som finns i 2 kap. 13 § TF vars innehåll nyss beskrivits. Detta innebär att de uppgifter som omfattas av sekretessen aldrig kan finnas dokumenterade i allmänna handlingar hos myndigheten.

Det bör noteras att det endast är sekretess till skydd för allmänna intressen som överförs. Sådana sekretessbestämmelser finns i 15–20 kap. OSL.

Av 11 kap. 8 § OSL följer att bestämmelsen inte gäller om en primär sekretessbestämmelse till skydd för samma intresse redan är tillämplig på uppgifterna hos den mottagande myndigheten. I sådant fall ska i stället den primära sekretessbestämmelsen tillämpas, oavsett om den primära sekretessen är starkare eller svagare än den sekundära sekretessen.

En sekretessbestämmelse till skydd för enskilds personliga och ekonomiska förhållanden

Sekretess gäller i verksamhet för enbart teknisk bearbetning eller teknisk lagring för någon annans räkning för uppgift om en enskilds personliga eller ekonomiska förhållanden (40 kap. 5 § OSL).

Bestämmelsen fick sin nuvarande lydelse genom lagändringar som trädde i kraft den 1 januari 2018. Dessförinnan var bestämmelsen utformad på det sättet att den angav att sekretess gällde i verksamhet för enbart teknisk bearbetning eller teknisk lagring för någon annans räkning av personuppgifter som avsågs i personuppgiftslagen (1998:204) (numera upphävd) för uppgift om enskilds personliga eller ekonomiska förhållanden.

Till grund för den lagändring som gjordes låg de förslag som lämnats i E-delegationens betänkande (SOU 2014:39) *Så enkelt så möjligt för så många som möjligt*. Delegationen gjorde bedömningen att bestämmelsens *föremål* (dvs. de uppgifter som kunde hemlighållas) – enligt den tidigare lydelsen – hade begränsats inte bara till uppgifter om enskildas personliga och ekonomiska förhållanden utan också till personuppgifter som avsågs i personuppgiftslagen (s. 63).

Regeringen delade E-delegationens allmänna bedömning nämligen att sekretessbestämmelsens tillämpningsområde behövde vidgas bl.a. av det skälet att det skulle underlätta utkontraktering av it-drift till myndigheter. Däremot menade regeringen att det utifrån bestämmelsens ordalydelse låg närmare till hands att uppfatta att inskränkningen till personuppgifter avsåg bestämmelsens *räckvidd* snarare än föremål (prop. 2016/17:198 s. 18). Bestämmelsen innebar således – enligt regeringen – att sekretessen gällde i verksamhet som enbart avsåg teknisk bearbetning och teknisk lagring av personuppgifter för annans räkning. Bestämmelsen var alltså inte tillämplig i alla typer av bearbetnings- eller lagringsverksamhet för annans räkning, utan bara i sådan verksamhet som omfattade bearbetning eller lagring av just personuppgifter.

Med den lydelse bestämmelsen nu har råder ingen tvekan om att dess räckvidd omfattar all verksamhet som enbart avser teknisk bearbetning och teknisk lagring av uppgifter för annans räkning. Sekretessens föremål är liksom tidigare enskilds personliga eller ekonomiska förhållanden. Sekretessen är absolut, dvs. någon skadeprövning ska inte göras.

Tillämpningsområdet för bestämmelsen är detsamma som för den undantagsbestämmelse som finns i 2 kap. 13 § TF.

Slutligen bör nämnas att bestämmelsen inte endast täcker in en situation där en myndighet utför tjänster på uppdrag av en annan myndighet. Även det fallet att en myndighet utför tjänster på uppdrag av en privat aktör omfattas.

Bestämmelserna om teknisk lagring och teknisk bearbetning i relation till röjandebegreppet

Inledningsvis kan vi konstatera att de bestämmelser som vi redogjort för ovan inte reglerar frågan när en uppgift ska anses vara röjd enligt OSL. En direkt tillämpning av bestämmelserna kan därmed inte leda

till antagandet att endast det förhållandet att handlingar enbart tekniskt bearbetas eller tekniskt lagras av någon på uppdrag av en myndighet ska innebära att uppdragsmyndigheten inte har röjt uppgifterna som finns i handlingarna enligt OSL.

Med utgångspunkt i det exempel att någon på uppdrag av en myndighet ska överföra ett maskinskrivet manuskript till ett magnetband anförde departementschefen – i specialmotiveringen till 2 kap. 6 § andra stycket TF (nuvarande 2 kap. 9 § tredje stycket) – att det var naturligt att se saken så att upptagningen aldrig hade befunnit sig utanför myndigheten. Uttalandet skulle kunna uppfattas på det sättet att lagstiftaren därigenom slog fast att – i sådana fall – de uppgifter som finns i handlingarna inte ska betraktas som röjda enligt OSL. Om man ska se saken så att handlingarna aldrig har lämnat myndigheten så kan förstås uppgifterna som finns i handlingarna inte heller vara röjda.

En invändning mot det sättet att resonera är att handlingarna faktiskt har lämnat myndigheten i sådana fall eftersom undantagsbestämmelsen i 2 kap. 9 § tredje stycket TF annars inte skulle fylla någon funktion.

Vi kan konstatera att det i lagmotiven till de aktuella bestämmelserna i TF inte finns något uttalande som egentligen stödjer antagandet att en myndighet som uppdrar åt en annan myndighet att enbart tekniskt bearbeta handlingar inte röjer uppgifterna som finns dokumenterade i dessa. Inte heller finns det stöd för ett sådant antagande i rättspraxis eller i litteraturen.

Till detta kommer att lagstiftaren har bedömt att det finns behov av att i 11 kap. 4 a § OSL införa en bestämmelse om överföring av sekretess. Får en myndighet i verksamhet för enbart teknisk bearbetning eller teknisk lagring för en annan myndighets räkning en uppgift som hos den senare myndigheten är sekretessreglerad av hänsyn till ett allmänt intresse, blir sekretessbestämmelsen tillämplig även hos den mottagande myndigheten.

Det är en berättigad fråga varför denna bestämmelse ens skulle behövas om det vore så att den uppdragsgivande myndigheten inte skulle anses ha röjt uppgifterna till den mottagande myndigheten. En bestämmelse om överföring av sekretess är enligt sin definition en bestämmelse som innebär att en sekretessbestämmelse som är tillämplig på en uppgift hos en myndighet, ska tillämpas på uppgiften även av en myndighet som uppgiften lämnas till eller som har elek-

tronisk tillgång till uppgiften hos den förstnämnda myndigheten (3 kap. 1 § OSL). En förutsättning för att en bestämmelse om överföring av sekretess ska tillämpas är alltså att en myndighet har lämnat uppgifter till en annan myndighet, eller givit den andra myndigheten tillgång till uppgiften, dvs. röjt uppgiften.

I detta sammanhang kan också tilläggas att det varken i lagmotiven till 11 kap. 4 a § eller 40 kap. 5 § OSL eller i lagmotiven till den senare bestämmelsens föregångare i 9 kap. 7 § i 1980 års sekretesslag finns något som stödjer antagandet att endast det förhållandet att handlingar enbart tekniskt bearbetas eller tekniskt lagras av någon på uppdrag av en myndighet ska innebära att uppdragsmyndigheten inte har röjt uppgifterna som finns i handlingarna enligt OSL (se Ds Ju 1977:11, Del 2, s. 455 ff., prop. 1979/80:2, Del A, s. 271 ff. och prop. 1997/98:44 s. 148).

Mot denna bakgrund gör vi bedömningen att det saknas grund för ett sådant antagande.

9.8.3 US CLOUD Act och liknande regleringar och 8 kap. 3 § OSL

Utredningens bedömning: Det förhållandet att det finns en risk för att en privat tjänsteleverantör i enlighet med den lagstiftning som denne är bunden av (t.ex. US CLOUD Act eller någon liknande reglering) kan bli tvungen att lämna ut uppgifter till en utländsk myndighet innebär inte att den svenska myndigheten handlar i strid med 8 kap. 3 § offentlighets- och sekretesslagen (2009:400) när den lämnar ut uppgifterna till tjänsteleverantören. Inte heller kan det bli fråga om ett otillåtet röjande enligt 8 kap. 3 § offentlighets- och sekretesslagen om tjänsteleverantören i ett senare skede lämnar ut uppgifterna till en utländsk myndighet.

Av våra direktiv framgår att vi särskilt ska analysera eventuella konsekvenser av att uppgifter som lämnas ut till en privat tjänsteleverantör kan komma att exponeras för andra staters rättsordningar, med särskilt fokus på betydelsen av rättsakter från tredjeland, t.ex. US CLOUD Act.

I 8 kap. 3 § OSL föreskrivs att en uppgift för vilken sekretess gäller enligt denna lag inte får röjas för en utländsk myndighet eller en mellanfolklig organisation, om inte utlämnande sker i enlighet med särskild föreskrift i lag eller förordning (p. 1), eller uppgiften i motsvarande fall skulle få lämnas ut till en svensk myndighet och det enligt den utlämnande myndighetens prövning står klart att det är förenligt med svenska intressen att uppgiften lämnas till den utländska myndigheten eller den mellanfolkliga organisationen (p. 2).

Bestämmelserna i 8 kap. 3 § OSL innebär alltså ett förbud för myndigheter att i vissa fall röja uppgifter för utländska myndigheter eller mellanfolkliga organisationer. Att en svensk myndighet för över uppgifter till privata tjänsteleverantörer som är bundna av US CLOUD Act eller någon liknande reglering innebär att det finns en risk för att tjänsteleverantörerna lämnar uppgifterna till utländska myndigheter.

Vi vill här framhålla att en risk för att uppgifterna ska överlämnas till utländska myndigheter inte enligt vår mening innebär att uppgifterna röjs till utländska myndigheter redan genom att de lämnas ut till tjänsteleverantörerna. Som vi ser det bryter alltså inte en myndighet mot 8 kap. 3 § OSL genom att lämna ut uppgifter till en tjänsteleverantör som är bunden av US CLOUD Act eller någon liknande reglering. Detta eftersom den nämnda bestämmelsen tar sikte på den situationen att en myndighet lämnar en uppgift direkt till en utländsk myndighet. Enligt vår bedömning kan det inte heller bli fråga om ett otillåtet röjande enligt 8 kap. 3 § OSL om tjänsteleverantören lämnar ut uppgifterna till en utländsk myndighet i ett senare skede eftersom det endast är en sådan aktör som är bunden av OSL som kan vidta en åtgärd som leder till att uppgifter röjs.

9.9 När är en uppgift röjd i den mening som avses i straffbestämmelsen om vårdslöshet med hemlig uppgift enligt NJA 1991 s. 103?

Utredningens bedömning: NJA 1991 s. 103 innebär att en hemlig uppgift som finns dokumenterad i en pappershandling ska anses ha röjts i den mening som avses i straffbestämmelsen om vårdslöshet med hemlig uppgift i 19 kap. 9 § brottsbalken, om någon vidtar en åtgärd som innebär att obehöriga tillgängliggörs den hemliga uppgiften under sådana omständigheter att man måste räkna med att den obehörige kommer att ta del av uppgiften.

9.9.1 Inledning

Som följer av vår redogörelse ovan uttalas i NJA 1991 s. 103 att avgörande för straffansvar främst bör vara om uppgiften har blivit tillgänglig för någon obehörig under sådana omständigheter, att man måste räkna med att den obehörige kommer att ta del av uppgiften.

Syftet med detta avsnitt är att närmare klargöra när en uppgift – enligt rättsfallet – ska anses som röjd enligt straffbestämmelsen om vårdslöshet med hemlig uppgift i 19 kap. 9 § brottsbalken.

Frågan om de i rättsfallet uppställda riktlinjerna kan användas för att avgöra om en utkontraktering innebär att uppgifter som omfattas av utkontrakteringen röjs enligt OSL behandlas i nästa kapitel.

9.9.2 Rättsfallet handlar om det objektiva rekvisitet röjer uppgift

I såväl tingsrättens som hovrättens domar diskuteras frågan om uppgifterna hade röjts i enlighet med 19 kap. 9 § brottsbalken. Ingressen till Högsta domstolens referat lyder *[f]råga om innebörden av uttrycket ”röjer uppgift” i 19 kap 9 § BrB (vårdslöshet med hemlig uppgift).* Vidare konstaterar Högsta domstolen i det sista stycket i sina domskäl att *[o]mständigheterna är inte heller sådana att de hemliga uppgifterna likväl kan anses ha röjts.*

Vi kan inte tolka dessa skrivningar på annat sätt än att rättsfallet handlar om det objektiva rekvisitet röjer uppgift i straffbestämmelsen om vårdslöshet med hemlig uppgift.

9.9.3 Besittning och tillgänglighet

Som vi uppfattar domskälen gör Högsta domstolen en åtskillnad mellan två olika situationer nämligen dels det fallet att en åtgärd leder till att en handling med en hemlig uppgift kommer i någon obehörigs *besittning*, dels det fallet att en åtgärd leder till att en hemlig uppgift blir *tillgänglig* för någon. En uppgift kan alltså vara tillgänglig för någon utan att denne har fått den handling i vilken uppgiften finns dokumenterad i sin besittning.

En åtgärd som innebär att en handling med hemliga uppgifter kommit i någon obehörigs besittning innebär – enligt huvudregeln – att uppgifterna som finns dokumenterade i handlingen röjs (den femte meningen i första stycket i de ovan citerade domskälen). Med tanke på vad rättsfallet handlar om finns skäl att utgå ifrån att Högsta domstolen med handling i detta fall avser en pappershandling, alltså ett fysiskt objekt. Detta ligger också i linje med det förhållandet att domstolen talar om besittning. Man kan vara i besittning av ett fysiskt objekt t.ex. en pappershandling. Däremot framstår det som tveksamt om man kan hävda att någon kan vara i besittning av uppgiften i sig.

Varje åtgärd som leder till att någon obehörig tillgängliggörs uppgifter som finns i en pappershandling leder inte till att uppgifterna i pappershandlingen röjs (den sjunde meningen i första stycket i de ovan citerade domskälen). Detta framstår som logiskt och följdriktigt. Antag t.ex. att en myndighetsanställd som sitter på ett tåg lämnar kvar en pappershandling med en hemlig uppgift i kupén när han lämnar den för att dricka en kopp kaffe i bistrovagnen. I ett sådant fall kanske man kan hävda att uppgiften i pappershandlingen genom denna åtgärd tillgängliggjorts för alla som sitter i kupén. Det framstår samtidigt som långtgående att göra gällande att uppgiften röjts för alla dessa personer. För att avgränsa innebörden av röjandebegreppet i tillgänglighetsfallen introducerar Högsta domstolen regeln att uppgiften – för att den ska anses ha röjts i ett sådant fall – måste ha blivit tillgänglig för någon obehörig under sådana omständigheter, att man måste räkna med att den obehörige kommer att ta del

av uppgiften (den åttonde meningen i första stycket i de ovan citerade domskälen).

9.9.4 Högsta domstolens slutsats och bedömning

Mot bakgrund av det ovan anförda bedömer vi att riktlinjer som Högsta domstolens genom rättsfallet introducerade kan beskrivas enligt följande. *Om någon vidtar en åtgärd som innebär att obehöriga tillgängliggörs en hemlig uppgift som finns dokumenterade i en pappershandling ska uppgiften anses ha röjts i den mening som avses i straffbestämmelsen om vårdslöshet med hemlig uppgift enligt 19 kap. 9 § brottsbalken om uppgiften har blivit tillgänglig för någon obehörig under sådana omständigheter att man måste räkna med att den obehörige kommer att ta del av uppgiften.*

I de ovan citerade domskälens tredje stycke prövade Högsta domstolen – med en tillämpning av de i domskälen introducerade riktlinjerna – om uppgifterna i pärmarna skulle betraktas som röjda genom att de tilltalade förvarat nycklarna till säkerhetsskåpet i ett vanligt skåp gjort av trä.

I den andra meningen i samma stycke konstateras att det inte kunnat klarläggas huruvida inbrottstjuven tagit någon befattning med de i säkerhetsskåpet förvarade hemliga handlingarna. Detta uppfattar vi som synonymt med ett konstaterande att det i målet inte är visat att den av de tilltalade vidtagna åtgärden lett till att inbrottstjuven haft handlingarna i sin besittning. Som vi uppfattar saken menade emellertid Högsta domstolen att åtgärden lett till att uppgifterna hade blivit tillgängliga för obehöriga. Frågan blev därmed om de hemliga uppgifterna – genom den åtgärd som de tilltalade hade vidtagit – tillgängliggjorts för inbrottstjuven under sådana omständigheter att man måste ha räknat med att han skulle ta del av dem. I den tredje meningen besvarade Högsta domstolen den frågan nekande.

Enligt vår tolkning ogillades således åtalet av den anledning att det objektiva rekvisitet röjer i den aktuella straffbestämmelsen inte bedömdes vara uppfyllt.

9.10 Våra samlade bedömningar

Det förekommer att en privat tjänsteleverantör eller en myndighet endast tekniskt bearbetar eller tekniskt lagrar uppgifter på uppdrag av en myndighet. Det finns inget stöd för antagandet att uppdragsmyndigheten inte röjer uppgifterna i enlighet med OSL i en sådan situation.

Det förhållandet att en privat tjänsteleverantör är bunden av US CLOUD Act eller någon liknande reglering innebär att det finns en risk för att leverantören överlämnar uppgifter som omfattas av en utkontraktering till en utländsk myndighet. En sådan risk innebär inte att myndigheten gör sig skyldig till ett otillåtet röjande enligt 8 kap. 3 § OSL genom att överföra uppgifterna till tjänsteleverantören. Detta eftersom den nämnda bestämmelsen tar sikte på den situationen att en myndighet lämnar en uppgift direkt till en utländsk myndighet. Enligt vår bedömning kan det inte heller bli fråga om ett otillåtet röjande enligt 8 kap. 3 § OSL om tjänsteleverantören lämnar ut uppgifterna till en utländsk myndighet i ett senare skede eftersom det endast är en sådan aktör som är bunden av OSL som kan vidta en åtgärd som leder till att uppgifter röjs.

NJA 1991 s. 103 innebär att en hemlig uppgift som finns dokumenterad i en pappershandling ska anses ha röjts i den mening som avses i straffbestämmelsen om vårdslöshet med hemlig uppgift i 19 kap. 9 § brottsbalken, om någon vidtar en åtgärd som innebär att obehöriga tillgängliggörs den hemliga uppgiften under sådana omständigheter att man måste räkna med att den obehörige kommer att ta del av uppgiften.

10 En sekretessbrytande bestämmelse

10.1 Utkontraktering och röjande

Utredningens bedömning: En myndighet som utkontrakterar it-drift får anses ha lämnat ut de uppgifter som omfattas av utkontrakteringen till den privata tjänsteleverantören. Detta gäller oavsett om omständigheterna när uppgifterna tillgängliggjordes tjänsteleverantören var sådana att man – t.ex. på grund av kryptering eller annan teknisk säkerhetsåtgärd – inte måste ha räknat med att tjänsteleverantören eller någon annan utomstående skulle komma att ta del av uppgifterna. Uppgifterna är röjda enligt offentlighets- och sekretesslagen (2009:400) eftersom ett utlämnande är en form av röjande.

Röjandet sker när uppgifterna lämnas ut till tjänsteleverantören oavsett om denne är bunden av US CLOUD Act eller någon liknande reglering.

10.1.1 Inledning

Om en myndighets[1] utkontraktering av it-drift innebär att sekretessreglerade uppgifter röjs för den privata tjänsteleverantören så krävs det, för att en utkontraktering ska vara förenlig med OSL, att utlämnande sker efter en av myndigheten utförd skadeprövning, som utmynnat i slutsatsen att uppgifterna kan lämnas ut, eller med stöd av en sekretessbrytande bestämmelse. Finns det ingen tillämplig sekretessbrytande bestämmelse så saknas det stöd för att lämna

[1] Med myndigheter avses i detta kapitel statliga myndigheter, kommuner och regioner om inget annat framgår av sammanhanget.

ut uppgifter som omfattas av absolut sekretess inom ramen för utkontrakteringen.

I våra direktiv framhålls den rättsliga osäkerhet som råder beträffande röjandefrågan. Det är tydligt att dagens situation inte är tillfredsställande. För att vi ska kunna utföra vårt uppdrag och ta ställning till om författningsändring bör föreslås fordras det att vi svarar på frågan om en utkontraktering innebär ett röjande.

Som vi framhållit flera gånger är det vår bedömning att ett utlämnade är en form av röjande. En uppgift kan därmed inte vara utlämnad utan att samtidigt vara röjd. Härav följer att en utkontraktering – enligt vår tolkning – innebär att uppgifter röjs om den innebär att uppgifter lämnas ut.

Det krävs dock ett ställningstagande till frågan vilket eller vilka kriterier som ska vara avgörande för om en uppgift ska betraktas som utlämnad och därmed som röjd vid en utkontraktering. Vi måste därför fylla uttrycken röjd och utlämnad – som dessa begrepp ska förstås i kontexten utkontraktering – med ett konkret innehåll.

10.1.2 NJA 1991 s. 103 och utkontraktering

Vad innebär en tillämpning av de i 1991 års rättsfall uppställda riktlinjerna i detta sammanhang?

Som vi redovisar i avsnitt 2.2.5 kan en utkontraktering av it-drift innebära många olika saker. Vad det i grund och botten handlar om är att en myndighet beslutar att uppdra åt en privat tjänsteleverantör att hantera hela eller delar av myndighetens it-drift. Vad som är kännetecknande för alla former av utkontraktering av it-drift är att uppgiftssamlingar blir tillgängliga för tjänsteleverantören.

En tillämpning av de i 1991 års rättsfall uppställda riktlinjerna i detta sammanhang skulle enligt vår bedömning innebära att uppgifterna ska anses ha röjts endast om omständigheterna vid tillgängliggörandet var sådana att man måste ha räknat med att den privata tjänsteleverantören kommer att ta del av uppgifterna. Om det saknas skäl för ett sådant antagande och uppgifterna i enlighet med det sagda inte ska anses ha röjts behöver myndigheten alltså inte iaktta bestämmelserna i OSL.

Transportstyrelseskandalen och Arbetsdomstolens bedömning

I samband med Transportstyrelseskandalen år 2017 prövade Arbetsdomstolen frågan om den dåvarande generaldirektören för Transportstyrelsen hade gjort sig skyldig till vårdslöshet med hemlig uppgift (dom nr 15/19, mål nr AD 152/17, meddelad den 6 mars 2019). Den dåvarande generaldirektören hade fattat beslut om att – enkelt uttryckt – utkontraktera myndighetens it-drift. Dessa beslut kom att ifrågasättas av olika skäl och generaldirektören blev förflyttad till Regeringskansliet. Efter en tid blev hon emellertid avskedad därifrån.

Den övergripande fråga som Arbetsdomstolen hade att ta ställning till var om det funnits tillräckliga skäl att avskeda generaldirektören. Vid denna bedömning ansågs frågan om generaldirektören hade begått vårdslöshet med hemlig uppgift när hon fattade de aktuella besluten vara av betydelse. Arbetsdomstolen hänvisade till 1991 års rättsfall och menade att de i rättsfallet uppställda riktlinjerna skulle ligga till grund för bedömningen. Frågan var närmare bestämt om två driftstekniker i Tjeckien hade haft tillgång till hemliga uppgifter. Arbetsdomstolen fann att det inte var visat att så var fallet och gjorde därför bedömningen att uppgifterna inte hade röjts.

Som vi tolkar domskälen kom Arbetsdomstolen alltså fram till att uppgifterna inte hade röjts redan på den grunden att de inte hade varit tillgängliga för den privata tjänsteleverantören. Vid den bedömningen saknade därmed Arbetsdomstolen skäl att – i enlighet med 1991 års rättsfall – ta ställning till frågan om uppgifterna hade blivit tillgängliga för tjänsteleverantören under sådana omständigheter att man måste ha räknat med att tjänsteleverantören eller någon annan utomstående skulle komma att ta del av uppgifterna.

Det viktiga i detta sammanhang är emellertid det förhållandet att Arbetsdomstolen ansåg sig oförhindrad att tillämpa de i 1991 års rättsfall uppställda riktlinjerna för att ta ställning till frågan om uppgifter röjts i den mening som avses i bestämmelsen om vårdslöshet med hemlig uppgift. Givet att röjandebegreppet i den aktuella straffbestämmelsen respektive OSL ska anses ha samma innebörd skulle Arbetsdomstolens dom kunna åberopas som argument för att de i 1991 års rättsfall uppställda riktlinjerna även kan användas när man tar ställning till frågan om uppgifter ska betraktas som utlämnade i samband med att en myndighet utkontrakterar it-drift.

Det finns skäl att framhålla att Arbetsdomstolen är en specialdomstol med uppgift att döma i arbetsrättsliga tvister. De uttalanden som Arbetsdomstolen gör i frågor som ligger utanför arbetsrätten kan inte betraktas som prejudicerande. Betydelsen av Arbetsdomstolens dom i detta sammanhang ska därför inte överdrivas.

Till bilden hör också – som nämns i avsnitt 9.6 – att Transportstyrelsen i sin rapport till regeringen efter turerna år 2017 gjorde en annan bedömning än Arbetsdomstolen.

10.1.3 En utkontraktering innebär att uppgifterna lämnas ut och därmed röjs

Som följer av det föregående behandlas i 1991 års rättsfall innebörden av det objektiva rekvisitet röjer i straffbestämmelsen om vårdslöshet med hemlig uppgift i 19 kap. 9 § brottsbalken. Frågan är inledningsvis om uttrycket röjer i nämnda straffbestämmelse ska ha samma innebörd som motsvarande uttryck i OSL.

Ett förhållande som kan vara värt att notera i detta sammanhang är att 1980 års sekretesslag inte gällde för det bolag som i 1991 års rättsfall hade till uppgift att förvara pärmarna med hemliga uppgifter. De hemliga uppgifterna i pärmarna var alltså redan röjda – genom att de lämnats ut till bolaget – i den mening som avses i OSL. Det var således inte fråga om att någon myndighet vidtagit någon åtgärd varigenom uppgifterna hade röjts enligt OSL.

Som vi redan har varit inne på bör uttrycket röjer i OSL ha samma innebörd som motsvarande uttryck i straffbestämmelsen om brott mot tystnadsplikt i 20 kap. 3 § brottsbalken. En utgångspunkt måste vara att uttryck som förekommer i brottsbalken (19 kap. 9 § och 20 kap. 3 §) måste ges samma innebörd även om de förekommer i olika bestämmelser. Vår slutsats är därmed att rättsfallet kan användas vid en tolkning av röjandebegreppet i OSL. Frågan är emellertid vilken räckvidd prejudikatet ska anses ha.

Vi återgår till det i avsnitt 9.9.3 anförda exemplet med en myndighetsanställd som sitter på ett tåg lämnar kvar en pappershandling med en hemlig uppgift i kupén när han lämnar den för att dricka en kopp kaffe i bistrovagnen. Även om uppgifterna som finns dokumenterade i pappershandlingen kanske kan sägas ha blivit tillgängliga för alla i kupén framstår det som rimligt att de inte ska anses ha röjts med mindre än att omständigheterna var sådana att det fanns skäl att

räkna med att någon obehörig skulle ta del av dem. Alla åtgärder som leder till att uppgifterna tillgängliggörs för utomstående ska med andra ord inte leda till att de röjs. Att tillämpa de i rättsfallet uppställda riktlinjerna i en situation som det var fråga om i rättsfallet eller i liknande situationer framstår som logiskt och begripligt.

Vi avfärdar däremot den tanken att man kan resonera på samma sätt vid en utkontraktering av it-drift eftersom det är fråga om en helt annan situation. Det är i dessa fall fråga om en åtgärd som grundas på ett formenligt myndighetsbeslut som innebär att uppgiftssamlingar i görs tillgängliga för en privat tjänsteleverantör, alltså en aktör utanför myndigheten (jfr 2 kap. 1 § OSL). Utkontrakteringen innebär dessutom att tjänsteleverantören i enlighet med ett avtal med myndigheten hanterar den senares uppgifter. Även om omständigheterna vid tillgängliggörandet var sådana att man inte måste ha räknat med att tjänsteleverantören skulle komma att ta del av uppgifterna ter sig en argumentation som går ut på att myndigheten – i analogi med 1991 års rättsfall – inte skulle ha lämnat ut uppgifterna till tjänsteleverantören som svårförståelig. Det är således vår bedömning att en myndighet får anses lämna ut de uppgifter som omfattas av utkontrakteringen till tjänsteleverantören. Av definitionen av sekretess i 3 kap. 1 § OSL framgår att ett utlämnande är en form av röjande. Uppgifter kan alltså inte vara utlämnade utan att samtidigt vara röjda. En utkontraktering innebär följaktligen att de uppgifter som omfattas av utkontrakteringen röjs.

10.1.4 Avtalsreglerad tystnadsplikt, kryptering och pseudonymisering

Enligt våra direktiv ska vi i vår analys lägga särskild vikt vid frågan om avtalsreglerad tystnadsplikt och tekniska säkerhetsåtgärder, tex. kryptering eller pseudonymisering, kan påverka möjligheten att lämna ut uppgifter.

Ett avtal mellan en utkontrakterande myndighet och en privat tjänsteleverantör som förpliktar den senare att inte sprida de uppgifter som omfattas av utkontrakteringen (avtalsreglerad tystnadsplikt) har ingen inverkan på det förhållandet att myndigheten lämnar ut och därmed röjer uppgifterna för tjänsteleverantören. I enlighet med den tolkning som görs i föregående avsnitt röjs alltså de uppgifter som

omfattas av en utkontraktering till tjänsteleverantören oavsett förekomsten av en avtalad tystnadsplikt.

Som vi ser saken bör bedömningen bli densamma i de fall den privata tjänsteleverantören i avtal med myndigheten förbundit sig att inte ta del av uppgifterna.

En annan sak är att avtalad tystnadsplikt kan ha betydelse vid en eventuell skadeprövning (se avsnitt 10.2.3).

Kryptering och pseudonymisering utgör exempel på tekniska säkerhetsåtgärder som en myndighet kan, och ibland är skyldig att, vidta i syfte att försvåra för en obehörig att ta del av uppgifter. I vilken utsträckning åtgärder av detta slag faktiskt försvårar åtkomst beror på hur åtgärden utformats och vilka kunskaper och resurser i övrigt som finns hos tjänsteleverantören.

Det finns inga nu kända säkerhetsåtgärder som gör det helt, både i teori och praktik, omöjligt för tjänsteleverantören att ta del av uppgifterna. De tekniska säkerhetsåtgärderna medför alltså endast att det blir mer osannolikt att tjänsteleverantören tar del av uppgifterna i jämförelse med vad som skulle ha varit fallet om åtgärderna inte hade vidtagits. Vid en utkontraktering kan uppgifterna ändå – trots förekomsten av dylika säkerhetsåtgärder – sägas ha gjorts tillgängliga (åtminstone teoretiskt) för tjänsteleverantören.

Kännetecknande för alla former av utkontraktering av it-drift är att den alltid innebär att en myndighet fattar ett beslut som leder till att uppgiftssamlingar blir tillgängliga för en privat tjänsteleverantör. Det är vår uppfattning att även om omständigheterna vid tillgängliggörandet var sådana att man inte måste ha räknat med att tjänsteleverantören skulle komma att ta del av uppgifterna t.ex. på grund av kryptering, en argumentation som går ut på att myndigheten inte skulle ha lämnat ut och därmed röjt uppgifterna till tjänsteleverantören ter sig svårbegriplig (jfr föregående avsnitt). Hur man än ser på saken går det inte komma ifrån att myndigheten genom ett formenligt beslut gjort uppgifterna tillgängliga för en utomstående aktör även om de är t.ex. krypterade.

En invändning mot detta skulle kunna vara att det i dag finns tekniska säkerhetsåtgärder som gör att det blir praktiskt sett omöjligt för en tjänsteleverantör att komma åt uppgifterna och att utkontrakteringen av det skälet inte bör betraktas som ett utlämnande av uppgifterna. Även om man skulle resonera på det sättet skulle det sannolikt inte leda till att alla tekniska säkerhetsåtgärder alltid skulle

bedömas innebära att uppgifterna i fråga inte skulle ha lämnats ut till tjänsteleverantören. Som just konstaterats finns ju inga nu kända säkerhetsåtgärder som gör det omöjligt i teori och praktik för tjänsteleverantören att ta del av uppgifterna. I vissa fall skulle säkerhetsåtgärderna leda till att uppgifterna inte ansågs utlämnande och i andra fall skulle de anses vara det trots säkerhetsåtgärder. Det skulle alltså bli nödvändigt att föra ett sannolikhetsresonemang.

Det kan konstateras att ett sannolikhetsresonemang skulle leda till svårbemästrade gränsdragningsproblem och därmed osäkerhet. Det finns många olika typer av säkerhetsåtgärder och vissa av dessa är väldigt säkra i den meningen att de bidrar till att göra det mycket osannolikt att tjänsteleverantören tar del av uppgifterna medan andra inte är lika säkra. Det finns skäl att anta att det inte alltid är så enkelt för den myndighet som står i begrepp att utkontraktera it-drift att avgöra vilka säkerhetsåtgärder som är tillräckligt säkra för att uppgifterna inte ska betraktas som utlämnade till tjänsteleverantören. Vi befarar att myndigheterna i många fall skulle vara utlämnade till den information om säkerhetsåtgärder som privata tjänsteleverantörer lämnar och att det kan vara svårt att på ett tillräckligt säkert sätt verifiera denna information.

Vi vill framhålla att det resonemang vi för ovan bör hållas isär från den skyldighet som kan finnas att skydda uppgifter genom t.ex. kryptering. Vi uttalar oss inte heller om värdet av kryptering eller andra säkerhetsåtgärder i sig. Förekomsten av sådana säkerhetsåtgärder kan vara helt avgörande för att uppgifter ska få hanteras t.ex. enligt säkerhetsskyddsregleringen. Kryptering och andra säkerhetsåtgärder kan också ha betydelse vid skadeprövningen enligt OSL (se avsnitt 10.2.3 och jfr beslut från JO den 4 juni 2019, Dnr 6794-2017, 6864-2017).

Mot denna bakgrund bedömer vi att en utkontraktering innebär att uppgifterna som omfattas av utkontrakteringen lämnas ut och därmed röjs i den mening som avses i OSL oavsett om de krypterats eller pseudonymiserats.

10.1.5 US CLOUD Act och liknande regleringar har ingen betydelse för frågan om uppgifterna anses ha röjts

I enlighet med vår bedömning ovan ska uppgifter som omfattas av en utkontraktering anses utlämnade till den privata tjänsteleverantören och därmed röjda. Röjandet sker när uppgifterna lämnas ut till

tjänsteleverantören oavsett om denne är bunden av CLOUD Act eller någon liknande reglering.

10.2 En sekretessbrytande bestämmelse behövs

Utredningens bedömning: En myndighet kan efter en övergripande skadeprövning finna att det inte finns något hinder mot att uppgifter lämnas ut och att en utkontraktering av it-drift som rör uppgifterna därmed kan ske. En sådan prövning kan emellertid vara svår att göra i en del fall.

Ett utlämnande med stöd av 10 kap. 14 § offentlighets- och sekretesslagen (2009:400) (utlämnande med förbehåll) kan i en utkontrakteringssituation ske endast i undantagsfall.

Det finns begränsade möjligheter för myndigheterna att utkontraktera it-drift om utkontrakteringen omfattar uppgifter som träffas av absolut sekretess. Ett utlämnande med stöd av undantagsbestämmelsen i 10 kap. 2 § offentlighets- och sekretesslagen (nödvändigt utlämnande) kan i en utkontrakteringssituation ske endast i undantagsfall.

Det finns behov av en sekretessbrytande bestämmelse som tar sikte på utkontraktering av it-drift.

Utredningens förslag: En sekretessbrytande bestämmelse som tar sikte på utkontraktering av it-drift bör införas.

10.2.1 Det finns ett behov av utkontraktering

Som vi redan konstaterat i vår kartläggning (kapitel 4) har många statliga myndigheter utkontrakterat delar av sin it-drift, t.ex. genom att använda olika typer av molntjänster. De statliga myndigheterna använder även andra typer av it-driftsrelaterade tjänster som inte kan betraktas som molntjänster. Det är sedan tidigare känt att många kommuner och regioner utkontrakterat it-drift. I Myndigheten för samhällsskydd och beredskaps rapport *Outsourcing av it-tjänster i kommuner* (2014) uppgav 80 procent av drygt 120 kommuner att de utkontrakterat it-tjänster.

I våra fallstudier har det framkommit att sekretessreglerade uppgifter ofta är uppblandade med icke sekretessreglerade uppgifter. Det är mot denna bakgrund inte orimligt att anta att myndigheter avstår från att utkontraktera it-drift för att undvika ett otillåtet röjande.

Det finns i vissa fall en möjlighet, i alla fall teoretiskt, för myndigheterna att hantera it-driften i egen regi i stället för att utkontraktera den. Det händer dock att myndigheter upplever praktiska hinder mot att bedriva it-drift i egen regi. Det kan t.ex. handla om att det saknas relevant kompetens inom verksamheten för att sköta it-driften i egen regi och att det är mer kostnadseffektivt att utkontraktera it-driften än att bygga upp den nödvändiga förmågan inom verksamheten.

Myndigheterna ska eftersträva en god ekonomisk hushållning i sin verksamhet. Utkontraktering kan vara ett nödvändigt led i att uppnå detta. Vi instämmer således med den bedömning som regeringen har gjort i lagmotiven till lagen (2020:914) om tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter (tystnadspliktslagen). I prop. 2019/20:201, s. 5 anförs följande:

> […] förvaltning och utveckling av it-drift och it-baserade funktioner [kräver ofta] specialistkompetens och avancerade tekniska hjälpmedel som inte alltid kan hanteras av varje myndighet för sig. För en del myndigheter är därför utkontraktering till en privat tjänsteleverantör eller anslutning till en samordnad myndighetsgemensam lösning för it-drift en förutsättning för att kunna bedriva verksamheten.

Det kan även finnas tekniska hinder som i praktiken gör det omöjligt att etablera it-drift av nödvändig funktionalitet inom den egna verksamheten.

Ett annat skäl som ofta framförs för utkontraktering av it-drift till privata tjänsteleverantörer är att den tjänsteleverantör som anlitas bedöms kunna erbjuda en säkrare hantering av myndighetens uppgifter än vad som hade varit fallet om myndigheten hanterat dessa i egen regi. Kraven på myndigheterna att åstadkomma en lämplig informationssäkerhet beror på verksamheternas uppdrag, karaktär och behov. Men även om it-drift i egen regi kan ge bättre förutsättningar för kontroll, leder det inte nödvändigtvis till bättre informationssäkerhet. Informationssäkerheten beror på flera olika faktorer, bl.a. verksamheternas kompetens, resurser och prioriteringar.

Enligt vår enkätundersökning hanterar 80 procent av de statliga myndigheter som svarade på enkäten sekretessreglerade uppgifter i sin kärnverksamhet. Vi vet inte exakt i vilken omfattning dessa uppgifter hanteras av privata tjänsteleverantörer inom ramen för de statliga myndigheternas utkontrakterade it-drift. Det får dock förutsättas att det förekommer utkontraktering som omfattar sekretessreglerade uppgifter. Om inte annat talar det behov av vägledning som av eSamverkansprogrammet (eSam) har bedömts finnas i denna fråga för en sådan slutsats.

Mot denna bakgrund anser vi att det är klarlagt att myndigheterna har behov av att utkontraktera it-drift som omfattar sekretessreglerade uppgifter.

10.2.2 Den nuvarande regleringssituationen

Inledning

Enligt direktiven är vi oförhindrade att föreslå ändringar i OSL. Våra förslag får dock inte innebära någon förändring av lagens struktur och begreppsapparat. Inte heller ska sådana förslag innefatta ändring av, eller tillägg till, lagens bestämmelser om beslutsordning eller sekretessprövningens metodik. I uppdraget ingår inte heller att föreslå ändringar i grundlag eller i säkerhetsskyddslagstiftningen.

För att klarlägga om det finns skäl att föreslå någon regeländring är det nödvändigt att dessförinnan inventera den nuvarande regleringssituationen. Det vi i första hand ser framför oss att detta delbetänkande kommer att utmynna i är förslag till ändringar i OSL med de begränsningar som beskrivs ovan. I linje med detta undersöker vi i detta avsnitt om den reglering som i dag finns i OSL ger fullgoda möjligheter för myndigheterna att med bibehållen säkerhet utkontraktera it-drift.

Utlämnande av sekretessreglerade uppgifter som omfattas av skaderekvisit

Regleringen i 2 kap. TF innebär att de uppgiftssamlingar som berörs av en utkontraktering kan utgöras av allmänna handlingar eller handlingar som inte är allmänna. Sekretess innebär ett förbud att röja upp-

gifter oavsett om dessa finns dokumenterade i allmänna handlingar eller handlingar som inte är allmänna. En annan sak är att offentlighetsprincipen endast ger en rätt att ta del av allmänna handlingar och uppgifter ur allmänna handlingar.

Vi har i det föregående (avsnitt 10.1.3) bedömt att röjandebegreppet i OSL ska tolkas på det sättet att en myndighets utkontraktering av it-drift innebär att den röjer de uppgifter som omfattas av utkontrakteringen. När beslutet om utkontraktering verkställs kommer uppgifterna som omfattas av utkontrakteringen att röjas oavsett om dessa finns dokumenterade i allmänna handlingar eller handlingar som inte är allmänna.

En myndighet som står i begrepp att utkontraktera it-drift måste analysera vilka uppgifter som berörs av utkontrakteringen. I de fall uppgifterna omfattas av sekretessbestämmelser med skaderekvisit uppstår frågan om regleringen medger en utkontraktering.

I 6 kap. 3 och 4 §§ OSL finns regler om hur en myndighet ska hantera en begäran om utlämnande av allmän handling och en begäran om utlämnande av en uppgift ur en allmän handling.

Det är tydligt att bestämmelserna i 6 kap. OSL är tänkta att tillämpas t.ex. när någon från allmänheten begär ut allmänna handlingar som förekommer i ett ärende som en befattningshavare på myndigheten handlägger.

Ett utlämnande av allmänna handlingar som sker med anledning av en utkontraktering, dvs. på myndighetens eget initiativ, skiljer sig på flera punkter från sådana utlämnanden som regleras i 6 kap. OSL. I OSL finns inga regler om sådana utlämnanden över huvud taget.

Inom statliga myndigheter är det myndighetens ledning som enligt myndighetsförordningen (2007:515) ansvarar för att verksamheten bedrivs effektivt och enligt gällande rätt. Myndighetens ledning beslutar i ärenden av principiell karaktär eller av större betydelse. De flesta andra ärenden får delegeras efter beslut av myndighetschefen eller den som denne beslutar. Vem som beslutar om ett utlämnande av uppgifter i samband med en utkontraktering får därför förutsättas följa av myndighetens arbets- och delegationsordning.

Inom kommuner är det enligt 6 kap. 6 § kommunallagen (2017:725) nämnderna som inom sitt respektive område ska se till att verksamheten bedrivs i enlighet med de lagar och bestämmelser som gäller för verksamheten. En nämnd får enligt 6 kap. 37 § kommunallagen uppdra åt presidiet, ett utskott, en ledamot, en ersättare eller en

anställd att besluta i ett ärende. Regleringen sker vanligen genom en delegationsordning.

En utkontraktering innebär ett utlämnande av uppgifter som sker på myndighetens eget initiativ. Ett sådant utlämnande är inte ett utslag av offentlighetsprincipen. Utlämnandet syftar snarare till att åstadkomma en väl fungerande it-driftlösning för myndigheten. I dessa situationer är det i regel inte möjligt att göra någon närmare granskning av varje enskild uppgift som lämnas ut. Den prövning som myndigheten har att göra blir därför ibland med nödvändighet övergripande.

Ett utlämnande av uppgifter behöver inte ske endast som ett led i ett förverkligande av offentlighetsprincipen. I 6 kap. 5 § OSL föreskrivs exempelvis att en myndighet ska på begäran av en annan myndighet lämna uppgift som den förfogar över, om inte uppgiften är sekretessbelagd eller det skulle hindra arbetets behöriga gång. I dessa fall sker alltså utlämnandet för den mottagande myndighetens skull.

S.k. massuttag som med nödvändighet förutsätter övergripande skadeprövningar förefaller inte heller vara något helt främmande. Saken berördes redan i lagmotiven till 1980 års sekretesslag (prop. 1979/80:2, Del A, s. 78 ff.). Enligt departementschefen bör det i de flesta fall finnas ett fullt tillräckligt underlag för bedömningen av om sekretessregleringen ska anses hindra ett utlämnande eller inte. Departementschefen hänvisade härvidlag till att befattningshavaren alltid har kännedom om beställarens identitet och oftast också dennes avsikt med uppgifterna.

I detta sammanhang bör den s.k. dataskyddssekretessen i 21 kap. 7 § OSL nämnas. Bestämmelsen innebär att sekretess gäller för personuppgift, om det kan antas att uppgiften efter ett utlämnande kommer att behandlas i strid med – såvitt här är av intresse – dataskyddsförordningen eller lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning.

I praktiken har bestämmelsen haft betydelse mestadels i fråga om massuttag eller uttag av s.k. selekterade uttag (se t.ex. RÅ 2002 ref. 54, NJA 2015 s. 180, NJA 2015 s. 624 och HFD 2014 ref. 66).

Även om det ovan nämnda uttalandet i lagmotiven till 1980 års sekretesslag och den praxis som finns i fråga om 21 kap. 7 § OSL och dess motsvarighet i 1980 års sekretesslag inte tar sikte på utkontrakteringssituationer kan konstateras att massuttag är något som förekommer och myndigheterna därmed ställs inför att hantera. Vi kan

inte se att det skulle finnas några betänkligheter mot att en myndighet efter en övergripande skadeprövning finner att det inte finns något hinder mot att uppgifter lämnas ut och att en utkontraktering av it-drift som rör uppgifterna därmed kan ske.

Något om skadeprövningen

Frågan är vilka omständigheter som bör tillmätas betydelse vid en sådan övergripande skadeprövning som föregår ett beslut om utkontraktering av uppgifter som omfattas av sekretess med ett skaderekvisit.

Som vi ser det måste man skilja mellan det fallet att uppgifterna omfattas av raka skaderekvisit och det fallet att de omfattas av omvända skaderekvisit. Av naturliga skäl måste man kunna anta att utrymmet för en utkontraktering är vidare i de fall uppgifterna som utkontrakteringen berör omfattas av raka skaderekvisit.

Ett sekretessavtal mellan den utkontrakterande myndigheten och en privat tjänsteleverantör innebär att den senare förbinder sig att inte utnyttja eller sprida de uppgifter som är föremål för utkontraktering. Genom ett sådant avtal åstadkoms därför en avtalsreglerad tystnadsplikt. I lagmotiven till vissa ändringar som gjordes i 1980 års sekretesslag uttalas att problemet med att personalen hos det företag som myndigheten har anlitat inte omfattas av sekretess oftast kan avhjälpas genom att det företag som myndigheten har anlitat har sekretessavtal med sina anställda (prop. 1981/82:186 s. 41–42). Sekretessavtal mellan den utkontrakterande myndigheten och en privat tjänsteleverantör kan alltså tillmätas betydelse i sammanhanget, i vart fall om uppgifterna i fråga omfattas av ett rakt skaderekvisit. I de fall uppgifterna omfattas av omvända skaderekvisit framstår det som mera tveksamt vilken betydelse ett sekretessavtal bör tillmätas. I det i avsnitt 9.3 refererade beslutet från JO – som avsåg uppgifter som omfattades av ett omvänt skaderekvisit – gjordes bedömningen att uppgifterna inte kunde lämnas ut trots förekomsten av ett sekretessavtal.

Som JO konstaterade följer en form av tystnadsplikt av dataskyddsregleringen. Den som behandlar personuppgifter i strid med dataskyddsregleringen, exempelvis genom att lämna ut dem när regleringen inte tillåter det, kan bli skadeståndsskyldig eller föremål för

tillsynsmyndighetens ingripande, inklusive sanktionsavgifter. En skillnad nu jämfört med vad som gällde vid tidpunkten för JO:s prövning är att dataskyddsförordningen nu tillämpas. Dataskyddsförordningen innebär skarpare sanktioner vid överträdelser av dataskyddsregelverket jämfört med vad som gällde enligt tidigare gällande lagstiftning. Detta kan möjligtvis få betydelse vid skadeprövningen men kan inte – såvitt vi kan bedöma – fullt ut kompensera för avsaknaden av en straffsanktionerad tystnadsplikt.

Enligt vår bedömning bör det däremot finnas utrymme för en annan bedömning i de fall mottagarna av uppgifterna omfattas av en straffsanktionerad tystnadsplikt. I sådana fall borde skadeprövningen oftare kunna mynna ut i att utkontraktering är möjlig även om uppgifterna i fråga omfattas av omvända skaderekvisit. Detta ligger för övrigt i linje med vad JO uttalar i det ovan omtalade beslutet.

Kryptering och andra tekniska åtgärder som försvårar för personalen hos en tjänsteleverantör att ta del av uppgifter som hanteras för myndighetens räkning bör enligt vår mening också kunna tillmätas betydelse vid skadeprövningen oavsett om uppgifterna i fråga omfattas av raka eller omvända skaderekvisit.

Av JO:s bedömningar följer vidare – såvitt vi förstår saken – att förekomsten av tystnadsplikt och tekniska åtgärder, exempelvis kryptering inte är de enda parametrarna som har betydelse vid skadeprövningen, oavsett om uppgifterna omfattas av raka eller omvända skaderekvisit. Enligt JO ska även frågan om vilka konsekvenser det skulle kunna leda till om tjänsteleverantörens personal sprider uppgifter vidare utan att det är tillåtet beaktas, exempelvis om straffrättsligt ansvar kan inträda.

Nödvändigt utlämnande

OSL innehåller inte någon sekretessbrytande bestämmelse som specifikt tar sikte på den situationen att en myndighet utkontrakterar sin it-drift till en privat tjänsteleverantör. Som nämns ovan innehåller OSL däremot en mera generell sekretessbrytande bestämmelse – s.k. nödvändigt utlämnande – i 10 kap. 2 §. Bestämmelsen innebär att sekretess inte hindrar att en myndighet lämnar ut en uppgift om det är nödvändigt för att myndigheten ska kunna fullgöra sin

verksamhet. Frågan är om den myndighet som står i begrepp att utkontraktera it-drift kan använda sig av denna bestämmelse.

I lagmotiven till motsvarande bestämmelse i 1980 års sekretesslag sägs att den ska tillämpas restriktivt. Det är inte tillräckligt att myndighetens arbete blir mer effektivt (prop. 1979/80:2 Del A s. 465 och 494). JO har i flera avgöranden haft anledning att resonera kring bestämmelsens räckvidd och har i dessa gett uttryck för den uppfattningen att bestämmelsen tar sikte på situationer av undantagskaraktär (se t.ex. JO 1982/83:JO1 s. 238, dnr 149-1980, JO 1984/85: JO1 s. 265, dnr 2616-1983 och JO:s beslut den 9 september 2014, dnr 3032-2011).

Synpunkten att ett röjande av uppgifter i samband med sådan utkontraktering som sker i syfte att dra nytta av utförarens expertkompetens eller tekniska utrustning i särskilda fall kan anses utgöra ett sådant nödvändigt utlämnande som kan ske trots sekretess har framförts av eSam. Som exempel på sådan utkontraktering har nämnts it-support, storskalig skanning av dokument, it-drift och e-arkivering (eSam, *Outsourcing – en vägledning om sekretess och persondataskydd*, 2016, s. 27 f.). Denna tolkning synes göras utifrån ett uttalande i lagmotiven till 1980 års sekretesslag om att det i särskilda fall kan vara nödvändigt för en tjänsteman att vända sig till en utomstående expert och upplysa denne om hemliga omständigheter (prop. 1979/80:2 Del A, s. 122). Detta resonemang fördes även i E-delegationens slutbetänkande, vilket möttes av invändningar av några remissinstanser som ansåg att delegationens tolkning var mer vidsträckt än vad uttalanden från JO och uttalanden i lagmotiven gav stöd för (se SOU 2015:66 s. 48 f. och bl.a. Livsmedelsverkets remissyttrande, den 14 december 2015, dnr 2015/07920 och Transportstyrelsens remissyttrande, den 14 december 2015, dnr TSG 2015-1422).

Digitaliseringsrättsutredningen tog upp denna fråga i sitt betänkande och gjorde bedömningen att den av eSam och E-delegationen förordade tolkningen framstår som långtgående (SOU 2018:25 s. 345). Enligt utredningen tyder bestämmelsens ordalydelse, i ljuset av uttalandena i lagmotiven om att bestämmelsen ska tillämpas restriktivt, på att den är tänkt att tillämpas i situationer då det inte finns någon annan realistisk utväg för myndigheten att fullgöra en arbetsuppgift.

Vi gör ingen annan bedömning i denna fråga än Digitaliseringsrättsutredningen. Vår slutsats blir därmed att bestämmelsen i 10 kap. 2 § OSL inte kan användas när en myndighet utkontrakterar sin it-drift annat än i vissa undantagsfall.

Utlämnande med förbehåll

Det finns i 10 kap. 14 § OSL en bestämmelse som innebär att myndigheter i vissa fall kan lämna ut sekretessbelagda uppgifter med förbehåll. Endast uppgifter som är sekretessbelagda enligt en sekretessbestämmelse som har ett skaderekvisit omfattas av bestämmelsen tillämpningsområde. Uppgifter som omfattas av absolut sekretess kan följaktligen inte lämnas ut med förbehåll.

Ett utlämnande av uppgifterna kan ske under förutsättning att den risk för skada, men eller annan olägenhet som hindrar att uppgifterna lämnas till den enskilde kan undanröjas genom förbehållet. Ett förbehåll kan t.ex. avse ett förbud mot att lämna uppgifterna vidare eller utnyttja dem. Förbehållet medför att tystnadsplikt uppkommer för den som tagit emot uppgifterna som inskränker rätten att meddela och offentliggöra uppgifterna (meddelarfrihet). Ett röjande av uppgifterna kan medföra straffansvar för brott mot tystnadsplikt.

I bestämmelsen uppställs avsevärda begränsningar kring hur och när ett förbehåll får ställas upp. För det första får ett förbehåll inte meddelas i förväg utan ska föregås av en prövning i varje särskilt fall och avse konkreta uppgifter. För det andra ska ett förbehåll meddelas som ett formligt beslut, dvs. det ska dokumenteras och innehålla en överklagandehänvisning. För det tredje ska uppgiftsutlämnandet ske till en utpekad fysisk person. Det går alltså inte att i avtal reglera generella förbehåll (se bl.a. JO 1992/93:JO1 s. 197, dnr 145-90, JO 1994/95:JO1 s. 574, dnr 2079-1993 och JO 2009/10: JO1 s. 194, dnr 4150-2007).

Mot den nu tecknade bakgrunden bedömer vi att bestämmelsen om utlämnande med förbehåll inte kan användas vid utkontraktering av it-drift annat än i vissa undantagsfall.

10.2.3 Behovet av författningsändringar

Det nu anförda innebär att det finns begränsade rättsliga förutsättningar för en myndighet – om vi nu utgår ifrån att uppgifterna är sekretessreglerade – att utkontraktera sin it-drift i mer varaktiga former med mindre än att myndigheten efter en övergripande skadeprövning funnit att uppgifterna kan lämnas ut. Det står klart att en sådan prövning i en del fall kan vara svår att göra. Man kan exempelvis tänka sig fall där det är svårt eller omöjligt att avskilja uppgifter som omfattas av svag sekretess från uppgifter som omfattas av starkare sekretess.

Ytterligare en komplikation som bör betonas är att det – givet vår tolkning av röjandebegreppet – finns begränsade möjligheter för myndigheterna att utkontraktera it-drift om utkontrakteringen omfattar uppgifter som träffas av absolut sekretess. Någon skadeprövning kan inte göras i de fallen. Ett utlämnande av uppgifter med stöd av 10 kap. 2 § OSL torde endast kunna ske i undantagsfall.

Som vi redan konstaterat är utkontraktering av it-drift för många myndigheter en förutsättning för att de ska kunna driva sin verksamhet på ett effektivt och ändamålsenligt sätt. En förutsättning för att myndigheter som är i behov av att utkontraktera sin it-drift också ska göra det är det finns ett regelverk som medger det. Den nuvarande regleringen kan inte betraktas som tillräcklig i detta avseende.

Vår bedömning är att det behövs en reglering som i större utsträckning än den nuvarande ger ett uttryckligt stöd för att lämna ut uppgifter inom ramen för en utkontraktering av it-drift. Det är vår uppfattning att ett sådant behov kan tillgodoses med en sekretessbrytande bestämmelse.

10.2.4 En sekretessbrytande bestämmelse bör införas

En sekretessbrytande bestämmelse bör inte införas med mindre än att myndighetens behov att lämna ut uppgifter väger tyngre än de intressen som sekretessen avser att skydda. Det är vår övergripande bedömning att myndigheternas behov av att utkontraktera it-drift väger tyngst i detta sammanhang. Vi föreslår därför att en sekretessbrytande bestämmelse som tar sikte på utkontraktering av it-drift införs.

10.3 Den sekretessbrytande bestämmelsens utformning

Utredningens förslag: Den sekretessbrytande bestämmelsen ska placeras i 10 kap. offentlighets- och sekretesslagen (2009:400) och ta sikte på fall då uppgifter lämnas ut till privata tjänsteleverantör eller andra myndigheter som har i uppdrag att utföra endast teknisk bearbetning eller teknisk lagring för den utlämnande myndighetens räkning (utkontraktering). Ett utlämnande ska inte ske om det intresse som sekretessen ska skydda har företräde framför intresset av utkontraktering.

Utredningens bedömning: Bestämmelsen ska inte villkoras med något lämplighetsrekvisit.

Det finns inte skäl att från bestämmelsens tillämpningsområde undanta vissa sekretessbestämmelser eller uppgifter som är säkerhetsskyddsklassificerade enligt säkerhetsskyddslagstiftningen.

10.3.1 Tillämpningsområdet

Avgränsning till it-drift är inte lämplig

Den fråga som inställer sig inledningsvis är om den sekretessbrytande bestämmelsen ska träffa utkontraktering av *it-drift*, eller om det finns skäl att göra dess tillämpningsområde smalare.

Det förstnämnda alternativet har den fördelen att det eliminerar risken för att en viss form av utkontraktering – utan att det framstår som sakligt motiverat – hamnar utanför den sekretessbrytande bestämmelsens tillämpningsområde.

Som följer av avsnitt 2.2.3 är det inte alltid givet vilken verksamhet som kan sägas falla in under begreppet it-drift och vilken verksamhet som faller utanför.

En sekretessbrytande bestämmelse innebär att sekretess som annars skulle ha skyddat vissa uppgifter inte längre ska gälla i en viss situation. För att inte tillämpningen av en sådan bestämmelse ska riskera att bli alltför varierad och oförutsägbar bör dess tillämpningsområde utformas på ett så tydligt sätt som möjligt. Den vaghet som

ligger i uttrycket it-drift innebär att man kan ifrågasätta om det är lämpligt att låta den sekretessbrytande bestämmelsen ta sikte på utkontraktering av it-drift.

Bestämmelsen bör avgränsas till teknisk bearbetning eller teknisk lagring

Som vi redogjort för ovan (avsnitt 9.8.2) förekommer formuleringen teknisk bearbetning eller teknisk lagring i TF och OSL. Uttrycket teknisk lagring eller teknisk bearbetning är därmed sedan länge inarbetat. Därtill kommer att uttrycket används i tystnadspliktslagen som har ett nära samband med de frågor som behandlas i detta betänkande. Även om uttrycket inte kan sägas vara alldeles entydigt framstår det som mer tydligt än uttrycket it-drift. Det nu nämnda talar för att den sekretessbrytande bestämmelsen bör avgränsas till att endast ta sikte på utkontraktering av teknisk bearbetning eller teknisk lagring av uppgifter.

Härutöver bör framhållas att vi – genom att låta den sekretessbrytande bestämmelsen ta sikte på utkontraktering av teknisk bearbetning eller teknisk lagring av uppgifter – undviker att introducera ett nytt begrepp med otydligt innehåll på ett rättsområde som redan nu måste betecknas som komplext.

Med hänsyn till det ovan anförda bör därför den sekretessbrytande bestämmelsen utformas på det sättet att den endast tar sikte på utkontraktering av teknisk bearbetning och teknisk lagring av uppgifter.

Bestämmelsen avser enbart teknisk bearbetning eller teknisk lagring

Avgränsningen till tjänster eller funktioner som enbart innebär teknisk bearbetning eller teknisk lagring för myndighetens räkning innebär att tjänster som visserligen innefattar moment av teknisk bearbetning eller teknisk lagring, men som inte enbart avser sådan bearbetning eller lagring inte omfattas av bestämmelsen.

Utkontraktering av arbetsuppgifter som är hänförliga till vård- och omsorgssektorns behandling av personuppgifter vid t.ex. journalföring, bedömning av röntgenbilder eller patientrådgivning, ut-

gör exempel på utkontraktering som faller utanför tillämpningsområdet.

Bestämmelsen avser hantering som sker för myndighetens räkning

Det ska betonas att den avgränsning av tillämpningsområdet som nu gjorts innebär att bestämmelsen endast träffar den hantering av uppgifter som sker *för myndighetens räkning*. Det följer av den föreslagna bestämmelsens ordalydelse att sådan hantering av uppgifter som en privat tjänsteleverantör utför för ändamål kopplade till den egna verksamheten faller utanför tillämpningsområdet. Tjänsteleverantörens hantering av myndighetens uppgifter för utveckling av egna produkter och tjänster kan nämnas som exempel. Det kan i sammanhanget tilläggas att ett personuppgiftsbiträdes behandling av personuppgifter för egna ändamål inte är tillåten enligt dataskyddsförordningen (se avsnitt 7.3.6). I praktiken innebär detta att myndigheten inte kan godta sådana avtalsvillkor som medger att tjänsteleverantören använder uppgifterna för egen räkning om den sekretessbrytande bestämmelsen ska tillämpas för utlämnandet.

Den föreslagna regleringen medför inte några nya hinder för utkontraktering avseende sådana arbetsuppgifter som faller utanför tillämpningsområdet eller sådan hantering som sker för tjänsteleverantörens egen räkning. Sådana utlämnanden får ske med stöd av de regler som gäller i dag, dvs. utlämnande efter skadeprövning eller med stöd av en sekretessbrytande bestämmelse.

10.3.2 Bestämmelsen bör även ta sikte på utkontraktering myndigheter emellan och placeras i offentlighets- och sekretesslagen

I detta delbetänkande har vi fokuserat på sådana fall då myndigheter uppdrar åt en privat tjänsteleverantör att helt eller delvis hantera myndighetens it-drift. I våra direktiv beskrivs detta som utkontraktering av it-drift.

En fråga vi har övervägt är om den sekretessbrytande bestämmelsen ska utformas på det sättet att den endast tar sikte på det som i direktiven beskrivs som utkontraktering av it-drift.

Det förekommer även att myndigheter får i uppdrag att helt eller delvis hantera it-drift åt en annan myndighet. I direktiven beskrivs denna verksamhet som samordnad it-drift.

Vi kan inte se att det finns några bärande skäl för att begränsa den sekretessbrytande bestämmelsen till att endast träffa det som i direktiven benämns utkontraktering av it-drift. Bestämmelsen bör därmed även ta sikte på det fallet att en myndighet på uppdrag av en annan myndighet tekniskt bearbetar eller lagrar uppgifter. Som vi ser det påverkar inte detta våra möjligheter att i slutbetänkandet återkomma med ytterligare författningsförslag som rör samordnad it-drift. Den sekretessbrytande bestämmelse bör därför ta sikte på såväl utkontraktering av it-drift till privata tjänsteleverantörer som utkontraktering av it-drift myndigheter emellan.

Denna bestämmelse bör lämpligen placeras i 10 kap. OSL som innehåller sekretessbrytande bestämmelser och bestämmelser om undantag från sekretess.

10.3.3 En villkorslös bestämmelse?

Som utgångspunkt gäller att det i första hand är lagstiftaren som har till uppgift att fullt ut ansvara för de avvägningar som måste göras mellan det intresse som föranlett den sekretessbrytande bestämmelsen och de intressen som sekretessen avser skydda och andra hänsynstaganden. I linje med detta uppställs särskilda villkor endast i ett fåtal sekretessbrytande bestämmelser (se t.ex. 10 kap. 27 § och 15 kap. 3 a § OSL).

Det står klart att den främsta fördelen med att inte införa några särskilda villkor för den sekretessbrytande bestämmelsen är att det skulle skapa en tydlig reglering i OSL. Det skulle därmed stå klart att sekretess inte hindrar en myndighet från att lämna ut uppgifter till en tjänsteleverantör som har i uppdrag att endast tekniskt bearbeta eller tekniskt lagra uppgifterna för myndighetens räkning. Fördelarna med en sådan ordning måste dock vägas mot eventuella nackdelar.

10.3.4 En intresseavvägning

Uppgifter som omfattas av sekretess kan vara mycket känsliga oavsett om det är fråga om sekretess till skydd för enskilda eller till skydd för det allmänna, beroende på omfattningen av och karaktären hos uppgifterna. Det är samtidigt så att den sekretessbrytande bestämmelse som vi föreslår ska tillämpas av samtliga myndigheter i många olika situationer. De förhållanden under vilka den sekretessbrytande bestämmelsen ska tillämpas är så varierande att det framstår som vanskligt att slå fast att intresset av utkontraktering i alla tänkbara situationer väger tyngre än de intressen som sekretessen avser att skydda. Vi menar därför att det – trots den under föregående rubrik beskrivna utgångspunkten – finns ett behov av att skapa en reglering som möjliggör hänsynstagande till sekretessintresset i det enskilda fallet där det framstår som nödvändigt. En sådan reglering skulle kunna utformas på det sättet att den sekretessbrytande bestämmelsen förses med det villkoret att den myndighet som avser att utkontraktera it-drift åläggs att innan ett beslut fattas göra en avvägning mellan intresset av en utkontraktering och de intressen som sekretessen avser att skydda.

Det är i detta sammanhang värt att framhålla att ett krav på en intresseavvägning skulle – till skillnad från en villkorslös sekretessbrytande bestämmelse – tvinga myndigheterna att i sina överväganden inför ett beslut om utkontraktering av it-drift beakta sekretessintresset, vilket kan ha ett värde i sig.

Av betydelse i sammanhanget är också att ett krav på intresseavvägning ytterst innebär att ansvar för brott mot tystnadsplikt enligt 20 kap. 3 § brottsbalken kan komma i fråga i de fall utkontraktering skett trots att sekretessintresset vägde tyngre.

En invändning som kan riktas mot att införa ett krav på en intresseavvägning är att det i viss utsträckning förtar poängen med en sekretessbrytande bestämmelse. Myndigheterna har redan i dag i vissa fall en möjlighet att utkontraktera it-drift efter en skadeprövning. Frågan är om det innebär någon reell förenkling för myndigheterna att göra en intresseavvägning i stället för en skadeprövning.

Det går inte att bortse ifrån att skadeprövningen i första hand tar sikte på fall där det finns förutsättningar för myndigheterna att göra en mer detaljerad bedömning, t.ex. när någon från allmänheten begär ut en handling ur en akt med sekretessreglerade uppgifter. Som vi

nämner ovan torde det i många fall vara förenat med svårigheter att göra en skadeprövning i samband med utkontraktering av it-drift, eftersom det i sådana fall är fråga om stora uppgiftsmängder där uppgifter kan vara reglerade av olika bestämmelser om sekretess. En intresseavvägning kan skapa förutsättningar för myndigheten att göra en mer övergripande prövning och skulle därmed innebära en förenkling för myndigheterna. Det bör också framhållas att även om det införs ett krav på en intresseavvägning, det ändå skulle innebära en utvidgning av möjligheten för myndigheterna att utkontraktera it-drift i jämförelse med vad som gäller i dag.

Vid en samlad bedömning anser vi att övervägande skäl talar för den sekretessbrytande bestämmelsen bör förses med det villkoret att den myndighet som avser att utkontraktera it-drift ska göra en avvägning mellan intresset av utkontraktering och det intresse som sekretessen avser att skydda innan ett beslut fattas.

10.3.5 Närmare om intresseavvägningen

Ett villkor för att utlämnande ska få ske bör således vara att de skäl som talar för att det intresse som sekretessen ska skydda har företräde framför intresset av att uppgiften lämnas ut. Det är viktigt att poängtera att endast sekretesshänsyn kan tas vid denna bedömning. Det finns alltså inte utrymme att inom ramen för intresseavvägningen beakta andra hänsyn som t.ex. om det från mera allmänna utgångspunkter är lämpligt att utkontraktering sker.

Vilka intressen som föranlett sekretessen, med vilken styrka som sekretessen är reglerad liksom uppgifternas art och omfattning är faktorer av betydelse. Det kan också – enligt vår bedömning – vara av betydelse vilken sekretess eller tystnadsplikt som gäller hos mottagaren av uppgifterna, och vilken styrka den sekretessen eller tystnadsplikten har. Vi menar att det finns fog för uppfattningen att det i detta sammanhang kan ha betydelse om det är fråga om en straffsanktionerad tystnadsplikt enligt OSL eller annan lagstiftning, eller en tystnadsplikt som följer av avtal (jfr JO:s beslut den 9 september 2014 /dnr 3032-2011/). Det förhållandet att det – med anledning av kravet på dubbel straffbarhet i 2 kap. brottsbalken – inte alltid kommer att vara möjligt att lagföra vissa utländska tjänsteleverantörer för

brott mot tystnadsplikt om de röjer uppgifter i strid med tystnadspliktslagen kan alltså vara av betydelse.

Hänsyn till möjligheten att lagföra ett brott mot tystnadsplikt utifrån kravet på dubbel straffbarhet kan emellertid bara tas i förhållande till länder utanför EU, eftersom sådana hänsyn annars skulle kunna stå i strid med EU-rättens likabehandlingsprincip.

Dataskyddsregelverket innebär i viss utsträckning en tystnadsplikt för personuppgifter som också kan vara relevant att ta i beaktande i bedömningen. Detsamma gäller förekomsten av avtalsreglerad tystnadsplikt samt förekomsten av tekniska säkerhetsåtgärder, som t.ex. kryptering, som gör det svårare för någon obehörig att ta del av uppgifterna.

10.3.6 Bestämmelsen bör inte villkoras med något lämplighetsrekvisit

Digitaliseringsrättsutredningens förslag

Digitaliseringsrättsutredningen föreslog att det skulle införas en sekretessbrytande bestämmelse i 10 kap. 2 a § OSL som – i likhet med vad vi föreslår – tar sikte på uppgiftsutlämnande till tjänsteleverantörer och andra myndigheter som utför uppdrag för enbart teknisk bearbetning eller teknisk lagring för den utlämnande myndighetens räkning.

För att ett utlämnande ska kunna ske enligt Digitaliseringsrättsutredningen förslag uppställs två villkor. Uppgifter ska inte lämnas ut om övervägande skäl talar för att det intresse som sekretessen ska skydda har företräde framför intresset av att uppgiften lämnas ut eller om det av andra skäl är olämpligt.

När det gäller det föreslagna lämplighetsrekvisitet nämnde Digitaliseringsrättsutredningen att utkontrakteringar som innebär att flera myndigheters system och information samlas i samma lagringsmedium kan framstå som olämpliga eftersom de kan innebära en ökad riskexponering för känsliga uppgifter. Även en tänkt geografisk lokalisering av uppgifterna kan, enligt den bedömning som utredningen gjorde, medföra att en utkontraktering som avser vissa känsliga uppgifter till tjänsteleverantören bedöms vara olämplig.

Våra överväganden

Vi har övervägt frågan om det finns behov av ett lämplighetsrekvisit liknande det som Digitaliseringsrättsutredningen föreslog. Det bör i detta sammanhang – vilket också Digitaliseringsrättsutredningen varit inne på – beaktas att ett sådant villkor bör ta sikte på andra intressekonflikter än den som står mellan intresset av utkontraktering och de sekretessintressen som sekretessen avser att skydda. Snarare skulle ett sådant villkor ta sikte på frågan om en utkontraktering framstår som lämplig från mera allmänna utgångspunkter. Det står klart att ett sådant villkor – som alltså avser annat än rena sekretesshänsyn – inte bör placerar i OSL. Skulle det finnas ett behov av ett lämplighetsrekvisit bör det antingen arbetas in i någon befintlig reglering eller införas i någon ny lag.

Det kan konstateras att den sekretessbrytande bestämmelse vi föreslår inte innebär att myndigheterna måste utkontraktera it-drift. Andra alternativ står alltjämt till buds om en myndighet av något skäl skulle bedöma att en utkontraktering vore mindre lämplig.

OSL är inte det enda regelverk som en myndighet har att beakta vid bedömningen av om en utkontraktering av it-drift är möjlig. Även om det inte uppställs något hinder i OSL kan alltså annan reglering hindra en utkontraktering. Man kan t.ex. tänka sig att en utkontraktering innebär en – enligt dataskyddsförordningen – otillåten överföring av personuppgifter till tredje land. Vidare kan man tänkta sig fall då en utkontraktering står i konflikt med säkerhetsskyddsregleringen eller informationssäkerhetsregleringen. Vi har svårt att tänka oss något fall där en utkontraktering måste betraktas som olämplig utan att den står i strid med något av dessa regelverk. Den nuvarande lagstiftningen uppställer således krav på att den myndighet som avser att utkontraktera it-drift – vid sidan om de bedömningar som är nödvändiga att göra enligt OSL – ska göra mera allmänna lämplighetsbedömningar.

En annan sak är att vår kartläggning visar att i synnerhet informationssäkerhetsregleringen inte efterlevs fullt ut bland myndigheterna. Det framgår av enkätresultaten att bristande informationsklassificering och bristande kompetens är de största hindren mot säker it-drift. Sårbarheter och brister i myndigheternas informationssäkerhet kan leda till kostnader i de fall de leder till it-incidenter. Det kan handla om störningar av tillgängligheten till information

och funktioner, manipulation eller stöld av känslig information. Samtidigt medför ofta åtgärder som syftar till att förbättra informationssäkerheten direkta eller indirekta kostnader. Sammantaget visar detta, enligt vår uppfattning, på brister i efterlevnaden av befintliga regelverk, snarare än på bristande reglering. Bristerna i efterlevnad avhjälps inte genom ett lämplighetsrekvisit, utan beror snarare bl.a. på avsaknad av tillsyn över efterlevnaden av informationssäkerhetsregleringen. Det är därmed vår slutsats att det saknas behov av att införa något lämplighetsrekvisit.

10.3.7 Undantag för försvarssekretess eller någon annan sekretessbrytande bestämmelse?

En särskild fråga som väckts under arbetets gång är om det finns skäl att från den sekretessbrytande bestämmelsens tillämpningsområde undanta den s.k. försvarssekretessen i 15 kap. 2 § OSL. Som skäl för en sådan ordning skulle kunna anföras att de uppgifter som försvarssekretessen tar sikte på är så skyddsvärda att de bör bli föremål för utkontraktering i så liten utsträckning som möjligt eller kanske inte alls.

Redan i dag finns en möjlighet att efter en skadeprövning utkontraktera uppgifter som omfattas av försvarssekretess. Skillnaden mellan en skadeprövning och den intresseavvägning som ska göras enligt den bestämmelse som vi föreslår ligger i att det i det senare fallet finns uttryckligt stöd för att göra en övergripande bedömning. Det skulle därför kunna hävdas att den bestämmelse vi föreslår innebär vidgade möjligheter att utkontraktera it-drift som rör uppgifter som omfattas av försvarssekretess och att ett undantag mot den bakgrunden är nödvändigt. Det är dock oundvikligt att även den skadeprövning som föregår en utkontraktering görs på ett övergripande plan. Det kan mot den bakgrunden ifrågasättas om skillnaden är särskilt stor i praktiken.

Det finns skäl att framhålla att försvarssekretessen inte intar någon särställning i OSL. De särskilda hänsyn som bör tillmätas uppgifter som rör säkerhetskänslig verksamhet och som därför omfattas av OSL tillgodoses inom ramen för säkerhetsskyddslagstiftningen. Det är vidare så att om vi skulle införa en ordning som innebar att försvarssekretessen undantogs, frågan skulle uppkomma om inte även andra sekretessbestämmelser skulle undantas. Detta

gäller särskilt sådana sekretessbestämmelser som till skillnad från försvarssekretessen har omvända skaderekvisit, dvs. där det finns en presumtion för sekretess, eller bestämmelser om absolut sekretess.

Det är mot denna bakgrund vår bedömning att det inte finns skäl att undanta försvarssekretessen från den sekretessbrytande bestämmelsens tillämpningsområde.

De skäl som nu anförts gör sig även gällande när det gäller övriga sekretessbestämmelser i OSL. Vi bedömer därför att det inte finns anledning att undanta någon sekretessbestämmelse från den sekretessbrytande bestämmelsens tillämpningsområde.

10.3.8 Säkerhetsskyddsklassificerade uppgifter

Som vi redovisat i avsnitt 6.2.2 ska med *säkerhetsskyddsklassificerade uppgifter* förstås uppgifter som rör säkerhetskänslig verksamhet och som därför omfattas av sekretess enligt OSL eller som skulle ha omfattats av sekretess enligt den lagen, om den hade varit tillämplig (1 kap. 2 § andra stycket säkerhetsskyddslagen /2018:585/).[2] Det finns alltså en koppling mellan säkerhetsskyddslagstiftningen och OSL. Frågan är om den sekretessbrytande bestämmelse vi föreslår på något sätt har betydelse för frågan om en uppgift ska betraktas som säkerhetsskyddsklassificerad. Det är vår utgångspunkt att säkerhetsskyddsklassificerade uppgifter bör undantas från den sekretessbrytande bestämmelsens tillämpningsområde om den skulle innebära att skyddet enligt säkerhetsskyddslagstiftningen för dessa uppgifter försämras.

Frågan är vad som avses med formuleringen uppgifter *som omfattas av sekretess enligt OSL*. I lagmotiven till säkerhetsskyddslagen talas på flera ställen om sekretessbelagda uppgifter (prop. 2017/18:89 s. 49 ff.). Även i lagmotiven till 1996 års säkerhetsskyddslag – som föregick den nuvarande lagen – talas om sekretessbelagda uppgifter (se prop. 1995/96:129 bl.a. s. 41). I det av Utredningen om säkerhetsskyddslagen avlämnade betänkandet (SOU 2015:25) *En ny säkerhetsskyddslag* talas däremot om *uppgifternas natur* (s. 288 f.). Inte någonstans i betänkandet förmedlas den uppfattningen att uppgifterna i fråga måste vara sekretessbelagda.

[2] För enkelhets skulle talar vi i det följande om uppgifter som omfattas av OSL.

Skrivningarna i lagmotiven skulle kunna tolkas som att det krävs att en uppgift är sekretessbelagd enligt OSL för att den ska kunna betraktas som säkerhetsskyddsklassificerad.

Uttrycket *sekretessbelagda uppgifter* definieras i 3kap. 1 § OSL som en uppgift för vilken sekretess gäller i ett enskilt fall. Man kan alltså endast i det enskilda fallet – efter en konkret utlämnandeprövning – veta om en uppgift är sekretessbelagd. En tolkning av uttrycket säkerhetsskyddsklassificerad i enlighet med lagmotiven leder därmed dels till att säkerhetsskyddslagens tillämpningsområde blir mycket begränsat, dels till att uppgifter som lämnats ut med stöd av en sekretessbrytande bestämmelse eller efter en skadeprövning inte kan betraktas som säkerhetsskyddsklassificerade eftersom de i så fall inte kan vara sekretessbelagda.

Det står enligt vår bedömning klart att formuleringen *omfattas av sekretess enligt OSL* i 1 kap. 2 § andra stycket säkerhetsskyddslagen inte rimligen kan uppfattas som att det krävs att uppgifterna är sekretessbelagda.

Enligt den tolkning vi gör är det däremot ett nödvändigt men inte tillräckligt villkor att en uppgift är sekretessreglerad enligt OSL för att den ska kunna betraktas som säkerhetsskyddsklassificerad. Härutöver krävs att uppgiften rör säkerhetskänslig verksamhet.

Sekretessreglerad uppgift definieras som en uppgift för vilken det finns en bestämmelse om sekretess (3 kap. 1 § OSL). En uppgift som är sekretessreglerad upphör inte att vara det endast av det skälet att den träffas av en sekretessbrytande bestämmelse. Detta innebär i sin tur att den sekretessbrytande bestämmelse vi föreslår inte kommer att ha någon inverkan på frågan om uppgifterna ska betraktas som säkerhetsklassificerade eller inte, även om de träffas av den sekretessbrytande bestämmelsen. Vi kan inte heller se att uppgifterna på någon annan grund inte längre skulle kunna betraktas som säkerhetsskyddsklassificerade med anledning av den bestämmelse vi föreslår. Vår slutsats är därmed att det inte finns någon anledning att undanta uppgifter som är säkerhetsskyddsklassificerade från den sekretessbrytande bestämmelsens tillämpningsområde.

11 En inskränkt meddelarfrihet

Utredningens förslag: Den i tryckfrihetsförordningen och yttrandefrihetsgrundlagen föreskrivna meddelarfriheten bör inskränkas för den krets av personer som träffas av lagen (2020:914) om tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter.

11.1 Tystnadsplikten

Regeringens avsikt är att den tystnadsplikt som åläggs tjänsteleverantörerna enligt lagen (2020:914) om tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter (tystnadspliktslagen) så långt som möjligt ska överensstämma med den tystnadsplikt som gäller enligt offentlighets- och sekretesslagen (2009:400) vid teknisk bearbetning och teknisk lagring hos det allmänna (prop. 2019/20:201 s. 18 och s. 24). Det innebär att tystnadsplikt gäller hos tjänsteleverantören för en uppgift som hos en myndighet skulle ha omfattats av sekretess till skydd för allmänna intressen enligt 11 kap. 4 a § OSL eller till skydd för enskilds personliga och ekonomiska förhållanden enligt 40 kap. 5 § OSL.

11.2 Meddelarfrihet

Rätten att meddela och offentliggöra uppgifter (meddelarfrihet) som framgår av 1 kap. 1 § andra stycket och 7 § första stycket tryckfrihetsförordningen (TF) samt 1 kap. 1 § första stycket och 10 § första stycket yttrandefrihetsgrundlagen (YGL) innebär en rätt att lämna uppgifter, även sådana som omfattas av sekretess eller tystnadsplikt, för offentliggörande i tryckt skrift, program eller genom

tekniska upptagningar. Tanken med denna frihet är att samhällsdebatten inte ska berövas uppgifter som är mycket betydelsefulla från allmän synpunkt av den anledningen att uppgifterna är sekretessbelagda av hänsyn till ett sekretessintresse som just i det aktuella sammanhanget väger mindre tungt. Rätten att meddela eller offentliggöra uppgifter som följer av TF och YGL har som utgångspunkt företräde framför tystnadsplikten.

Regeringen har uttalat att som grundprincip gäller att stor återhållsamhet bör iakttas vid prövningen av om undantag från meddelarfrihet ska göras i ett enskilt fall. Den berörda sekretessbestämmelsens konstruktion kan ge viss vägledning. När det är fråga om bestämmelser om absolut sekretess kan det finnas större anledning att överväga undantag från meddelarfriheten än i andra fall. Det bör också beaktas om uppgiften har lämnats av en enskild i en förtroendesituation eller om uppgiften hänför sig till myndighetsutövning. I det förra fallet bör rätten att meddela och offentliggöra uppgifter normalt sett inskränkas, medan denna rätt normalt sett bör ha företräde när det är fråga om uppgifter som hänför sig till myndighetsutövning (se prop. 1979/80:2 del A s. 104 f.).

Offentliga funktionärers tystnadsplikt för uppgift om enskilds personliga eller ekonomiska förhållanden som hanteras i verksamhet för endast teknisk bearbetning eller teknisk lagring inskränker meddelarfriheten (40 kap. 5 och 8 §§ OSL). Meddelarfriheten är även inskränkt för uppgift som är sekretessreglerad av hänsyn till ett allmänt intresse enligt en bestämmelse som har företräde framför meddelarfriheten och som hanteras i verksamhet för endast teknisk bearbetning eller teknisk lagring för en annan myndighets räkning. Det gäller dock inte om en annan primär sekretessbestämmelse till skydd för samma intresse, som inte har företräde framför meddelarfriheten, är tillämplig hos den uppgiftsmottagande myndigheten (jfr 11 kap. 4 a och 8 §§ OSL).

11.3 Meddelarfriheten bör inskränkas för den krets av personer som träffas av tystnadspliktslagen

Det ovan anförda innebär att det – vid samordnad it-drift, dvs. utkontraktering av it-drift myndigheter emellan – inte finns någon rätt för de offentliga funktionärerna hos den uppgiftsmottagande myn-

digheten att meddela och offentliggöra uppgifter som omfattas av sekretess till skydd för enskilds personliga eller ekonomiska förhållanden för offentliggörande i tryckt skrift, program eller genom tekniska upptagningar. När det gäller uppgifter som är sekretessreglerade av hänsyn till ett allmänt intresse följer som sagt av 11 kap. 4 a och 8 §§ OSL att meddelarfriheten i vissa situationer är inskränkt och i andra inte.

För den krets av personer som träffas av tystnadspliktslagen föreskrivs däremot ingen inskränkning i meddelarfriheten. Digitaliseringsrättsutredningen analyserade inte frågan närmare. Regeringen ansåg inte att det fanns skäl att föreslå en inskränkning av meddelarfriheten men uteslöt inte att det vid behov kunde finnas anledning att på nytt överväga frågan (prop. 2019/20:201 s. 20).

Det kan ifrågasättas om det är en rimlig ordning att den tystnadsplikt som gäller för de offentliga funktionärerna har företräde framför meddelarfriheten samtidigt som meddelarfriheten har företräde framför den tystnadsplikt som följer av tystnadspliktslagen. Det är vidare så att den sekretessbrytande bestämmelse vi föreslår innebär en utvidgning av möjligheten att utkontraktera it-drift till privata tjänsteleverantörer vilket – enligt vår bedömning – utgör ytterligare ett argument för att inskränka meddelarfriheten.

Vid en sammantagen bedömning bedömer vi att meddelarfriheten bör inskränkas för den krets av personer som träffas av tystnadspliktslagen.

12 Konsekvensutredning

12.1 Inledning

Vi ska enligt våra utredningsdirektiv bedöma förslagens konsekvenser i enlighet med kommittéförordningen (1998:1474) och förordningen (2007:1244) om konsekvensutredning vid regelgivning.

Vi redovisar två förslag i detta delbetänkande. Det första förslaget avser införande av en sekretessbrytande bestämmelse i offentlighets- och sekretesslagen (2009:400) (OSL) om utkontraktering av teknisk bearbetning och teknisk lagring av uppgifter. Det andra förslaget avser en inskränkt meddelarfrihet.

Konsekvensanalysen utgår från de krav som ställs i kommittéförordningen och förordningen om konsekvensutredning vid regelgivning. Vi analyserar inte konsekvenser av våra slutsatser om röjande eller överföring till tredje land.

12.2 Nuläge och problembild

Som vi beskriver i detta delbetänkande är utkontraktering av it-drift en viktig förutsättning för statliga myndigheter, kommuner och regioner att kunna bedriva sin verksamhet på ett effektivt och ändamålsenligt sätt. Vår kartläggning visar att utkontraktering av it-drift och användning av molntjänster är ett vanligt sätt för statliga myndigheter att hantera sin it-drift. Detsamma gäller för kommuner och regioner.

En utkontraktering av it-drift handlar i grund och botten om att en statlig myndighet, kommun eller region uppdrar åt en privat tjänsteleverantör att hantera hela eller delar av it-driften.

Utkontraktering av it-drift kan innebära fördelar som effektivisering, besparingar och ökad säkerhet. Utkontraktering kan också föra med sig nackdelar som leverantörsberoende och säkerhetsut-

maningar. Kravställningsarbetet som görs i samband med upphandling av it-drift är därför viktigt, och lämpliga avvägningar behöver göras utifrån verksamhetens krav och förutsättningar. Vid anlitande av en privat tjänsteleverantör av it-driftstjänster måste de krav som ställs på informationssäkerhet, säkerhetsskydd, sekretess och dataskydd alltid upprätthållas.

Beslut om utkontraktering som grundar sig på ett bristande informationssäkerhetsarbete kan innebära säkerhetsrisker. Vår kartläggning visar att ungefär hälften av de statliga myndigheter som besvarat enkäten behöver etablera och utveckla ett systematiskt informationssäkerhetsarbete i sin verksamhet. Informationsklassning ingår här som en viktig del. Även kommunerna och regionerna behöver stärka sitt systematiska informationssäkerhetsarbete. Detta är en förutsättning för att kunna göra en lämplig avvägning mellan säkerhet och kostnadseffektivitet vid beslut om utkontraktering av it-drift.

Bland statliga myndigheter och i kommunsektorn råder det i dag en viss osäkerhet i fråga om de rättsliga förutsättningarna för utkontraktering till privata tjänsteleverantörer. Det gäller främst tolkningen av när en uppgift ska anses röjd enligt OSL.

En förutsättning för att statliga myndigheter, kommuner och regioner som är i behov av att utkontraktera sin it-drift också ska kunna göra det är att det finns ett regelverk som skapar förutsättningar för utkontraktering. Dagens reglering medger utkontraktering av it-drift men med vissa begränsningar. Vår bedömning är att det behövs en reglering som i större utsträckning än den nuvarande ger ett uttryckligt stöd för att lämna ut uppgifter vid utkontraktering av it-drift. Därför föreslår vi en sekretessbrytande bestämmelse i OSL.

12.3 Allmän bedömning av förslagets påverkan på aktörernas beteende

En förväntad konsekvens av våra förslag blir en minskad osäkerhet om vad som gäller vid utkontraktering av it-drift till privata tjänsteleverantörer. Det bör få positiva konsekvenser för statliga myndigheter, kommuner och regioner men också för branschen. För statliga myndigheter, kommuner och regioner som haft behov av att utkontraktera men som valt att avvakta på grund av det osäkra rättsläget,

kan våra slutsatser om röjande och vårt förslag till sekretessbrytande bestämmelse underlätta beslut om vägval.

Redan i dag måste en statlig myndighet, kommun eller region som överväger utkontraktering av it-drift säkerställa att utkontrakteringen kan ske på ett sätt som uppfyller krav på informationssäkerhet, säkerhetsskydd, sekretess och dataskydd. Vårt förslag till bestämmelse ger dels ett uttryckligt stöd för att lämna ut uppgifter som omfattas av absolut sekretess, dels stöd för att utlämnande av uppgifter där sekretessen är reglerad med skaderekvisit kan ske efter en mer övergripande bedömning än vad som är möjligt i dag.

Vår bedömning är att införandet av en sekretessbrytande bestämmelse i praktiken innebär en begränsad förändring för statliga myndigheter, kommuner och regioner när det gäller vilka överväganden som behöver göras inför en utkontraktering av it-drift. Förslagets påverkan på deras beteende kan möjligen variera beroende på hur de enskilda aktörerna hittills förhållit sig till utkontraktering och om de har tidigare erfarenhet av utkontraktering. Sammantaget bedömer vi dock att vårt förslag på det stora hela innebär relativt små förändringar i övervägandesituationen vid beslut om utkontraktering.

12.4 Påverkan på kostnader eller intäkter för staten, kommuner, regioner, företag eller andra enskilda

En utgångspunkt för förslaget i delbetänkandet är att statliga myndigheter, kommuner och regioner fortsatt ska ha möjlighet att – med bibehållen säkerhet – utkontraktera it-drift. En förväntad konsekvens av vårt förslag blir en minskad osäkerhet om vad som gäller vid utkontraktering till privata tjänsteleverantörer. Det förväntas få positiva konsekvenser både för offentlig sektor där en del nu väntar med att agera, men också för branschen som kan anpassa sina tjänster utifrån det klargjorda rättsläget.

Införandet av en sekretessbrytande bestämmelse med villkor i form av intresseavvägning kan inledningsvis ställa krav på vissa förändringar i rutiner vid genomförande av upphandlingar som kan kräva mer tid och resurser för varje enskild aktör. Det kan därmed antas att den nya administrativa rutinen inledningsvis medför vissa merkostnader för aktörerna. Över tid, i takt med att rutiner etableras och aktörerna får mer erfarenhet, bör arbetssättet i högre grad kunna standardi-

seras och eventuella ökade kostnader för den nya rutinen kunna minska. Kostnaderna kan eventuellt bli lägre än dagens kostnader för skadeprövning i samband med upphandlingar av it-drift. Det som talar för detta är att den sekretessbrytande bestämmelsen ger stöd för en mer övergripande prövning vid utlämnande än vad nu gällande regelverk medger. Vilka effekterna blir kommer rimligen att variera med hänsyn till hur verksamheternas it-drift är organiserad i dag. För en statlig myndighet, kommun eller region som hittills hanterat sin it-drift i egen regi, men som överväger utkontraktering, kan förutsättningarna påverkas på ett annat sätt än för en myndighet, en kommun eller en region som redan har utkontrakterat hela eller delar av sin it-drift.

Den sekretessbrytande bestämmelsen som vi föreslår innebär att det införs ett uttryckligt stöd för att göra en mer övergripande bedömning, i form av en intresseavvägning, än vad som är fallet vid en skadeprövning. Vår bedömning är därför att den sekretessbrytande bestämmelsen på sikt kommer att innebära en förenkling vid utlämnande av uppgifter i samband med utkontraktering jämfört med vad som gäller i dag. Bestämmelsen möjliggör dessutom utlämnande av uppgifter som omfattas av absolut sekretess.

Eftersom förslaget bygger på att varje aktör själv ska svara för intresseavvägningen är det svårt att i detta läge bedöma hur bedömningar och praxis kan komma att utvecklas. Utifrån vår kartläggning vet vi att statliga myndigheter ser kompetensbrist som den största riskfaktorn för säker it-drift. Motsvarande bild framkommer i rapporter etc. som avser kommuner och regioner. Vi vet också att många statliga myndigheter anser att det är svårt att upprätthålla kompetens för att göra avvägningar mellan säker och kostnadseffektiv it-drift. För att säkerställa utkontraktering med bibehållen säkerhet bedömer vi att den sekretessbrytande bestämmelsen med intresseavvägning bör kompletteras med central vägledning och stöd till statliga myndigheter, kommuner och regioner. Vi avser att återkomma med förslag om detta i vårt slutbetänkande.

Sammantaget bedöms kostnadseffekterna av förslaget bli begränsade för berörda aktörer. Förslagen bedöms inte heller leda till några mer betydande konsekvenser för samhällsekonomin i övrigt.

Förslaget om inskränkt meddelarfrihet bedöms inte ha någon påverkan på kostnader eller intäkter för staten, kommuner, regioner, företag eller andra enskilda.

12.5 Effekter av betydelse för företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt

12.5.1 Berörda företag, branscher m.m.

De företag som berörs av vårt förslag finns i första hand inom it-sektorn. För att illustrera sektorns storlek kan nämnas att IT- och Telekomföretagen, som är bransch- och arbetsgivarorganisation på området, har cirka 1 300 medlemsföretag, vilka sammantaget har närmare 100 000 medarbetare i Sverige. Alla branschens företag är dock inte medlemmar i IT- och Telekomföretagen. Statistik på organisationens hemsida visar att den svenska it- och telekombranschen 2017 totalt sysselsatte nästan 210 000 personer, fördelat på cirka 50 000 företag. De flesta företagen i branschen är små – statistiken på IT- och Telekomföretagens hemsida visar att 97 procent av företagen har färre än 20 anställda och 0,5 procent har fler än 100 anställda.

Flertalet av de företag som nämns ovan arbetar dock med annat än it-driftstjänster. It-driftstjänsternas del av den samlade it-marknaden är dock omfattande. Exakt hur stor är dock svårt att ange. För att ändå försöka exemplifiera har det beräknats att statsförvaltningens it-kostnader uppgår till mellan 25 och 30 miljarder kronor per år och att omkring 15 procent av de statliga myndigheternas it-verksamhet är utkontrakterad mätt i andel av de totala it-kostnaderna. För kommuner och regioner saknas motsvarande uppgifter. Enligt Digitaliseringsrättsutredningen uppgår dock de statliga myndigheternas, kommunernas och regionernas sammanlagda årliga it-kostnader till 45 miljarder kronor. Bland de företag, i synnerhet de större, som säljer it-driftstjänster på den svenska marknaden har många sin huvudsakliga hemvist i andra länder. Många företag har också svenskt säte eller ursprung. Som illustration kan nämnas Kammarkollegiets ramavtalsområde It-drift. Nuvarande ramavtal för it-drift omfattar två områden: ett för myndigheter med 100–400 anställda, och ett som vänder sig till myndigheter med fler än 400 anställda. Totalt finns 13 tjänsteleverantörer med på endera eller båda områdena. Knappt hälften av dessa företag har sitt ursprung i Sverige, men har i flera fall gått samman med utländska företag. Övriga företag är svenska dotterbolag till – inte sällan mycket stora – multinationella företag

med sitt ursprung i andra länder. Några av ramavtalsleverantörerna har fusionerat med varandra sedan nuvarande ramavtal tecknades.

12.5.2 Tidsåtgång och administrativa kostnader för företagen

Vårt förslag till sekretessbrytande bestämmelse kan leda till att statliga myndigheter, kommuner och regioner ställer hårdare krav på de privata tjänsteleverantörerna. Det är dock svårt att bedöma hur kravnivån generellt kommer att utvecklas eftersom förslaget innebär att varje enskild aktör själva ska svara för intresseavvägningen och dess kriterier.

Om vårt förslag i förlängningen leder till förändrade och eventuellt hårdare krav på de privata tjänsteleverantörerna, så kan detta medföra att anbudsgivarna behöver ägna mer tid och resurser åt att utforma anbuden. Det får dock anses ligga i rollen som anbudsgivare att förhålla sig till de krav som ställs av de aktörer som upphandlar it-driftstjänster. Så länge en förändrad kravbild har sin grund i ett skäligt intresse av värnande av sekretess och säkerhet bedöms därför att denna påverkan på anbudsgivarna är av liten betydelse.

Det ska i sammanhanget också framhållas att vår bedömning är att förslaget snarare innebär en förenkling för de aktörer som vill utkontraktera it-drift jämfört med vad som gäller i dag.

12.5.3 Andra kostnader och förändringar i företagens verksamhet

Utöver de kostnads- och konkurrenskonsekvenser som tidigare beskrivits bedöms vårt förslag inte ha några mer betydande konsekvenser i dessa hänseenden.

12.5.4 Påverkan på konkurrensförhållandena för företagen

Som vi beskrivit ovan kan vårt förslag eventuellt leda till att statliga myndigheter, kommuner och regioner ställer hårdare krav på de privata tjänsteleverantörerna än i dag. Det kan möjligen medföra att antalet tänkbara tjänsteleverantörer minskar i antal, med försämrad konkurrens och högre priser som följd. Eftersom vi föreslår att varje

enskild aktör själv ska svara för intresseavvägningen är det dock svårt att bedöma hur kravnivån generellt kommer att utvecklas och därmed hur stor denna effekt kan få för företagen.

12.5.5 Påverkan i andra avseenden på företagen

Utöver vad som tidigare redogjorts för bedöms förslaget inte ha någon betydande påverkan i andra avseenden på företagen.

12.5.6 Särskilda hänsyn till små företag

It-driftsbranschen präglas av stordriftsfördelar. Små företag har i regel sämre arbetsförutsättningar och konkurrensförmåga än stora företag. I någon mån lär detta förhållande komma att förstärkas med förslagen i delbetänkandet, eftersom ett litet företag kan antas ha mindre marginal för att möte de hårdare krav som kan antas bli följden av vårt förslag. Denna effekt bedöms dock vara marginell.

Om små privat tjänsteleverantörer verkligen kommer att påverkas negativt jämfört med stora företag beror dock mycket på hur den genomsnittliga kravnivån på tjänsteleverantörer vid utkontraktering av it-driftstjänster kommer att utvecklas till följd av kravet på intresseavvägning. Om statliga myndigheter, kommuner och regioner skulle börja ställa krav på att tjänsteleverantörerna bör ha svensk hemvist skulle det kunna ha en positiv effekt för små, inhemska tjänsteleverantörer jämfört med stora utländska företag.

12.5.7 Förslaget om inskränkt meddelarfrihet

Förslaget om inskränkt meddelarfrihet bedöms inte få några effekter av betydelse för företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt.

12.6 Överensstämmelse med skyldigheter som följer av Sveriges anslutning till EU

Enligt vår bedömning är våra förslag till författningsändringar förslag i linje med de skyldigheter som följer av EU-rätten. Som påtalas i delbetänkandet finns det annan lagstiftning som en offentlig aktör behöver beakta innan beslut om en utkontraktering, bl.a. dataskyddsförordningen.

Vårt förslag på en sekretessbrytande bestämmelse med en intresseavvägning är inte utformat på ett sådant sätt att det exkluderar europeiska aktörer.

12.7 Särskilda hänsyn avseende tidpunkten för ikraftträdande och om behov av speciella informationsinsatser

Vi har förslagit tidpunkt för ikraftträdande med beaktande av dels behovet av beredningstid, dels utifrån ett uttalat behov om ett så snabbt införande som möjligt

Vi bedömer att det kan finnas behov av vägledning och informationsinsatser om en sekretessbrytande bestämmelse med intresseavvägning införs i OSL. Vi avser att återkomma till detta i vårt slutbetänkande.

12.8 Övriga konsekvenser av förslaget

12.8.1 Konsekvenser för den kommunala självstyrelsen

Vår intention är att förslaget ska ge fortsatt möjlighet för statliga myndigheter, kommuner och regioner att med bibehållen säkerhet utkontraktera sin it-drift. En förväntad konsekvens av vårt förslag blir en minskad osäkerhet om vad som gäller för kommuner och regioner vid utkontraktering.

Förslaget innebär inte en inskränkning i den kommunala självstyrelsen. Att kommuner och regioner enligt förslaget själva ska svara för intresseavvägningen bör ge visst utrymme för dem att anpassa kraven till en för dem lämplig nivå.

Förslaget om inskränkt meddelarfrihet bedöms inte få några konsekvenser för den kommunala självstyrelsen.

12.8.2 Konsekvenser för brottsligheten och det brottsförebyggande arbetet

Förslaget om en sekretessbrytande bestämmelse bedöms ha liten betydelse för brottsligheten och det brottsförebyggande arbetet. Möjligen kan sägas att om kravet på intresseavvägning leder till att statliga myndigheter, kommuner och regioner ställer hårdare krav på de privata tjänsteleverantörerna i samband med upphandling av it-driftstjänster, så bör det minska risken för att tjänsteleverantörer med brottsliga intentioner ges möjlighet att komma i fråga för uppdrag på området. Med hänsyn till marknadens struktur och nuvarande upphandlingars karaktär (vad gäller inriktning, omfattning m.m.) kan det dock antas att riskerna i detta hänseende är små redan med nuvarande regelverk.

Förslaget om inskränkt meddelarfrihet innebär att det blir straffbart att lämna ut uppgifter till grundlagsskyddad media för den som omfattas av lagen (2020:914) om tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter. Förslaget innebär på så vis en utvidgning av det straffbara området. Vi ser dock inga skäl att tro att det skulle ske straffbara gärningar i någon större omfattning till följd av den nya kriminaliseringen, eller att det skulle bli fråga om en stor mängd nya åtal. Vi bedömer därför att förslaget om inskränkt meddelarfrihet får begränsade konsekvenser för brottsligheten och det brottsförebyggande arbetet.

12.8.3 Konsekvenser för sysselsättning och offentlig service i olika delar av landet

Vi bedömer det som mindre sannolikt att förslaget kommer att få någon direkt betydelse för utbudet av offentlig service i olika delar av landet.

Förslagets konsekvenser på sysselsättningen i Sverige generellt och i olika delar av landet mer specifikt beror mycket på hur den genomsnittliga kravnivån på privata tjänsteleverantörer vid utkontraktering av it-driftstjänster kommer att utvecklas. Möjligen kan

tänkas att om kraven på tjänsteleverantörerna utvecklas mot att vissa svenska tjänsteleverantörer inte längre kan komma i fråga för it-driftsuppdrag åt statliga myndigheter, kommuner och regioner, så kan behovet av personal hos dessa tjänsteleverantörer komma att minska. Om utvecklingen å andra sidan skulle bli sådan att intresseavvägningarna tenderar att gynna inhemska tjänsteleverantörer före utländska, så skulle det kunna skapa möjligheter att etablera en större marknad för svenska tjänsteleverantörer. Sannolikt skulle det samlade behovet av personal hos svenska tjänsteleverantörer då öka. Det är dock svårt att bedöma hur stora dessa eventuella effekter kan bli, liksom om storleken på dem skulle variera mellan olika delar av landet.

I sammanhanget bör också upprepas att hur den genomsnittliga kravnivån vid upphandling av it-driftstjänster kommer att utvecklas när det nya kravet på intresseavvägning införs helt beror på vilka val de enskilda aktörerna kommer att göra. Det är upp till varje enskild aktör som vill göra en utkontraktering att utöver intresseavvägningen även beakta krav på säkerhetsskydd, sekretess och dataskydd. Det är i slutändan också upp till varje enskild aktör att ta ställning till om det, utifrån den samlade bedömningen utifrån samtliga tillämpliga regelverk, finns anledning att ställa krav på leverans från exempelvis Sverige.

Förslaget om inskränkt meddelarfrihet bedöms inte få några konsekvenser för sysselsättning och offentlig service i olika delar av landet.

12.8.4 Konsekvenser för små företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt i förhållande till större företag

It-driftsbranschen präglas av tydliga stordriftsfördelar. Små företag har närmast definitionsmässigt sämre arbetsförutsättningar och konkurrensförmåga än stora företag. I någon mån lär detta förhållande komma att förstärkas med förslaget i delbetänkandet, eftersom ett litet företag kan antas ha mindre marginal för att hantera de förändrade krav på tjänsteleverantörerna som eventuellt kan bli följden av en sekretessbrytande bestämmelse med villkor i form av intresseavvägning. Sett som andel av de samlade storleksnackdelar som små företag på den berörda marknaden har jämfört med stora företag bedöms dock denna effekt vara marginell.

Om små tjänsteleverantörer av it-driftstjänster kan komma att påverkas negativt jämfört med stora företag beror på hur den genomsnittliga kravnivån på leverantörer vid utkontraktering av it-drift kommer att utvecklas till följd av kravet på intresseavvägning.

Förslaget om inskränkt meddelarfrihet bedöms inte få några konsekvenser för små företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt i förhållande till större företag.

12.8.5 Jämställdheten mellan kvinnor och män

Inget av de två förslagen bedöms ha betydelse för jämställdheten mellan kvinnor och män.

12.8.6 Möjligheterna att nå de integrationspolitiska målen

Inget av de två förslagen bedöms ha betydelse för möjligheterna att nå de integrationspolitiska målen.

12.9 Alternativa lösningar och effekter om någon reglering inte kommer till stånd

Vår analys av dagens förhållanden vad gäller statliga myndigheters, kommuner och regioners utkontraktering av it-drift leder till slutsatsen att det finns behov av en sekretessbrytande bestämmelse. Eftersom ett oklart rättsläge för utkontraktering till privata tjänsteleverantörer och avsaknaden av en lagbestämmelse som ger ett uttryckligt stöd för utlämnande av sekretessreglerade uppgifter inom ramen för utkontraktering av it-drift bedöms utgöra själva problemet är det svårt att se alternativa lösningar som skulle kunna hantera problemet på ett bättre sätt.

Vår slutsats att utkontraktering av it-drift innebär att de uppgifter som överförs till tjänsteleverantören röjs, ger en signal att den praxis som tillämpas av vissa statliga myndigheter, kommuner och regioner, och som innebär att uppgifter som lämnas ut till den privata tjänsteleverantören inte betraktas som röjda, inte är hållbar utifrån ett rättsligt perspektiv. Man kan därför anta att våra slutsatser, även om det inte skulle införas en sekretessbrytande bestämmelse, kan

leda till att statliga myndigheter, kommuner och regioner ser över och förändrar sitt beteende. Som vi påpekat är dock utkontraktering av it-drift en förutsättning för många statliga myndigheter, kommuner och regioner att kunna bedriva sin verksamhet på ett effektivt och ändamålsenligt sätt. Det framstår därför inte som sannolikt att dessa aktörer helt skulle upphöra med utkontraktering av it-drift om en sekretessbrytande bestämmelse inte införs.

13 Vårt fortsatta arbete

Enligt direktiven ska vi i vår delredovisning redogöra för förslag till inriktning för det fortsatta utredningsarbetet när det gäller samordnad it-drift.

Som framgår av avsnitt 2.3.1 ska vi i slutbetänkandet redovisa följande delar:

- en utvärdering av Försäkringskassans uppdrag om samordnad it-drift samt erfarenheter av andra exempel på samordnad it-drift i Sverige,
- en analys av de säkerhetsmässiga och rättsliga förutsättningarna för samordnad statlig it-drift,
- förslag om samordnad, säker och kostnadseffektiv statlig it-drift, och
- en konsekvensutredning.

I detta kapitel beskriver vi inriktningen för det fortsatta utredningsarbetet inför vårt slutbetänkande.

13.1 Våra samlade bedömningar i delbetänkandet

Utöver vad som framgår av direktiven är delbetänkandet en självklar utgångspunkt för det fortsatta arbetet och för utformningen av förslag om samordnad statlig it-drift. I detta ingår våra definitioner av säker och kostnadseffektiv it-drift på aktörs- och samhällsnivå liksom slutsatserna från vår kartläggning av statliga myndigheters it-drift och exemplen från andra länder. Våra slutsatser från vår rättsliga analys av förutsättningar för utkontraktering av it-drift till privata tjänsteleverantörer är relevanta även för den samordnade it-driften.

I kapitel 6–10 har vi redogjort för de regler om säkerhetsskydd, informationssäkerhet, dataskydd och sekretess som statliga myndigheter, kommuner och regioner har att beakta vid utkontraktering av it-drift till privata tjänsteleverantörer. Till det kommer de generella krav som ställs på offentlig verksamhet avseende bl.a. legalitet, objektivitet, saklighet och god hushållning med allmänna medel. Det finns med andra ord ett omfattande regelverk som myndigheter måste förhålla sig till vid utkontraktering av it-drift och som enligt vår mening inte lämnar utrymme för utkontraktering av it-drift till privata tjänsteleverantörer som är olämplig eller osäker. Detta under förutsättning att de rättsliga regler och krav som finns följs och att det finns ett systematiskt informationssäkerhetsarbete på plats inom statliga myndigheter, kommuner och regioner.

Vår kartläggning av statliga myndigheters it-drift i kapitel 4 visar dock att det finns brister i de statliga myndigheternas informationssäkerhetsarbete. Ungefär hälften av de myndigheter som besvarat vår enkät behöver etablera och utveckla sitt systematiska informationssäkerhetsarbete i verksamheten. Informationsklassning ingår här som en viktig del. Små och medelsmå myndigheter har i regel inte kommit lika långt i sitt informationssäkerhetsarbete som medelstora och stora myndigheter. I vår kartläggning har vi också ställt frågor om hinder för säker och kostnadseffektiv it-drift. Här framkommer att de största hindren för säker it-drift enligt myndigheterna är avsaknad av relevant kompetens och bristande informationsklassificering. Flera myndigheter lyfter också svårigheterna att omsätta tillämpliga regelverk i kravställning vid exempelvis utkontraktering som ett problem. Vi kan konstatera att det inte finns någon tillsyn över myndigheternas informationssäkerhetsarbete, men har i övrigt inte gjort några analyser eller bedömningar när det gäller styrning och organisering på informationssäkerhetsområdet.

I vår konsekvensutredning i kapitel 12 gör vi bedömningen att den sekretessbrytande bestämmelsen med intresseavvägning bör kompletteras med central vägledning och stöd till statliga myndigheter, kommuner och regioner för att säkerställa utkontraktering med bibehållen säkerhet.

Mot bakgrund av våra samlade bedömningar i delbetänkandet ser vi anledning att i vårt arbete med slutbetänkandet återkomma med fortsatt analys på bl.a. informationssäkerhetsområdet. Detta som underlag för förslag på lämpliga åtgärder för att åstadkomma en säker

it-drift oavsett om den bedrivs i egen regi, utkontrakterad eller genom samordnad it-drift. Detta ligger också i linje med våra direktiv.

Vår samlade bedömning i delbetänkandet är dock att de befintliga regelverk som statliga myndigheter, kommuner och regioner har att beakta vid utkontraktering av it-drift – korrekt tillämpade – ger förutsättningar för en säker utkontraktering av it-drift till privata tjänsteleverantörer samt att dessa regelverk inte innehåller några omotiverade begränsningar för sådan utkontraktering.

13.2 Utgångspunkter för det fortsatta arbetet

För att ta ställning till förutsättningarna för en **säker och kostnadseffektiv samordnad statlig it-drift** ser vi att följande punkter är centrala och bör löpa som en röd tråd i det fortsatta arbetet:

- **organisering** (befintlig myndighet, samverkan mellan myndigheter, ny myndighet)
- **tjänsteutbud** (standardiserade lösningar eller anpassning utifrån kundbehov och säkerhetskrav)
- **målgrupp** (verksamhet, myndighetsstorlek, behov, säkerhetskrav, myndigheter och information som inte bör omfattas av samordnad it-drift)
- **anslutning** (frivilligt eller obligatoriskt, prioriteringsmodeller för anslutning)
- **finansiering** (avgiftsfinansiering eller anslagsfinansiering)
- **införande** (nära kopplat till anslutningsmodell)
- **privata tjänsteleverantörer** (kommersiella it-driftstjänster som del av en samordnad statlig it-drift, hybridlösningar, samordnad upphandling av kommersiella it-driftstjänster).

Ett antal aspekter är viktiga att analysera i samband med de förslag som vi ska lämna om en samordnad statlig it-drift. Det gäller styrkor, svagheter, möjligheter och hot förknippade med olika sätt att styra myndigheternas it-drift, som staten har att välja på. En central marknadsplats för ackrediterade molntjänster som myndigheterna kan avropa (jfr G-Cloud i Storbritannien får sannolikt andra konsekvenser

än om en myndighet ges ett permanent uppdrag att koncentrera och sköta andra myndigheters it-drift (jfr Valtori i Finland). För att lämna väl underbyggda förslag kommer vi i slutbetänkandet att analysera dessa aspekter med utgångspunkt i myndigheternas behov av en säker och kostnadseffektiv it-drift.

13.3 Arbetssätt

Öppenhet och dialog med dem som berörs av våra eventuella förslag är viktigt även i vårt fortsatta arbete. Utöver avstämning och förankring i expertgrupp och referensgrupp kommer vi även fortsättningsvis att stämma av och kvalitetssäkra vårt arbete inom de arbetsgrupper inom juridik och säkerhet som vi etablerat. Det kan också vara aktuellt att etablera ytterligare en arbetsgrupp med inriktning på mer tekniska it-driftsfrågor.

Även om merparten av arbetet med utformning av förslag kommer att grunda sig på de analyser vi genomför i utredningsarbetet ser vi också ett behov av att involvera myndigheter och andra relevanta aktörer för att få synpunkter på förslagen. Vår ambition är att under våren 2021 genomföra en uppföljande workshop med myndigheter med fördjupade frågeställningar om samordnad it-drift samt ett öppet webinarium där vi presenterar våra tänkta förslag och vägvalen bakom dem.

13.4 Erfarenheter av samordnad it-drift i Sverige

Det finns flera exempel på samordnad it-drift i den statliga förvaltningen. Några har byggts upp på eget initiativ medan andra har etablerats genom regeringsbeslut. Utöver det kan även andra exempel på samordning inom den statliga förvaltningen vara intressanta som underlag för våra förslag om samordnad statlig it-drift.

13.4.1 Utvärdering av Försäkringskassans uppdrag om samordnad och säker it-drift

Försäkringskassan har sedan år 2017 ett regeringsuppdrag att erbjuda samordnad och säker it-drift till vissa myndigheter. Det övergripande syftet med uppdraget är att pröva och utvärdera former för samordnad och säker it-drift för lämpliga myndigheter. Uppdraget sträckte sig till en början fram till år 2020, men förlängdes i ett regeringsbeslut till den 31 december 2022 (I2019/02515/DF). Enligt regeringsbeslutet ska fokus under uppdragets fortsatta löptid ligga på att bibehålla den förmåga till samordnad och säker statlig it-drift som Försäkringskassan upparbetat hittills.

Enligt våra direktiv ska vi utvärdera Försäkringskassans uppdrag att tillhandahålla samordnad och säker statlig it-drift och redovisa vilka slutsatser som kan dras i fråga om bl.a. upparbetad organisation, finansieringsmodell, anslutningsprocess, tjänsteleverans, samordningsvinster samt påverkan på kärnverksamheten i fråga om bl.a. resursbehov och prioriteringar inom verksamheten. Här ingår också att utvärdera Försäkringskassans arbete med informationssäkerhet, säkerhetsskydd och kund- och avtalsförvaltning. Utvärderingen ska innehålla en analys av vilka eventuella samordningsvinster och andra nyttor (kostnadseffektivitet, ökad säkerhet, flexibilitet och skalfördelar) som kan uppnås vid samordnad statlig it-drift i jämförelse med it-drift i egen regi och utkontraktering. I detta ingår att också redovisa vilka eventuella nackdelar som kan följa av samordnad statlig it-drift. Vi ska därutöver analysera vilka lärdomar, erfarenheter och investeringar som är relevanta att vidareutveckla inom ramen för förslag till mer varaktiga former för samordnad statlig it-drift.

Utvärderingen kommer att genomföras genom dokumentstudier, intervjuer med företrädare för olika delar av Försäkringskassan samt med företrädare för kundmyndigheter, myndigheter som överväger att gå in i en samordning med Försäkringskassan samt samverkansmyndigheter. Försäkringskassan lät genomföra en extern utvärdering av uppdraget år 2019 och det är naturligt att följa upp delar av denna utvärdering och komplettera med de specifika frågeställningar som framgår av utredningsdirektiven.

Den närmare planeringen av utvärderingen kommer att läggas fast i början av 2021. I korthet kommer vi att inleda med dokumentstudier och intervjuer med dem som arbetat närmast uppdraget inom

Försäkringskassan (projektledare, kundansvariga samt ansvariga chefer inom it-avdelningen). Därefter kommer vi att fördjupa oss i frågor om anslutningsprocess, tjänsteleverans, säkerhet, ekonomimodell, avtal, etc. Även i denna del kommer vi att genomföra dokumentstudier och intervjuer med olika företrädare för Försäkringskassan samt med företrädare för kundmyndigheterna. Utöver detta ska vi intervjua företrädare för kärnverksamheten inom Försäkringskassan samt de samverkansmyndigheter som pekats ut i Försäkringskassans uppdrag.

När det gäller nyttor med samordnad it-drift behöver vi ta del av uppföljningar både från Försäkringskassan och kundmyndigheterna för att se utvecklingen över tid för olika nyckelindikatorer samt prognosen framåt. Vi vet dock från tidigare utvärderingar att det finns begränsad information att tillgå, särskilt vad gäller nollvärden för kundmyndigheterna när de gick in i samordningen med Försäkringskassan. Detta måste tas i beaktande.

Vi har under våren tagit fram en kravställning gentemot Försäkringskassan där det bl.a. framgår vilka roller och funktioner vi vill intervjua i organisationen samt vad vi i övrigt behöver för att kunna genomföra utvärderingen. Kravställningen har efter dialog godkänts av Försäkringskassan och kommer utgöra grund för samarbetet oss emellan.

13.4.2 Andra exempel på samordnad it-drift

Av direktiven framgår att vi ska dra lärdomar även av andra exempel på samordnad it-drift i Sverige, som exempelvis Skatteverkets it-driftshantering åt Kronofogdemyndigheten och Valmyndigheten samt länsstyrelsernas samordnade it-drift. Vi bedömer att även samordningen inom universitets- och högskolesektorn genom SUNET kan vara av intresse.

I denna del kommer vi att arbeta huvudsakligen med intervjuer för att fånga positiva och negativa erfarenheter av samordnad it-drift, lärdomar, förändringar som gjorts över tid samt vilka utmaningar som finns i dag och framåt. Utgångspunkt tas i punkterna i avsnitt 13.2.

13.4.3 Erfarenheter av Statens servicecenter

I vår kartläggning av statliga myndigheters it-drift, och särskilt behoven av it-drift, har flera myndigheter gjort jämförelser med Statens servicecenters (SSC) samordning av bl.a. löne- och ekonomitjänster. Exempelvis har flera myndigheter lyft fram att det är relevant att titta på anslutningsmodell, finansieringsmodell, tjänsteutveckling samt ansvarsförhållanden mellan SSC och kundmyndigheter. Erfarenheter för olika typer av myndigheter, t.ex. små respektive stora myndigheter är också av intresse. Vi har under våren varit i kontakt med SSC för att få deras beskrivning av erfarenheter och utmaningar i uppdraget. Vår uppfattning är att det kan finnas erfarenheter att lära av exemplet SSC såväl från kundmyndighetsperspektivet, tjänsteleverantörsperspektivet som när det gäller regeringens styrning som underlag för våra förslag om samordnad statlig it-drift.

13.5 Säkerhetsmässiga och rättsliga förutsättningar för samordnad statlig it-drift

13.5.1 Inledning

Detta delbetänkande innehåller en kartläggning och analys av de rättsliga förutsättningarna för att utkontraktera it-drift till privata tjänsteleverantörer, utifrån regelverken om säkerhetsskydd, informationssäkerhet, dataskydd samt offentlighet och sekretess.

Enligt våra direktiv ingår det även i vårt uppdrag att analysera de säkerhetsmässiga förutsättningarna för samordnad statlig it-drift, särskilt när det gäller krav på säkerhetsskydd och informationssäkerhet samt sekretess och skyddet för den personliga integriteten. Vidare ska vi enligt direktiven analysera de rättsliga förutsättningarna för samordnad statlig it-drift, särskilt när det gäller avtals- och upphandlingsfrågor samt konkurrens- och marknadsrättsliga frågor. Vi ska även vid behov lämna författningsförslag som möjliggör att inrätta samordnad statlig it-drift. Dessa frågor kommer vi att behandla i slutbetänkandet.

I slutbetänkandet avser vi även återkomma till de säkerhetsmässiga för- och nackdelarna för statliga myndigheter att ansluta sig till samordnad it-drift jämfört med att hantera it-drift i egen regi eller utkontraktera driften. Denna analys bör enligt våra direktiv bl.a.

innehålla fördjupade resonemang om hur regelverken om säkerhetsskydd, informationssäkerhet, offentlighet och sekretess samt skyddet för den personliga integriteten kan upprätthållas och utvecklas.

I detta avsnitt redogör vi översiktligt för de principiella frågeställningar som vi bedömer behöver analyseras i slutbetänkandet. Uppräkningen är inte uttömmande, utan fler frågor kan tillkomma.

13.5.2 Avtal mellan myndigheter

En allmän utgångspunkt för statliga myndigheters möjligheter att ingå avtal, som innehåller ekonomiska förpliktelser för staten, är att myndigheterna inte utgör några självständiga juridiska enheter (rättssubjekt). De utgör endast delar av rättssubjektet staten. En konsekvens av detta är att de inte kan ingå bindande avtal med varandra; ett avtal förutsätter att det sluts av två självständiga parter. De överenskommelser mellan statliga myndigheter som förekommer är alltså en särskild från avtalet skild rättsfigur som inte regleras i lagstiftningen. Det medför också att de sedvanliga tvistelösningsmekanismerna, rättegång enligt rättegångsbalken och förfarande enligt lagen (1929:145) om skiljemän, inte står till förfogande om det uppkommer någon tvist om tillämpningen av en överenskommelse mellan de myndigheter som träffat överenskommelsen.

En viktig fråga i det fortsatta utredningsarbetet blir därför hur myndigheters inbördes förhållanden kan och bör regleras vid samordnad it-drift. Vidare finns det anledning att överväga vilka tvistelösningsmekanismer som bör stå till buds och hur ansvar lämpligen kan utkrävas.

13.5.3 Upphandling

En central fråga i förhållande till samordnad statlig it-drift är om det är förenat med upphandlingsplikt när en myndighet erhåller it-drift från en eller flera andra myndigheter. Upphandlingsregelverket ska tillämpas när en upphandlande myndighet åtar sig att erlägga betalning i utbyte mot att en leverantör utför en prestation. Avtalet måste innefatta rättsligt bindande skyldigheter av ömsesidig karaktär och kravet på bundenhet innebär att skyldigheterna ska kunna fullgöras genom rättsliga åtgärder. Det finns flera undantag från upphand-

lingsplikten, bl.a. för intern upphandling, för upphandling mellan upphandlande myndigheter och vid tilldelning av tjänstekontrakt på grund av ensamrätt.

Vid upphandling på försvars- och säkerhetsområdet gäller särskilda regler.

Det är nödvändigt att i det fortsatta utredningarbetet analysera vilka konsekvenser regelverket om offentlig upphandling får för tillhandahållandet av samordnad it-drift och vilka författningsåtgärder som kan och bör vidtas för att skapa förutsättningar för samordnad it-drift utifrån upphandlingssynpunkt.

13.5.4 Konkurrensrätt

I våra direktiv anges det att det behöver utredas om det finns konkurrens- och marknadsrättsliga förutsättningar för samordnad it-drift och om det är nödvändigt att författningsreglera anslutning till sådan it-drift.

I 3 kap. 27 § konkurrenslagen (2008:579) finns en konfliktslösningsregel som kan tillämpas vid konkurrensbegränsande offentlig säljverksamhet i kommunal eller statlig regi. Regeln innebär, för statlig verksamhets del, att staten får förbjudas att i sådan säljverksamhet som omfattas av konkurrenslagen tillämpa ett visst förfarande om förfarandet snedvrider, eller är ägnat att snedvrida, förutsättningarna för en effektiv konkurrens på marknaden, eller hämmar, eller är ägnat att hämma, förekomsten eller utvecklingen av en sådan konkurrens.

Enligt bestämmelsen får dock förbud inte meddelas för förfaranden som är försvarbara från allmän synpunkt. I specialmotiveringen till bestämmelsen anges att vid prövningen om ett förfarande från allmän synpunkt ska särskilt beaktas om förfarandet strider mot en lag, en annan författning eller något annat för staten bindande direktiv. Vidare anges att det kan vidare vara fråga om t.ex. ett regeringsbeslut utan samband med normgivning. Den principiella utgångspunkten är att ett förfarande som strider mot lag etc. saknar försvarbarhet från allmän synpunkt (prop. 2008/09:231, s. 58 f.).

En konkurrensrättslig fråga som vi behöver utreda är därför vilka förfaranden i fråga om samordnad it-drift som omfattas av konfliktlösningsregeln avseende konkurrensbegränsande offentlig säljverksamhet och vilka åtgärder som kan och bör vidtas för att säkerställa

och tydliggöra att en samordnad statlig it-drift tillgodoser samhälleliga intressen som överväger konkurrensintresset.

13.5.5 Dataskydd

En grundläggande utgångspunkt för upprätthållandet av dataskyddsregelverket är att det är klarlagt och tydligt vem som är personuppgiftsansvarig för behandlingen av personuppgifter. Myndigheter är vanligen personuppgiftsansvariga för den behandling av personuppgifter som de utför, antingen på grund av att personuppgiftsansvaret är författningsreglerat eller utifrån bedömningen att det är myndigheten som bestämmer ändamål och medel för behandlingen av personuppgifter.

Om beslut om ändamål och medel fattas av flera myndigheter gemensamt så kan ett gemensamt personuppgiftsansvar uppstå. En myndighet som behandlar personuppgifter för en annan myndighets räkning kan också vara personuppgiftsbiträde åt den uppdragsgivande (och personuppgiftsansvariga) myndigheten.

Det finns behov av att analysera och klarlägga hur personuppgiftsansvaret förhåller sig vid samordnad it-drift. Det behöver också övervägas om det finns skäl att fastställa personuppgiftsansvaret i författning för att ansvarsfördelningen för behandling av personuppgifter vid samordnad it-drift ska vara tydlig.

Administrationen av personuppgiftsbiträdesavtal upplevs ofta som betungande. Det finns därför anledning att ta ställning till om hanteringen av personuppgifter vid tillhandahållande av samordnad it-drift bör regleras genom författning i stället för genom avtal mellan uppdragsgivande myndighet och den eller de myndigheter som tillhandahåller it-driften, i syfte att minska den administrativa bördan.

Bortsett från dessa två mer specifika frågor så behöver givetvis en genomlysning av hur samtliga krav som dataskyddsregelverket ställer kan uppfyllas vid samordnad it-drift, beroende på hur denna utformas. Det behöver också övervägas om det finns behov att författningsreglera andra delar av personuppgiftsbehandlingen än de som rör personuppgiftsansvar och personuppgiftsbiträdets hantering av uppgifter.

13.5.6 Sekretess

I våra direktiv ingår att analysera hur regelverket om sekretess kan upprätthållas och utvecklas vid samordnad it-drift. Redan i dag gäller sekretess för uppgifter som hanteras av en myndighet som ett led i teknisk bearbetning och lagring för en annan myndighets räkning genom bestämmelserna om överföring av sekretess enligt 11 kap. 4 § OSL och absolut sekretess för enskildas personliga och ekonomiska förhållanden vid teknisk bearbetning och lagring enligt 40 kap. 5 § OSL.

Om den samordnade it-driften innehåller moment som kan bedömas gå utöver vad som innefattas i teknisk bearbetning och teknisk lagring så kan det finnas skäl att överväga införande av ytterligare bestämmelser om sekretess hos den myndighet eller de myndigheter som tillhandahåller samordnad it-drift.

Vi föreslår i detta delbetänkande en sekretessbrytande bestämmelse för utlämnande av uppgifter för teknisk bearbetning och lagring. Den bestämmelse som vi föreslår gäller för utlämnanden av sekretessreglerade uppgifter till såväl en privat tjänsteleverantör som till annan myndighet. Eftersom bestämmelsen är begränsad till teknisk bearbetning och teknisk lagring s kan det finnas anledning att överväga att införa en bredare sekretessbrytande bestämmelse för utlämnanden till andra myndigheter, beroende på hur den samordnade it-driften utformas och vad den ska innehålla.

13.5.7 Säkerhetsskydd och informationssäkerhet

Vi ska enligt utredningsdirektiven analysera de säkerhetsmässiga förutsättningarna för samordnad statlig it-drift, särskilt när det gäller krav på säkerhetsskydd och informationssäkerhet. Vi ska enligt direktiven också analysera de säkerhetsmässiga för- och nackdelarna för statliga myndigheter att ansluta sig till samordnad it-drift jämfört med att hantera it-drift i egen regi eller utkontraktera driften. Det finns därför anledning för oss att i vårt fortsatta arbete särskilt undersöka, utifrån regelverken om säkerhetsskydd och informationssäkerhet, betydelsen av att samla en potentiellt omfattande mängd information från flera olika myndigheter i en samordnad it-drift.

13.5.8 Allmänna handlingar och arkivering

Handlingar, det vill säga framställningar i skrift eller bild och upptagningar som endast med tekniska hjälpmedel kan läsas, avlyssnas eller uppfattas på annat sätt (2 kap. 3 § TF, tryckfrihetsförordningen), är allmänna om de förvaras hos en myndighet och är att anse som inkommen till eller upprättad hos en myndighet (2 kap. 4 § TF).

En handling som förvaras hos en myndighet endast som ett led i en teknisk bearbetning eller teknisk lagring för någon annans räkning anses dock inte som allmän handling hos den myndigheten (2 kap. 13 § TF).

Enligt 3 § arkivlagen bildas en myndighets arkiv av de allmänna handlingarna från myndighetens verksamhet. Utgångspunkten i 4 § arkivlagen är att varje myndighet själv svarar för vården av sitt arkiv, vilket innebär att myndigheten har ansvaret för att uppfylla de krav som ställs på arkivvården enligt arkivlagen.

I den mån som en myndighet vid tillhandahållande av samordnad it-drift befattar sig med handlingar på ett sätt som går utöver enbart teknisk bearbetning och lagring så kan allmänna handlingar uppkomma i myndighetens verksamhet. Frågan uppstår då om och hur arkivansvaret kan fördelas mellan kundmyndigheten och tillhandahållande myndighet.

13.5.9 Behov av författningsreglering och förslag till sådan reglering

Förvaltningslagens legalitetsprincip innebär att det ska finnas någon form av normmässig förankring för all typ av verksamhet som en myndighet bedriver (prop. 2016/17:180 s. 59). Det finns därför anledning att överväga vilken typ av övergripande styrning som krävs för att en eller flera myndigheter ska tillhandahålla samordnad it-drift.

Det kan också finnas skäl utifrån utfallet av analyserna av konkurrens- och upphandlingsregelverken som talar för en författningsreglering av exempelvis anslutning till den samordnade it-driften. Som vi lyfter ovan kan det också finnas skäl att reglera vissa aspekter av personuppgiftsbehandlingen, exempelvis personuppgiftsansvaret och villkoren för personuppgiftsbiträdets behandling.

Det finns även andra skäl än strikt juridiska som gör en tydlig styrning önskvärd. Vi återkommer till detta i vårt slutbetänkande.

13.6 Förslag om samordnad, säker och kostnadseffektiv statlig it-drift

Enligt utredningsdirektiven ska vi, utifrån resultatet av övriga delar i utredningsarbetet, överväga vilka behov som finns av att inrätta mer varaktiga former av samordnad it-drift för den statliga förvaltningen samt om det är lämpligt ur säkerhetssynpunkt. Vi ska lämna alternativa och rangordnade förslag på organisationsmodeller och med utgångspunkt i dessa även lämna förslag på en eller flera alternativa införandeplaner. Eventuella förslag som har övervägts men avfärdats ska redovisas och motiveras. Förslagen ska grunda sig på en analys av säkerhetsmässiga, samhällsekonomiska och budgetära konsekvenser av att inrätta samordnad it-drift. Vi ska också ta hänsyn till eventuella risker med centralisering av statsförvaltningens it-drift, geografisk placering och fysiskt skydd av datorhallar, potentiell exponering av myndigheters information mot andra länders rättsordningar samt risken för att informationen görs åtkomlig för obehöriga.

Vid utformningen av förslagen utgår vi från de utgångspunkter som vi presenterar i avsnitt 13.2 samt de slutsatser som vi dragit i delbetänkandet och i våra analyser av erfarenheterna av samordnad it-drift och de säkerhetsmässiga och rättsliga förutsättningarna för samordnad it-drift. Till detta kommer vårt perspektiv på säker och kostnadseffektiv it-drift på aktörs- och samhällsnivå som vi beskrivit i avsnitt 2 i detta delbetänkande. Förslagen om samordnad it-drift behöver i detta sammanhang också analyseras ur ett riskperspektiv, utifrån olika hotnivåer i samhället och utifrån ett totalförsvarsperspektiv.

Vid sidan av de rangordnade förslagen ska vi även föreslå hur generella och myndighetsspecifika krav på informationssäkerhet och säkerhetsskydd kan tillgodoses. Vi ser, utöver detta, att det kan finnas anledning att lämna även andra förslag om styrning och ansvarsfördelning på aktörs- och samhällsnivå vad gäller säker och kostnadseffektiv it-drift.

13.7 Konsekvensutredning

Vi ska enligt utredningsdirektiven analysera förslagens konsekvenser i enlighet med kommittéförordningen (1998:1474) och förordningen om konsekvensutredning vid regelgivning (2007:1244). Vi ska ana-

lysera de samhällsekonomiska effekterna och även redogöra för konsekvenserna av status quo, dvs. att inte samordna myndigheternas it-drift. Ekonomiska konsekvenser för enskilda myndigheter som direkt berörs av förslagen ska redovisas. Om vi lämnar förslag som innebär en verksamhetsövergång eller avveckling av verksamhet ska de budgetära och verksamhetsmässiga konsekvenserna för detta särskilt analyseras. Vidare ska vi redogöra för eventuella marknadseffekter och konkurrenspåverkan för det privata näringslivet i förhållande till de potentiella samordningsvinster som kan uppnås av samordnad it-drift för hela eller delar av den statliga förvaltningen.

14 Ikraftträdande

14.1 Ikraftträdande

Utredningens förslag: Ändringarna i offentlighets- och sekretesslagen ska träda i kraft den 1 januari 2022.

Skälen för vårt förslag: Vi bedömer att det är angeläget att den sekretessbrytande bestämmelsen som vi föreslår träder i kraft så snart som möjligt, för att underlätta statliga myndigheters, kommuners och regioners utkontraktering av it-drift och för att ge ett tydligt rättsligt stöd för utlämnande av sekretessreglerade uppgifter.

Vi bedömer också att det är angeläget att den föreslagna inskränkningen i meddelarfriheten träder i kraft så fort som möjligt, för att göra lagen (2020:914) om tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter så verkningsfull som möjligt.

Med hänsyn till den tid som kan beräknas gå åt för remissförfarande, fortsatt beredning inom Regeringskansliet och riksdagsbehandling bör de lagbestämmelser utredningen föreslår tidigast kunna träda i kraft den 1 januari 2022. Förslagen är inte av den arten att de kräver några särskilda övergångsregler.

15 Författningskommentar

15.1 Förslaget till lag om ändring i offentlighets- och sekretesslagen (2009:400)

10 kap.

2 a §

Sekretess hindrar inte att en uppgift lämnas ut till ett företag eller en annan enskild eller till en annan myndighet som har i uppdrag att utföra endast teknisk bearbetning eller teknisk lagring för den utlämnande myndighetens räkning.

En uppgift ska inte lämnas ut om det intresse som sekretessen ska skydda har företräde framför intresset av att uppgiften lämnas ut.

Paragrafen är ny.

Genom bestämmelsen införs en sekretessbrytande bestämmelse som kan tillämpas när en myndighet lämnar ut uppgifter till någon som ska utföra teknisk bearbetning eller teknisk lagring för myndighetens räkning. De överväganden som ligger till grund för bestämmelsen finns i avsnitt 10.2.4–10.3.8.

Bestämmelsen är tillämplig när en myndighet lämnar ut uppgifter till såväl privata tjänsteleverantörer som till andra myndigheter.

Den sekretessbrytande bestämmelsen är avgränsad till utlämnanden för uppdrag som innebär endast teknisk bearbetning eller teknisk lagring för myndighetens räkning. Innebörden av teknisk bearbetning eller teknisk lagring är densamma som i 2 kap. 9 § tredje stycket tryckfrihetsförordningen (jfr 2 kap. 13 § första stycket tryckfrihetsförordningen).

Att bestämmelsen är tillämplig när en tjänsteleverantörs uppdrag är att endast tekniskt bearbeta eller tekniskt lagra uppgifter innebär att ett uppdrag som innehåller annat än enbart sådana tekniska mo-

ment faller utanför tillämpningsområdet. I situationer där en myndighet rörande uppgifter utkontrakterar uppdrag av olika karaktär till samma tjänsteleverantör, t.ex. ett uppdrag som innebär att leverantören endast tekniskt bearbetar eller tekniskt lagrar uppgifter och ett annat uppdrag som omfattar åtgärder rörande uppgifterna som går utöver detta, är lagen bara tillämplig i det förstnämnda fallet och bara på sådana uppgifter som inte dessutom hanteras inom ramen för det andra uppdraget (jfr prop. 2019/20:201, s. 22).

Bestämmelsens avgränsning innebär att den endast träffar hantering av uppgifter som tjänsteleverantören utför för myndighetens räkning. Sådan hantering av uppgifter som en tjänsteleverantör utför för egna ändamål faller utanför bestämmelsens tillämpningsområde.

Ett villkor för att utlämnande ska få ske är att de skäl som talar för att det intresse som sekretessen ska skydda har företräde framför intresset av att uppgiften lämnas ut. Detta innebär att den utlämnande myndigheten måste bedöma om intresset av sekretess för uppgifterna överväger intresset av att uppgiften lämnas ut. Vilka intressen som föranlett sekretessen, liksom med vilken styrka som sekretessen är reglerad, bör tas i beaktande i denna bedömning. Även uppgifternas art och omfattning är av relevans.

Det kan också vara av relevans vilken sekretess eller tystnadsplikt som gäller hos mottagaren för uppgifterna, och vilken styrka den sekretessen eller tystnadsplikten har. Det kan därvid ha betydelse om det är fråga om en straffsanktionerad tystnadsplikt enligt offentlighets- och sekretesslagen (2009:400) eller annan lagstiftning, eller en tystnadsplikt som följer av avtal. Det bör i sammanhanget även beaktas att det inte alltid kommer att vara möjligt att lagföra vissa utländska tjänsteleverantörer för brott mot tystnadsplikt om de röjer uppgifter i strid med lagreglerad tystnadsplikt. Detta beror på att det i enlighet med reglerna om dubbel straffbarhet i 2 kap. brottsbalken krävs att gärningen även är straffbar på gärningsorten för att svensk domstol ska vara behörig.

Hänsyn till möjligheten att lagföra ett brott mot tystnadsplikt utifrån kravet på dubbel straffbarhet kan dock bara tas i förhållande till länder utanför EU, eftersom sådana hänsyn annars skulle kunna stå i strid med EU-rättens likabehandlingsprincip.

Dataskyddsregelverket innebär i viss utsträckning en tystnadsplikt för personuppgifter som också kan vara relevant att beakta i bedömningen. Detsamma gäller förekomsten av tekniska säkerhets-

åtgärder som gör det svårare för någon obehörig att ta del av uppgifterna i klartext, som t.ex. kryptering.

44 kap.

5 §

Rätten enligt 1 kap. 1 och 7 §§ tryckfrihetsförordningen och 1 kap. 1 och 10 §§ yttrandefrihetsgrundlagen att meddela och offentliggöra uppgifter inskränks av den tystnadsplikt som följer

1. av beslut som har meddelats med stöd av 7 § lagen (1999:988) om förhör m.m. hos kommissionen för granskning av de svenska säkerhetstjänsternas författningsskyddande verksamhet,

2. av 7 kap. 1 § 1 lagen (2006:544) om kommuners och regioners åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap,

3. av 4 kap. 16 § försäkringsrörelselagen (2010:2043),

4. av 5 kap. 15 § lagen (1998:293) om utländska försäkringsgivares och tjänstepensionsinstituts verksamhet i Sverige,

5. av 32 § lagen (2020:62) om hemlig dataavläsning, och

6. av 4 § lagen (2020:914) om tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter.

Paragrafen är ändrad genom att en hänvisning till lagen om tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter lagts till.

I paragrafen föreskrivs inskränkningar i rätten att meddela och offentliggöra uppgifter. Den tystnadsplikt som följer av lagen om tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter har företräde framför rätten att meddela och offentliggöra uppgifter. Övervägandena finns i avsnitt 11.3.

Referenser

Offentligt tryck

Propositioner

Regeringens proposition 1975/76:160 *Om nya grundlagsbestämmelser om allmänna handlingars offentlighet.*

Regeringens proposition 1975/76:204 *om ändringar i grundlagsregleringen av tryckfriheten*.

Regeringens proposition 1979/80:2, Del A *med förslag till sekretesslag m.m.*

Regeringens proposition prop. 1981/82:186 *Om ändringar i sekretesslagen (1980:100)*, *m.m.*

Regeringens proposition 1995/96:129 *Säkerhetsskydd.*

Regeringens proposition 1997/98:44 *Personuppgiftslag.*

Regeringens proposition 2008/09:150 *Offentlighets- och sekretesslag.*

Regeringens proposition prop. 2016/17:198 *Utökat sekretesskydd i verksamhet för teknisk bearbetning och lagring.*

Regeringens proposition 2017/18:89 *Ett modernt och stärkt skydd för Sveriges säkerhet – ny säkerhetsskyddslag*.

Regeringens proposition 2019/20:201 *Tystnadsplikt vid utkontraktering av teknisk lagring eller teknisk bearbetning av uppgifter.*

Statens offentliga utredningar

SOU 2014:39 *Så enkelt så möjligt för så många som möjligt*. Betänkande av E-delegationen.

SOU 2015:25 *En ny säkerhetsskyddslag.* Betänkande av utredningen om en ny säkerhetsskyddslag.

SOU 2015:66 *En förvaltning som håller ihop.* Betänkande av E-delegationen.

SOU 2018:25 *Juridik som stöd för förvaltningens digitalisering.* Betänkande av Digitaliseringsrättsutredningen.

SOU 2018:82 *Kompletteringar till den nya säkerhetsskyddslagen*. Betänkande av Utredningen om vissa säkerhetsskyddsfrågor.

Departementsserien

Ds Ju 1977:1 och 11 *Handlingssekretess och tystnadsplikt*.

Rapporter, vägledningar, strategier, m.m.

Ahlström K., Offentlighets- och sekretesslag, Lexino, JUNO.

Artikel 29-gruppen (2010), *Opinion 1/2010 on the concepts of "controller" and "processor" (WP 169)*, antagen den 16 februari 2010.

Beckman m.fl., *Kommentar till brottsbalken II*, 4 uppl. 1978.

Cirio Advokatbyrå AB, *Molntjänster, offentlighet- och sekretess i offentlig sektor. Utredning om och förslag till lagstiftning rörande offentlig sektors möjligheter att använda publika molntjänster* (2020), https://cirio.se/assets/uploads/images/hero-images/Molntjanster-offentlighet-och-sekretess-i-offentlig-sektor-Cirio-12-maj-2020-002.pdf.

Computer Sweden, *Varför bemöter inte Esam och försäkringskassan huvudpunkterna i vår kritik?* (2020), https://computersweden.idg.se/2.2683/1.735508/esam-forsakringskassan-kritik.

Computer Weekly (2016) *The Problem With G-Cloud*, https://www.computerweekly.com/microscope/news/450301066/The-problem-with-G-Cloud.

Computer Weekly (2019a) *Government 'cloud-first' policy under review by CCS and GDS*, https://www.computerweekly.com/news/252463001/Government-cloud-first-policy-under-review-by-CCS-and-GDS.

Computer Weekly (2019b) *G-Cloud 11 goes live with 4,200 suppliers securing a place on the framework*, https://www.computerweekly.com/news/252466129/G-Cloud-11-goes-live-with-4200-suppliers-securing-a-place-on-the-framework.

Computer Weekly (2019c) *Competitive threats: What the growth in new public sector cloud frameworks means for G-Cloud*, https://www.computerweekly.com/feature/Competitive-threats-What-the-growth-in-new-public-sector-cloud-frameworks-means-for-G-Cloud.

Corell H. m.fl. *Sekretesslagen, Kommentar till 1980 års lag med ändringar*, Norstedts juridik, tredje uppl., Stockholm, 1991.

Digg (2019) *Myndigheters digitala mognad och it-kostnader. En enkätundersökning riktad till statliga myndigheter*, dnr 2019-469.

Difi (2018) *Innkjøpsordning/markedsplass for skytjenester (2018:6)*, https://www.difi.no/sites/difino/files/innkjopsordning-markedsplass-for-skytjenester-difi-rapport-2018-6.pdf.

Digitaliseringsstyrelsen (2016) *Den fællesoffentlige digitaliseringsstrategi 2016–2020*, https://digst.dk/strategier/digitaliseringsstrategien/.

Digitaliseringsstyrelsen (2017) *Strategi for it-styring i staten*, https://digst.dk/strategier/strategi-for-it-styring-i-staten/.

Digitaliseringsstyrelsen (2018) *National strategi for cyber- og informationssikkerhed 2018–2021*, https://digst.dk/strategier/cyber-og-informationssikkerhed/.

Digitaliseringsstyrelsen (2019) *Vejledning til anvendelse af cloud*, https://digst.dk/media/21070/vejledning-i-anvendelse-af-cloudservices-v1-tilgaengelig.pdf.

E-delegationen (2012) *Effektiv IT-drift inom staten. Förstudie*, 2012-04-27.

E-delegationen (2015) *Sekretess vid outsourcing – en förstudie*, Fi 2009:01/2015/4.

eSam (2020), *Kommentar till kritisk rapport om molntjänster i offentlig sektor*, https://www.esamverka.se/aktuellt/nyheter/nyheter/2020-05-26-kommentar-till---kritisk-rapport-om-molntjanster-i-offentlig-sektor.html.

eSam (2018), *Rättsligt utlåtande om röjande och molntjänster*, (VER 2018:57), https://www.esamverka.se/download/18.1d126bc174ad1e6c39c4db/1576749838091/Outsoursing 2.0 sekretess och dataskydd 2019.pdf

eSam (2015), *Röjandebegreppet enligt offentlighets- och sekretesslagen*, VER 2015-190.

eSam (2019), *Outsourcing 2.0 En vägledning om sekretess och dataskydd.*

EDPB (2020), *Guidelines 2/2020 on articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies*, antagna den 18 januari 2020.

EDPB (2020), *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*, antagna den 10 november 2020.

EDPB (2020), *Recommendations 02/2020 on the European Essential Guarantees for surveillance measures*, antagna den 10 november 2020.

ESV (2015) *Fördjupat it-kostnadsuppdrag. Delrapport 2 Kartläggning av it-kostnader*, Dnr 139/2015, 2015-10-23.

ESV (2017) *Myndigheters strategiska it-projekt och it-kostnader,*

Delrapport it-användningsuppdraget, P-2017-77, 2017-12-21.

ESV (2018a) *Myndigheters strategiska it-projekt, it-kostnader och mognad*, ESV 2018:30, Dnr: 2017-01701, 2018-03-14.

ESV (2018b) *Pilotprojekt om ramverk för it-kostnader (TBM)*, 2018:28, 2018-03-15.

EU-deklaration om molntjänster (2020) *Member States Joint Declaration on Cloud*, undertecknad den 15 oktober 2020 av medlemsländernas telekomministrar.

EU-kommissionen (2020) *EU:s datastrategi*, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593073685620&uri=CELEX%3A52020DC0066.

Finlands finansutskott (2012) *betänkande FiUB 12/2012 rd*, https://www.eduskunta.fi/SV/vaski/Mietinto/Documents/fiub_12+2012.pdf.

Finlands regering (2011a) *regeringsprogram,* https://vnk.fi/julkaisu?pubid=3605.

Finlands regering (2011b) *Ett produktivt och nyskapande Finland – Digital agenda för åren 2011–2020,* https://www.lvm.fi/sv/-/utveckling-av-informationssamhallet-hojer-produktiviteten-781229.

Finlands regering (2016) *Projektet för att koncentrera statsförvaltningens branschoberoende informations- och kommunikationstekniska (IKT) uppgifter (TORI)*, https://web.archive.org/web/20160911022733/https://vm.fi/sv/projektet-for-att-koncentrera-statsforvaltningens-branschoberoende-ikt-uppgifter-tori-.

Finlands regering (2019a) *regeringsprogram*, https://valtioneuvosto.fi/sv/marin/regeringsprogrammet/varldens-basta-offentliga-forvaltning.

Finlands regering (2019b) *Pressmeddelande: Halvtidsrapport om den externa utvärderingen av Palkeet och Valtori färdig*, https://vm.fi/-/palkeiden-ja-valtorin-ulkopuolisen-arvioinnin-valiraportti-on-valmistunut?languageId=sv_SE.

Finland's Cyber Security Strategy (2019) https://turvallisuuskomitea.fi/en/finlands-cyber-security-strategy-2019/.

Försäkringskassan (2019), Vitbok Molntjänster i samhällsbärande verksamhet – risker, lämplighet och vägen framåt, Dnr 013428-2019.

GAIA-X (2020) *A Federated Data Infrastructure for Europe*, https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html.

Government Digital Services (2019a) *Cloud First is here to stay*, https://technology.blog.gov.uk/2019/10/31/cloud-first-is-here-to-stay/.

Government Digital Services (2019b) *Cloud guide for the public sector*, https://www.gov.uk/government/publications/cloud-guide-for-the-public-sector/cloud-guide-for-the-public-sector.

Johansson S. m.fl. Brottsbalken m.m., Norstedts Juridik, JUNO.

Kammarkollegiet (2019), *Förstudierapport webbaserat kontorsstöd*, Dnr 23.2-6283-18.

Lenberg E. m.fl., Offentlighets- och sekretesslag, Nordstedts Juridik, JUNO.

Livsmedelsverkets remissyttrande över E-delegationens betänkande En förvaltning som håller ihop (SOU 2015:55), 2015-12-14, dnr 2015/07920.

McKinsey & Company (2019) *Defining a public-cloud strategy: An interview with Michael Ørnø, of Denmark's Statens IT*, https://www.mckinsey.com/industries/public-and-social-sector/our-insights/defining-a-public-cloud-strategy-an-interview-with-michael-orno-of-denmarks-statens-it.

Microsoft, *Molntjänster och säkerhet* (2018), https://news.microsoft.com/sv-se/2018/12/13/molntjanster-och-sakerhet/.

MSB (2014) *Outsourcing av it-tjänster i kommuner*, MSB728 – Augusti 2014.

MSB (2015) *Informationssäkerhet trender 2015*, MSB779 – januari 2015.

MSB och Örebro universitet (2018) *Säkerhet vid molnlösningar*, MSB1196 – maj 2018.

MSB (2018) *Upphandla informationssäkert: en vägledning*, MSB1177 – november 2018.

MSB (2019) *Vägledning för identifiering av samhällsviktig verksamhet*, MSB1408 – juni 2019.Nederländernas regering (2011a) *brev från Inrikesdepartementet till parlamentet*, https://zoek.officielebekendmakingen.nl/kst-26643-179.html.

Nederländernas regering (2011b) *The Central Government Reform Programme*, https://zoek.officielebekendmakingen.nl/kst-31490-54.html.

Nederländernas regering (2016) *Strategische i-agenda Rijksdienst 2016–2017.*

Nederländernas regering (2018a) *Digital Government Agenda*, https://www.nldigitalgovernment.nl/digital-government-agenda/.

Nederländernas regering (2018b) *National Cybersecurity Agenda*, https://english.ncsc.nl/topics/national-cybersecurity-agenda/documents/publications/2019/juni/01/national-cyber-security-agenda.

Nederländernas regeringen (2018c) *Brev från Inrikesdepartementet till representanthuset om att utarbeta åtgärder för att öka informationssäkerheten i statsförvaltningen*, https://www.rijksoverheid.nl/documenten/kamerstukken/2018/10/16/kamerbrief-over-verhogen-informatieveiligheid-bij-de-overheid.

Nederländernas regering (2018d) *Konsekvensbedömning av Microsoft Office (Data Protection Impact Assessment op Microsoft Office)*, https://www.rijksoverheid.nl/documenten/rapporten/2018/11/07/data-protection-impact-assessment-op-microsoft-office.

Nederländernas regering (2019a) *Data Agenda Government*, https://www.nldigitalgovernment.nl/document/data-agenda-government/.

Nederländernas regeringen (2019b) *Säkerhetstjänstens undersökning av molntjänsters säkerhet och förslag till vägledning (Verkenning Cloudbeleid voor de Nederlandse Rijksdienst).*

Nexia Management Consulting (2015) *Kartlegging og analyse av landskapet for offentlige datasenter i Norge*.

Norska regeringen (2016a) *Digital agenda for Norge — IKT for en enklere hverdag og økt produktivitet*, Meld. St. 27 (2015–2016), https://www.regjeringen.no/no/dokumenter/meld.-st.-27-20152016/id2483795/.

Norska regeringen (2016b) *Nasjonal strategi for bruk av skytenester*, https://www.regjeringen.no/no/dokumenter/nasjonal-strategi-for-bruk-av-skytenester/id2484403/.

Norska regeringen (2016c) *En digital offentlig sektor: Digitaliseringsstrategi for offentlig sektor 2019–2025*, https://www.regjeringen.no/no/tema/statlig-forvaltning/ikt-politikk/digitaliseringsstrategi-for-offentlig-sektor/id2612415/.

Norska regeringen (2016d) *Nasjonal strategi for digital sikkerhet*, https://www.regjeringen.no/no/dokumenter/nasjonal-strategi-for-digital-sikkerhet/id2627177/.

NOU 2015:13 *Digital sårbarhet – sikkert samfunn — Beskytte enkeltmennesker og samfunn i en digitalisert verden*, https://www.regjeringen.no/no/dokumenter/nou-2015-13/id2464370/.

OECD (2005) *Government Review of Norway.*

OECD (2017) *Government Review of Norway.*

Open Source Observatory (2017) *Open source makes Dutch government cloud a reality*, https://joinup.ec.europa.eu/collection/open-source-observatory-osor/document/open-source-makes-dutch-government-cloud-reality.

Paagman A. m.fl. (2015). *An integrative literature review and empirical validation of motives for introducing shared services in government organizations*, i International Journal of Information Management, 35(1), s. 110–123.

Pensionsmyndigheten (2015) *Molntjänster i staten. En ny generation av outsourcing*, Dnr VER 2015-157.

Public Technology (2018) *Crown Hosting CEO: We have taken away all the cloud excuses*, https://www.publictechnology.net/articles/features/crown-hosting-ceo-'we-have-taken-away-all-cloud-excuses'.

Riksrevisionen i Nederländerna (2019) *Staat van de rijksverantwoording 2019*, https://www.rekenkamer.nl/publicaties/rapporten/2020/05/20/staat-van-de-rijksverantwoording-2019.

Roos M-A., Brottsbalken, Karnov, JUNO.

SSC (2015), *En förvaltningsgemensam tjänst för e-arkiv – delrapport*, Dnr 10444-2014/1221.

SSC (2017) *En gemensam statlig molntjänst för myndigheternas it-drift. Delrapport i regeringsuppdrag om samordning och omlokalisering av myndighetsfunktioner*, 2017-01-30, Dnr 10052-2016/1121.

Statens Revisionsverk (2019) *Centraliserade ICT-tjänster och -anskaffningar*, https://www.vtv.fi/sv/publikationer/centraliserade-ict-tjanster-och-anskaffningar/.

Storbritanniens regering (2011) *Policy paper från Cabitnet Office, "Data Centre Consolidation"*, https://www.gov.uk/government/publications/data-centre-consolidation.

Storbritanniens regering (2011a) *Government ICT Strategy*, https://www.gov.uk/government/publications/uk-government-ict-strategy-resources.

Storbritanniens regering (2011b) *Government Cloud Strategy: A sub strategy of the Government ICT Strategy*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/266214/government-cloud-strategy_0.pdf.

Storbritanniens regering (2012) *Government Digital Strategy*, https://www.gov.uk/government/publications/government-digital-strategy.

Storbritanniens regering (2013a) *Presentation från Cabinet Office om G-Cloud för EU-parlamentet, "UK's G-Cloud Project"*, https://www.europarl.europa.eu/cmsdata/61100/att_20130514ATT66093-3134663336091827431.pdf.

Storbritanniens regering (2013b) *Government Cloud First Policy*, https://www.gov.uk/guidance/government-cloud-first-policy.

Storbritanniens regering (2016) *National Cyber Security Strategy*, https://www.gov.uk/government/publications/government-digital-strategy.

Storbritanniens regering (2017a) *Government Transformation Strategy*, https://www.gov.uk/government/publications/government-transformation-strategy-2017-to-2020.

Storbritanniens regering (2017b) *UK Digital Strategy*, https://www.gov.uk/government/publications/uk-digital-strategy/uk-digital-strategy.

Storbritanniens regering (2019a) *Technology Code of Practice*, https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice.

Storbritanniens regering (2019b) *G-Cloud buyers' guide*, https://www.gov.uk/guidance/g-cloud-buyers-guide.

Storbritanniens regering (2019c) *G-Cloud framework sales (up to 31 December 2018)*, https://www.gov.uk/government/statistical-data-sets/g-cloud-framework-sales-up-to-31-december-2018.

Storbritanniens regering (2019d) *The Crown Hosting Data Centres framework on the Digital Marketplace*, https://www.gov.uk/guidance/the-crown-hosting-data-centres-framework-on-the-digital-marketplace#the-crown-hosting-data-centres-framework.

Storbritanniens regering (2019e) *How the Home Office's Immigration Technology department reduced its cloud costs by 40 %*, https://www.gov.uk/government/case-studies/how-the-home-offices-immigration-technology-department-reduced-its-cloud-costs-by-40.

Säkerhetspolisen (2019), *Vägledning i säkerhetsskydd Introduktion om säkerhetsskydd – juni 2019.*

Säkerhetspolisen (2019), *Vägledning i säkerhetsskydd Säkerhetsskyddad upphandling – juni 2019*.

Säkerhetspolisen (2020), *Vägledning i säkerhetsskydd Informationssäkerhet – september 2020*.

Transportstyrelsen (2018), *Kartlägga hanteringen av vissa uppgifter Till regeringen*, 2018-01-23, Dnr TSG 2017-2515.

Transportstyrelsens remissyttrande över E-delegationens betänkande En förvaltning som håller ihop (SOU 2015:66) 2015-12-14, dnr TSG 2015-1422.

Voister, *Esam om Cloud Act kritik* (2019), https://www.voister.se/artikel/2019/07/esam-om-cloud-act-kritik/.

Rättsfall

Europadomstolen

Airey mot Irland, nr 6289/73, dom meddelad den 9 oktober 1979.

X och Y mot Nederländerna, nr 8978/80, dom meddelad den 26 mars 1985.

K.U. mot Finland, nr 2872/02, dom meddelad den 2 december 2008.

Söderman mot Sverige, nr 5786/08, dom meddelad den 12 november 2013.

EU-domstolen

Dom av den 20 maj 2003, *Österreichischer Rundfunk m.fl.*, C-465/00, C-138/01 och C-139/01, EU:C:2003:294.

Dom av den 6 november 2003, *Lindqvist*, C-101/01, EU:C:2003:596.

Dom av den 16 december 2008, *Satakunnan Markkinapörssi och Satamedia*, C-73/07, EU:C:2008:727.

Dom av den 9 november 2010, *Volker und Markus Schecke och Eifert*, C-92/09 och C-93/09, EU:C:2010:662.

Dom av den 8 april 2014, *Digital Rights Ireland och Seitlinger m.fl.*, C-293/12, EU:C:2014:238.

Dom av den 13 maj 2014, *Google Spain och Google*, C-131/12, EU:C:2014:317.

Dom av den 6 oktober 2015, *Schrems*, C-362/14, EU:C:2015:650.

Dom av den 21 december 2016, *Tele2 Sverige*, C-203/15, EU:C:2016:970.

Dom av den 5 juni 2018, *Wirtschaftsakademie Schleswig-Holstein*, C-210/16, EU:C:2018:388.

Dom av den 16 juli 2020, *Facebook Ireland och Schrems*, C-311/18, EU:C:2020:559.

Svenska domstolar

NJA 1953 s. 654.

NJA 1991 s. 103.

NJA 2015 s. 180.

NJA 2015 s. 624.

HFD 2014 ref. 66.

HFD 2019 ref. 24.

RÅ 2002 ref. 54.

Arbetsdomstolens dom nr 15/19, mål nr AD 152/17, meddelad den 6 mars 2019.

Beslut från Riksdagens ombudsmän

JO 1982/83:JO1 s. 138, dnr 149-1980.

JO 1984/85:JO1 s. 265, dnr 2616-1983.

JO 1992/93:JO1 s. 197, dnr 145-90.

JO 1994/95:JO1 s. 574, dnr 2079-1993.

JO 2009/10:JO1 s. 194, dnr 4150-2007.

JO:s beslut den 9 september 2014, dnr 3032-2011.

Kommittédirektiv 2019:64

Säker och kostnadseffektiv it-drift för den offentliga förvaltningen

Beslut vid regeringssammanträde den 26 september 2019

Sammanfattning

En särskild utredare ska kartlägga och analysera statliga myndigheters behov av säker och kostnadseffektiv it-drift samt hur dessa behov tillgodoses. Utredaren ska vidare analysera säkerhetsmässiga och rättsliga förutsättningar för samordnad statlig it-drift och lämna förslag på mer: varaktiga former för sådan it-drift, om det bedöms lämpligt ur ett säkerhetsperspektiv, och de författningsförslag som detta kräver. Utredaren ska också analysera de rättsliga förutsättningarna för statliga myndigheter, kommuner och landsting att med bibehållen säkerhet utkontraktera it-drift till privata leverantörer och vid behov lämna författningsförslag. Syftet med utredningen är att skapa bättre förutsättningar för den offentliga förvaltningen att få tillgång till säker och kostnadseffektiv it-drift genom antingen samordnad statlig it-drift eller tydligare rättsliga förutsättningar för att kunna anlita privata leverantörer av it-drift.

Uppdragen att kartlägga och analysera statliga myndigheters it-drift och den offentliga förvaltningens rättsliga förutsättningar för utkontraktering med bibehållen säkerhet, inklusive eventuella författningsförslag, ska redovisas senast den 31 augusti 2020. Uppdraget att föreslå mer varaktiga former för samordnad statlig it-drift ska redovisas senast den 31 maj 2021.

Bakgrund

It-drift i den offentliga förvaltningen

Begreppet it-drift har ingen tydlig avgränsning utan omfattar både fysisk hårdvara som servrar och datorer, och mjukvara som datorprogram och operativsystem. Digitalisering och it skapar förutsättningar för en rättssäker och effektiv verksamhet och leverans av god service till enskilda. Eftersom myndigheter ofta hanterar uppgifter som omfattas av sekretess eller är av integritetskänsligt slag ställs särskilda krav på myndigheternas it-verksamhet. It-driften inom den offentliga förvaltningen ska också uppfylla krav på säkerhetsskydd och informationssäkerhet.

It-drift i egen regi

Motiven för en myndighet att hantera sin it-drift i egen regi kan variera. I en del fall handlar det om att få kontroll över systemen och tätare kontakt mellan verksamheten och systemdriften. I andra fall kan det finnas säkerhetsmässiga fördelar, t.ex. att slippa kommunicera över öppna nätverk för att nå en tjänst. Säkerhetsmässigt kan det också vara enklare att integrera ett system i en myndighets befintliga it-miljö med de administrativa och tekniska säkerhetslösningar som redan används. Men it-drift i egen regi kan också medföra begränsningar. Det kan röra sig om låg skalbarhet, dvs. svårigheter att förändra kapacitetsutnyttjandet, låg potential för utveckling och sämre utbud av möjliga säkerhetslösningar. En myndighet med it-drift i egen regi kan också gå miste om stordriftsfördelar som kan följa av samordning eller utkontraktering av it-drift.

Samordnad it-drift

Ett alternativ till utkontraktering är att en myndighet får i uppdrag att helt eller delvis hantera it-drift åt en annan myndighet, s.k. samordnad it-drift. Exempel på sådan samordning är att Skatteverket hanterar it-driften åt bl.a. Kronofogdemyndigheten och Valmyndigheten och att Länsstyrelsen i Västra Götaland samordnar it-driften för samtliga länsstyrelser.

Ett annat exempel på samordnad it-drift är Försäkringskassans tidsbegränsade uppdrag att tillhandahålla samordnad och säker it-drift för vissa statliga myndigheter. Syftet med uppdraget är att pröva och utvärdera former för samordnad it-drift inom staten. Intresset för att ansluta sig till Försäkringskassans tjänster har varit stort bland de statliga myndigheterna, och Försäkringskassans uppfattning är att behovet av ett totalåtagande är omfattande och angeläget (dnr Fi2017 /03257 /DF). Detta stärker uppfattningen i tidigare rapporter, dvs. att det finns ett stort intresse för samordnad it-drift bland statliga myndigheter (se bl.a. Statens servicecenter, En gemensam statlig molntjänst för myndigheternas it-drift, dnr Fi2016/00274/SFÖ). Samordnad it-drift skulle också kunna ge bättre förutsättningar för sådan samverkan mellan myndigheter som syftar till att utveckla och erbjuda gemensamma digitala tjänster till medborgare och företag.

Vid samordnad it-drift är det viktigt att poängtera att en myndighet alltid är ytterst ansvarig för att den information som lämnas ut får ett effektivt och ändamålsenligt skydd och i övrigt hanteras i enlighet med gällande rätt. Risker med bl.a. centralisering av flera myndigheters information behöver också beaktas.

Utkontrakterad it-drift

Begreppet utkontraktering används ofta för att beskriva när en verksamhetsutövare lägger ut drift, underhåll, skötsel eller liknande av en viss del av verksamheten till en utomstående leverantör. Utkontraktering har ingen legal definition och innebär inte heller någon tydlig avgränsning mellan olika organisatoriska enheter. Med utkontraktering av it-drift avses i dessa direktiv att en myndighet genom offentlig upphandling eller på något annat sätt uppdrar åt en privat leverantör att hantera hela eller delar av myndighetens it-drift.

Det kan finnas flera bakomliggande motiv till utkontraktering av it-drift. Det kan t.ex. röra sig om effektivitets- och besparingsskäl, men även att myndigheten vill dra nytta av säkerhetslösningar, expertkompetens, innovationer eller annan teknisk utveckling hos privata leverantörer. Även om utkontraktering av it-drift kan innebära fördelar för en myndighet, kan det också innebära säkerhetsrisker. Privata leverantörers affärsmodeller är ofta komplexa vilket kan göra dem svåra att överblicka och förstå. Det förekommer också att underleve-

rantörer anlitas eller byts ut, att uppgiftsmängder hanteras utanför Sveriges gränser och att avtalsförhållandena är komplicerade. I sammanhanget är det viktigt att poängtera att en myndighet aldrig genom utkontraktering kan undandra sig sitt ansvar utan är ytterst ansvarig för att den information som lämnas ut får ett effektivt och ändamålsenligt skydd och i övrigt hanteras i enlighet med gällande rätt.

Säkerhetspolisen har framhållit att utkontraktering kan leda till att den mängd information som samlas hos en leverantör medför att leverantörens verksamhet sammantaget är av stor betydelse för Sveriges säkerhet. Säkerhetspolisen har också konstaterat att leverantören riskerar att bli ett attraktivt mål för bl.a. andra länders underrättelseinhämtning (Säkerhetspolisens årsbok 2017). Sådan centralisering, där flera myndigheters information samlas hos en leverantör, innebär en ökad riskexponering bl.a. för känsliga uppgifter. Samtidigt kan utkontraktering innebära att en myndighets informationstillgångar får ett bättre tekniskt och administrativt skydd än vad som skulle varit fallet om myndigheten hanterat sin it-drift i egen regi.

Rättsliga förutsättningar och säkerhet

Oavsett hur en myndighet väljer att anordna sin it-drift ställs den inför en mängd komplexa rättsliga frågor som måste hanteras. Vid utkontraktering kan myndigheten dessutom behöva ta ställning till vilka eventuella rättsliga konsekvenser den allt mer globaliserade marknaden får för hanteringen av myndighetens information, t.ex. om myndighetens informationstillgångar kommer att exponeras för andra staters rättsordningar och lättare bli åtkomliga för utländska myndigheter och organisationer eller andra aktörer.

Upphandling och avtal

Rätt använt är offentlig upphandling och avtalsförvaltning nyckelfaktorer som ger en myndighet goda förutsättningar att ta del av marknadens it-driftstjänster på ett kostnadseffektivt och juridiskt hållbart sätt (se t.ex. Nationella upphandlingsstrategin). På motsatt sätt kan t.ex. en icke strategisk upphandling av it-drift medföra oönskade och långdragna konsekvenser i form av inlåsningseffekter, leverantörsberoende, oförutsedda kostnader och obalanserade avtals-

villkor. Det ställs således höga krav på en myndighets verksamhets- och beställarkompetens samt förmåga att formulera ändamålsenliga avtalsvillkor och följa upp leverantörens hantering av de utkontrakterade tjänsterna. Upphandlingsmyndigheten tillhandahåller stöd och vägledning för upphandling och avtalsförvaltning (se bl.a. Avtalsförvaltning, vägledning nr 2, 2016). MSB har tagit fram en vägledning för att upphandla informationssäkert (MSB1177, november 2018).

Sekretess och dataskydd

En förutsättning för att en myndighet ska kunna samordna sin it-drift med en annan myndighets eller utkontraktera den är att bestämmelser om sekretess och dataskydd inte hindrar att uppgifter lämnas ut till och behandlas av den mottagande myndigheten eller leverantören.

Bland myndigheterna råder i dag en viss osäkerhet i fråga om de rättsliga förutsättningarna för utkontraktering. Det gäller främst tolkningen av när en uppgift ska anses röjd enligt sekretesslagstiftningen, något som bl.a. kommit till uttryck i eSamverkansprogrammets rättsliga uttalanden om röjande och molntjänster och om röjandebegreppet enligt offentlighets- och sekretesslagen (VER 2018:57 och VER 2015:90). I Digitaliseringsrättsutredningens slutbetänkande uttrycks att det finns en oro över att uppgifter som lämnas ut till en privat leverantör kan komma att röjas i strid med sekretesslagstiftningen (SOU 2018:25 s. 106). Denna oro har förstärkts det senaste året till följ av att den amerikanska rättsakten The Clarifying Lawful Overseas Use of Data Act (CLOUD Act) trädde i kraft under våren 2018. CLOUD Act syftar bl.a. till att förenkla för amerikanska rättsvårdande myndigheter att få tillgång till vissa uppgifter som finns lagrade hos leverantörer som omfattas av den amerikanska jurisdiktionen, oavsett var uppgifterna finns rent geografiskt.

Om ett uppgiftsutlämnande inkluderar personuppgifter, behöver den utkontrakterande myndigheten också säkerställa att den behandling av personuppgifter som kommer att utföras är förenlig med dataskyddsregleringen. Här avses främst Europaparlamentets och rådets förordning (EU) 2016 / 679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) samt lagen (2018:218)

med kompletterande bestämmelser till EU:s dataskyddsförordning. Även myndighets- eller sektorsspecifika registerförfattningar kan aktualiseras.

En särskild utmaning för en utkontrakterande myndighet kan vara att bedöma om leverantören kan ge tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder så att behandlingen uppfyller kraven i dataskyddsförordningen, att den registrerades rättigheter skyddas och att uppgifter inte olovligen förs över till ett tredjeland, dvs. ett land utanför EU- och EES-området.

Säkerhetsskydd

Den som till någon del bedriver verksamhet som är av betydelse för Sveriges säkerhet eller omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd (säkerhetskänslig verksamhet) omfattas av säkerhetsskyddslagen (2018:585) och de bestämmelser i förordning och föreskrifter som kompletterar lagen. Med säkerhetsskydd avses skydd av säkerhetskänslig verksamhet mot spionerі, sabotage, terroristbrott och andra brott som kan hota verksamheten samt skydd i andra fall av säkerhetsskyddsklassificerade uppgifter. Enligt säkerhetsskyddslagstiftningen gäller särskilda krav om en statlig myndighet avser att ge en leverantör tillgång till eller möjlighet att förvara säkerhetsskyddsklassificerade uppgifter av visst slag utanför myndighetens lokaler eller om leverantören kan få tillgång till vissa typer av säkerhetskänsliga informationssystem utanför myndighetens lokaler. En myndighet som t.ex. avser att utkontraktera hela eller delar av sin it-drift ska identifiera och dokumentera vilka uppgifter eller informationssystem som leverantören kan få del av och som kräver säkerhetsskydd och samråda med den berörda tillsynsmyndigheten innan ett sådant förfarande inleds. Tillsynsmyndigheten får förelägga myndigheten att vidta säkerhetshöjande åtgärder och ytterst besluta att myndigheten inte får genomföra utkontrakteringen. I betänkandet Kompletteringar till den nya säkerhetsskyddslagen (SOU 2018:82) föreslås bl.a. att denna reglering ska utökas och träffa alla aktörer som omfattas av lagen samt att tillsynsmyndigheterna ska ges utökade befogenheter. Betänkandet bereds för närvarande inom Regeringskansliet.

Informations- och cybersäkerhet

Det finns stora mängder information och it-system som är av avgörande betydelse för samhällets funktionalitet och säkerhet eller som innehåller integritetskänsliga uppgifter. Om känslig information förloras, stjäls, manipuleras eller sprids till obehöriga kan det få allvarliga följder, se Nationell strategi för samhällets informations- och cybersäkerhet, skr. 2016/17:213 med en senare kompletterande bilaga: Uppdatering om genomförandet av Nationell strategi för samhällets informations- och cybersäkerhet. Likaså kan störningar i funktionaliteten hos it-system få allvarliga följder för samhällsviktig verksamhet. Den som ansvarar för ett it-system måste utgå från att attacker kan riktas mot såväl systemets funktionalitet som den information som hanteras. Informationssäkerhet måste därför vara en självklar och integrerad del i allt arbete på alla nivåer. Säkerhetsåtgärder syftar till att skapa en mer robust informationshantering vid samhällets normaltillstånd och att hantera mer allvarliga störningar, kriser under höjd beredskap och ytterst krig.

En myndighet som står inför valet att samordna sin it-drift med en annan myndighets eller utkontraktera måste säkerställa att den information som kommer att lämnas ut är tillräckligt skyddad hos mottagaren och att kraven på tillgänglighet och funktionalitet uppfylls. Vid en bedömning av säkerhetsrisker behöver myndigheten bl.a. beakta riskerna med en allt högre grad av centralisering av den offentliga förvaltningens it-drift och informationstillgångar. Centralisering kan medföra att leverantören blir ett attraktivt mål för antagonistiska attacker (Informationssäkerhet – trender MSB779, januari 2015). Centraliserad it-drift kan också innebära risk för bredare skadeverkningar vid lyckade attacker mot systemfunktionalitet eller information.

Trots riskbilden kan samordnad it-drift eller utkontraktering ge bättre förutsättningar för samhällets informations- och cybersäkerhet. Samordnad drift kan t.ex. förenkla införandet av enhetliga säkerhetsnivåer och ge utökade möjligheter till kontroll och uppföljning. Därtill skulle svåråtkomlig kompetens kunna utnyttjas på ett mer effektivt sätt. Samordnad it-drift kan också underlätta införande och användning av andra gemensamma tjänster och metoder som kan resultera i ökad informations- och cybersäkerhet i samhället.

Uppdraget att kartlägga och analysera statliga myndigheters it-drift

Statliga myndigheters behov av säker och kostnadseffektiv it-drift

Det saknas en heltäckande bild av statliga myndigheters behov av säker och kostnadseffektiv it-drift och hur behoven tillgodoses i dagsläget. En konsekvens av detta är att det inte heller finns en klar kostnadsbild över statsförvaltningens sammanlagda utgifter för it-drift. Det saknas också övergripande analyser av vilka ekonomiska, rättsliga, säkerhetsmässiga och övriga konsekvenser samordning respektive utkontraktering av it-drift lede till för varje enskild myndighet och för den statliga förvaltningen som helhet i förhållande till it-drift i egen regi.

I syfte att klarlägga statliga myndigheters behov och hantering av säker och kostnadseffektiv it-drift behöver dessa frågor kartläggas och analyseras. Kartläggningen ska omfatta ett representativt urval av statliga myndigheter, försvarsmyndigheterna och Säkerhetspolisen undantagna. Kriterier som ska beaktas vid urvalet av de myndigheter som ska ingå i kartläggningen är bl.a. att de ska ha olika storlek och finansieringsform samt ha uppgifter inom olika verksamhetsområden. Kartläggningen ska klargöra hur de utvalda myndigheterna hanterar sin nuvarande it-drift, vilka specifika och prioriterade behov myndigheterna har av att samordna eller utkontraktera it-drift samt vilka behov myndigheterna bedömer sig ha över de kommande åren. De kartlagda myndigheternas kostnader för it-drift ska redovisas. I denna del kan utredaren bl.a. ta utgångspunkt i Ekonomistyrningsverkets rapporter inom ramen för it-användningsuppdraget (se bl.a. ESV 2018:30). Där det finns relevanta jämförelseobjekt och avtal ska en jämförelse göras mellan kostnaderna för it-drift i egen regi och utkontraktering i förhållande till samordning av it-drift.

Det behöver också kartläggas i vilken utsträckning it-drift i egen regi och samordning respektive utkontraktering av it-drift kan svara mot de statliga myndigheternas behov av och krav på it-drift och andra närliggande tjänster. I detta sammanhang är det särskilt relevant att undersöka och jämföra i vilken utsträckning de olika it-driftsformerna förmår leva upp till rättsliga och säkerhetsmässiga krav, t.ex. krav på säkerhetsskydd och informationssäkerhet samt sekretess och skyddet för den personliga integriteten. Vidare ska utredaren, oavsett myndigheternas val av driftsform, kartlägga myndigheternas beställarkompetens och förmåga att identifiera vilka säkerhetskrav

som ska ställas på it-drift. Utredaren ska också kartlägga myndigheternas förmåga att identifiera risker för inlåsningseffekter och möjlighet att dra nytta av teknisk innovation.

Den efterföljande analysen ska svara på vilka huvudsakliga behov olika typer av myndigheter har av samordning eller utkontraktering av sin it-drift. Det kan t.ex. röra sig om i vilken utsträckning myndigheter har behov av ett helhetsåtagande för drift och förvaltning respektive mer specifika åtaganden, t.ex. drift av särskilt krävande digitala tjänster som kräver viss expertkompetens. Det kan också röra sig om behov av att utkontraktera annan närliggande verksamhet såsom stöd vid utveckling och teknisk utrustning. Om behoven skiljer sig åt exempelvis för myndigheter av olika storlek eller inom olika sektorer, ska dessa redovisas. Analysen ska också redogöra för för- och nackdelar av olika driftsformer samt jämföra kostnadsbilden för samordning respektive utkontraktering av it-drift jämfört med it-drift i egen regi. För att tydligare redovisa de kartlagda myndigheternas sammanlagda utgifter för it-drift ska de kostnader som kvarstår på myndigheterna vid utkontraktering av it-drift framgå av kostnadsbilden. Eftersom myndigheterna bär det yttersta ansvaret även vid utkontrakterad it-drift ska även kostnader för att upprätthålla ändamålsenlig kompetens på myndigheterna beaktas.

Vidare ska analysen belysa eventuella skillnader samt för- och nackdelar vid samordnad-it-drift med andra statliga myndigheter jämfört med utkontraktering till en privat leverantör. Det kan exempelvis gälla kvalitet, kontinuitet riskhantering, säkerhet, skalbarhet, flexibilitet, transparens eller möjlighet at dra nytta av teknisk utveckling och digital innovation.

Utredaren ska därför

- kartlägga och analysera statliga myndigheters behov av säker och kostnadseffektiv it-drift, hur behoven är tillgodosedda och kostnaderna för dessa,
- kartlägga och analysera i vilken utsträckning olika it-driftsformer – i egen regi, samordning respektive utkontraktering – kan svara mot statliga myndigheters behov av och krav på it-drift, samt vilka förutsättningar myndigheter har för ändamålsenlig kravställning inom området, och

- analysera vilka behov av it-drift och närliggande tjänster hos statliga myndigheter, respektive olika verksamhetshetssektorer, som utifrån behovsanalysen är mest prioriterade att tillgodose.

Samordnad it-drift - omvärldsanalys

Det finns mycket att lära både av hur man nationellt och i andra länder har valt att hantera frågor om samordnad statlig it-drift och offentlig-privat samverkan kring it-drift. Dessa erfarenheter behöver kartläggas och analyseras för att det ska gå att bättre förstå vilka alternativ som står till buds och hur de olika lösningarna står sig mot varandra utifrån bl.a. säkerhet och kostnadseffektivitet, samt vilka utmaningar och problem de olika länderna har stött på. Finland har genomfört en större reform genom ökad centralisering och övergång till samordnad statlig it-drift genom myndigheten Valtori. Även Danmark och Norge har erfarenheter av samordnad statlig it-drift. Utanför Norden finns flera intressanta och relevanta exempel på såväl samordnad statlig it-drift som offentlig-privat samverkan kring molntjänster och it-drift. Tyskland har infört en lösning med en statlig molntjänst som hanterar it-drift för flera centrala myndigheter frikopplat från internet. Storbritannien har genom en gemensam molntjänstportal valt att samordna utkontraktering till kommersiella molntjänstleverantörer. I Sverige finns flera exempel på samordnad statlig it-drift som bör analyseras, t.ex. Skatteverkets hantering av it-drift åt Kronofogdemyndigheten och Valmyndigheten samt länsstyrelsernas samordnade it-drift. De lärdomar som dragits nationellt och i andra länder av samordnad statlig it-drift bör tas till vara och utgöra en del av underlaget inför förslag om inriktning för en mer varaktig form av samordnad statlig it-drift i Sverige.

Utredaren ska därför

- kartlägga och analysera relevanta modeller för myndigheters it-drift såväl nationellt som i ett urval av särskilt intressanta länder med såväl samordnad statlig it-drift som offentlig-privat samverkan kring samordnad it-drift.

Uppdraget att föreslå mer varaktiga former för samordnad statlig it-drift

Försäkringskassans uppdrag om samordnad och säker statlig it-drift

De erfarenheter och den kompetens Försäkringskassan har byggt upp inom ramen för sitt uppdrag att tillhandahålla samordnad och säker statlig it-drift behöver tas till vara i det fortsatta arbetet att föreslå samordnad statlig it-drift. Försäkringskassans uppdrag behöver därför utvärderas och analyseras. Utredaren ska bl.a. redovisa hur Försäkringskassan byggt upp sin organisation kring de tjänster som tillhandahålls, för- och nackdelar med finansieringsmodell, hur anslutningsprocesserna med kundmyndigheterna har fortlöpt och om uppdraget i övrigt föranlett några särskilda utmaningar t.ex. när det gäller informationssäkerhet, säkerhetsskydd eller kund- och avtalsförvaltning. Utvärderingen ska innehålla en analys av vilka eventuella samordningsvinster och andra nyttor, t.ex. kostnadseffektivitet, ökad säkerhet, flexibilitet och skalfördelar, som kan uppnås vid samordnad statlig it-drift, i jämförelse med it-drift i egen regi respektive utkontraktering. Utredaren ska också redovisa vilka eventuella nackdelar som kan följa av samordnad statlig it-drift.

Utredaren ska därför

- utvärdera Försäkringskassans uppdrag att tillhandahålla samordnad och säker statlig it-drift och redovisa vilka slutsatser som kan dras i fråga om bl.a. upparbetad organisation, finansieringsmodell, tjänsteleverans, samordningsvinster samt påverkan på kärnverksamhet i fråga om bl.a. resursbehov och prioriteringar inom verksamheten, och
- analysera vilka lärdomar, erfarenheter och investeringar som är relevanta att vidareutveckla inom ramen för förslag till mer varaktiga former för samordnad statlig it-drift.

Säkerhetsmässiga och rättsliga förutsättningar för samordnad statlig it-drift

Samordning av statlig it-drift skulle innebära en allt högre grad av centralisering av den statliga förvaltningens it- och informationstillgångar, vilket leder till särskilda säkerhetsmässiga utmaningar. Många

statliga myndigheter bedriver verksamhet som till någon del är av betydelse för Sveriges säkerhet och träffas därigenom av säkerhetsskyddslagen. I dessa fall är det säkerhetsskyddslagstiftningen som sätter ramarna för om det över huvud taget är möjligt för en myndighet att samordna eller utkontraktera sin it-drift. Även en aggregering av flera statliga myndigheters informationstillgångar kan leda till att information som fristående inte skulle bedömas falla inom ramen för säkerhetsskyddslagen ändå omfattas av lagen, då de samlade informationstillgångarna får en annan hotbild och ett annat skyddsvärde. Vidare ansvarar varje myndighet för att beakta och planera för totalförsvarets krav, i enlighet med vad som bl.a. föreskrivs i förordningen (2015:1053) om totalförsvar och höjd beredskap.

De säkerhetsmässiga för- och nackdelarna för statliga myndigheter att ansluta sig till samordnad it-drift jämfört med att hantera it-drift i egen regi eller utkontraktera driften behöver analyseras. Analysen bör bl.a. innehålla fördjupade resonemang om hur regelverken om säkerhetsskydd, informationssäkerhet, offentlighet och sekretess samt skyddet för den personliga integriteten kan upprätthållas och utvecklas.

Även de rättsliga förutsättningarna för samordnad it-drift i övrigt behöver genomlysas. I analysen ska särskilt fokus läggas på avtalsrättsliga förhållanden, bl.a. när det gäller statliga myndigheters förutsättningar att ingå rättsligt bindande avtal med varandra, ansvarsförhållanden och funktioner för ansvarsutkrävande, prioritering av driftbehov vid incidenter, avtalsförvaltning m.m. I analysen bör de avtalsmodeller som tagits fram inom ramen för Statens servicecenters tillhandahållande av tjänster beaktas. Det behöver vidare utredas om det finns konkurrens- och marknadsrättsliga förutsättningar för samordnad it-drift, hur statligt tillhandahållen it-drift förhåller sig till regelverken om offentlig upphandling och om det är nödvändigt att författningsreglera anslutning till sådan it-drift.

Utredaren ska därför

- analysera de säkerhetsmässiga förutsättningarna för samordnad statlig it-drift särskilt när det gäller krav på säkerhetsskydd och informationssäkerhet samt sekretess och skyddet för den personliga integriteten,

- analysera de rättsliga förutsättningarna för samordnad statlig it-drift, särskilt när det gäller avtals- och upphandlingsfrågor samt konkurrens- och marknadsrättsliga frågor, och
- vid behov lämna författningsförslag som möjliggör att inrätta samordnad statlig it-drift.

Eventuella författningsförslag ska utformas med hänsyn tagen till kraven på säkerhetsskydd och informationssäkerhet, offentlighet och sekretess samt skyddet för den personliga integriteten. Om ändringar i offentlighets- och sekretesslagen föreslås ska de inte innebära någon förändring av lagens struktur och begreppsapparat. Inte heller ska sådana förslag innefatta ändring av, eller tillägg till, lagens bestämmelser om beslutsordning eller sekretessprövningens metodik. I uppdraget ingår inte heller att föreslå ändringar i grundlag eller i säkerhetsskyddslagstiftningen.

Samordnad, säker och kostnadseffektiv statlig it-drift

Utifrån resultatet av övriga delar av utredningen ska utredaren överväga vilka behov som finns av att inrätta mer varaktiga former av samordnad it-drift för den statliga förvaltningen samt om detta är lämpligt ur säkerhetssynpunkt. Utredaren ska också bedöma vilket tjänsteutbud som är mest prioriterat att tillhandahålla och beakta att samordnad it-drift ska vara säker, konkurrenskraftig och kostnadseffektiv.

Vidare ska utredaren analysera och ta ställning till vilka myndigheters it-drift som lämpar sig för samordning, och om vissa myndigheters it-drift på grund av säkerhetsmässiga förutsättningar eller särskilda myndighetsspecifika behov inte lämpar sig för sådan samordning.

Utredaren ska vidare lämna förslag på hur samordnad it-drift för den statliga förvaltningen kan organiseras och finansieras på ett kostnadseffektivt sätt. Här ingår att analysera om it-drift bör tillhandahållas av en ny eller befintlig myndighet eller om tjänsterna kan tillhandahållas av flera olika myndigheter, t.ex. utifrån sektorsspecifika behov. En utgångspunkt är att den kapacitet och de förmågor och erfarenheter som har byggts upp inom ramen för Försäkringskassans pågående uppdrag att erbjuda samordnad och säker statlig it-drift ska tas till vara. Utredaren ska lämna alternativa och rangordnade

förslag på organisationsmodeller, och med utgångspunkt i dessa även lämna förslag på en eller flera alternativa införandeplaner. Eventuella förslag som har övervägts men avfärdats ska redovisas och motiveras.

Utredaren ska också överväga om det bör vara obligatoriskt för delar av den statliga förvaltningen att ansluta sig till samordnad it-drift eller om anslutning ska grunda sig på frivillighet. Utredaren ska i denna del särskilt analysera konsekvenserna av obligatorium respektive frivillighet på inledande och avbrytande av it-driftssamverkan mellan myndigheterna samt rättsliga överväganden kopplat till detta. Vidare ska risker och konsekvenser för anslutande myndigheters specifika behov eller verksamhet vid införande av en obligatorisk anslutning särskilt analyseras, bl.a. risken att myndighetens kärnverksamhet blir lidande om myndighetens behov inte kan tillgodose eller prioriteras av den myndighet som sköter it-driften. Det behöver även analyseras om det finns behov av särskilda prioriteringsmodeller eller funktioner för anslutning med anledning av specifika eller brådskande behov hos vissa myndigheter.

Utredaren ska vid utformningen av förslagen beakta möjligheterna att använda privata leverantörer vid tillhandahållandet av samordnad it-drift för att dra nytta av fördelar i termer av säkerhet, teknikutveckling, innovationskraft och kostnadseffektivitet. Utredaren bör särskilt överväga om och hur kommersiella it-driftstjänster kan ingå i den samordnade it-driften. Det kan exempelvis vara i form av hybridlösningar där kommersiella it-driftstjänster används för att hantera hög belastning eller uppgifter som är mindre känsliga. Det kan också handla om lösningar där den aktör som tillhandahåller samordnad it-drift även upphandlar och samordnar användningen av kommersiella it-driftstjänster vid sidan av den samordnade statliga it-driften.

Utredarens förslag ska i samtliga delar grunda sig på en analys av säkerhetsmässiga, samhällsekonomiska och budgetära konsekvenser av att inrätta samordnad it-drift. I analysen ska det även ingå konsekvensbeskrivningar för det alternativet att it-driften inte samordnas, dvs. att varje myndighet fortsätter att ha it-drift i egen regi. När det gäller de säkerhetsmässiga konsekvenserna ska analysen beakta krav på säkerhetsskydd och informationssäkerhet samt sekretess och skyddet för den personliga integriteten såväl ur ett samhällsövergripande perspektiv som ur ett enskilt myndighetsperspektiv. Analysen ska även beakta de krav som ställs mot bakgrund av att planeringen för totalförsvaret har återupptagits (prop. 2014/15:109, bet. 2014/15:FöUl 1,

rskr. 2014/15:251). Utredaren ska också ta hänsyn till eventuella risker med centralisering av statsförvaltningens it-drift, geografisk placering och fysiskt skydd av datorhallar, potentiell exponering av myndigheters information mot andra länders rättsordningar samt risken för att informationen görs åtkomlig för obehöriga.

Utredaren ska därför

- analysera och lämna alternativa och rangordnade förslag på utformning och organisering av samordnad it-drift utifrån myndigheternas generella och specifika behov, tillsammans med införandeplaner,
- föreslå vilket tjänsteutbud som ska tillhandahållas inom ramen för samordnad it-drift, utifrån myndigheternas prioriterade behov,
- föreslå hur generella och myndighetsspecifika krav på informationssäkerhet och säkerhetsskydd kan tillgodoses,
- redogöra för om det finns vissa myndigheter eller typer av myndigheter, utöver försvarsmyndigheterna och Säkerhetspolisen, eller viss särskilt känslig information som inte bör hanteras inom ramen för samordnad it-drift,
- analysera om och föreslå hur privata leverantörer kan användas vid tillhandahållande av samordnad it-drift, och
- analysera och redogöra för budgetära, samhällsekonomiska och säkerhetsmässiga konsekvenser av de förslag som redovisas samt lämna förslag till finansiering.

Utredaren kan vid behov behandla sådana närliggande frågor som har samband med de frågeställningar som ska utredas, under förutsättning att uppdraget ändå bedöms kunna redovisas i tid samt att de eventuella förslag som läggs fram är finansierade.

Uppdraget att utreda rättsliga förutsättningar för utkontraktering till privata leverantörer

Utgångspunkten inom EU är att data ska kunna flöda fritt, vilket bl.a. kommer till uttryck i Europaparlamentets och rådets förordning (EU) 2018/1807 av den 14 november 2018 om en ram för det fria flödet av andra data än personuppgifter i Europeiska unionen

(dataflödesförordningen). En statlig myndighet, en kommun eller ett landsting som avser att utkontraktera it-drift till en privat leverantör, oavsett var denne är lokaliserad, måste dock beakta en mängd olika regelverk. Det gäller t.ex. sådana som rör offentlighet och sekretess, behandling av personuppgifter, arkivhantering, upphandling, informationssäkerhet och säkerhetsskydd samt upphovs- och avtalsrättsliga frågor. Behovet av säkerhetsskydd och informationssäkerhet är centralt.

Vid utkontraktering kan de rättsliga bedömningarna försvåras som en följd av t.ex. leverantörers komplexa affärsmodeller och en allt mer globaliserad marknad. Det gäller inte minst i fråga om kraven på hanteringen av sekretesskyddade uppgifter och bedömningen av när en uppgift ska anses röjd i offentlighets- och sekretesslagens mening. Samma sak gäller för hur det kan säkerställas att regelverket om dataskydd följs. I syfte att klargöra statliga myndigheters, kommuners och landstings möjligheter att anlita privata leverantörer behöver de rättsliga förutsättningarna för sådan utkontraktering kartläggas och analyseras.

Analysen ska bl.a. innehålla fördjupade resonemang kring kraven på hantering av sekretesskyddade uppgifter och risk för röjande av sekretessbelagda uppgifter. Här bör särskild vikt läggas vid frågan om huruvida avtalsreglerad tystnadsplikt och tekniska säkerhetsåtgärder, t.ex. kryptering eller pseudonymisering, kan påverka möjligheten att lämna ut uppgifter. Utredaren ska också särskilt analysera eventuella konsekvenser av att uppgifter som lämnas ut till en privat leverantör kan komma att exponeras för andra staters rättsordningar. Särskilt fokus ska ligga på betydelsen av rättsakter från tredjeland, t.ex. amerikanska CLOUD Act.

I uppdraget ingår också att analysera hur regelverket kring dataskydd kan uppfyllas, i synnerhet vid behandling av känsliga personuppgifter. I denna del ska särskild uppmärksamhet ägnas åt frågor som rör det organisatoriska och avtalsmässiga förhållandet mellan personuppgiftsansvarig och personuppgiftsbiträde, överföring av personuppgifter till tredjeland och skydd för den registrerades rättigheter.

Om utredaren finner att det finns lagstiftning som hindrar eller försvårar för statliga myndigheter, kommuner och landsting att utkontraktera it-drift till privata leverantörer, trots att säkerhetsmässiga, ekonomiska eller andra skäl talar för utkontraktering, ska

detta redogöras för. Det kan också gälla omotiverade datalokaliseringskrav som ska upphävas enligt dataflödesförordningen.

Utredaren ska därför

- kartlägga i vilken utsträckning det förekommer lagstiftning som hindrar eller försvårar för statliga myndigheter, kommuner och landsting att, med bibehållen säkerhet, utkontraktera it-drift till privata leverantörer,
- analysera de rättsliga förutsättningarna för utkontraktering, och
- vid behov lämna författningsförslag som tydliggör förutsättningarna för sådan utkontraktering.

Eventuella författningsförslag ska utformas med hänsyn tagen till kraven på säkerhetsskydd, informationssäkerhet, offentlighet och sekretess samt skyddet för den personliga integriteten. Om ändringar i offentlighets- och sekretesslagen föreslås ska de inte innebära någon förändring av lagens struktur och begreppsapparat. Inte heller ska sådana förslag innefatta ändring av, eller tillägg till, lagens bestämmelser om beslutsordning eller sekretessprövningens metodik. I uppdraget ingår inte heller att föreslå ändringar i grundlag eller i säkerhetsskyddslagstiftningen.

Konsekvensbeskrivningar

Utredaren ska analysera de samhällsekonomiska effekterna i utredningsarbetets alla delar, från problembeskrivning och syfte till analys av alternativ och motiv till förslag. I den samhällsekonomiska analysen ska det även redogöras för konsekvenserna av status quo, dvs. att inte samordna myndigheternas it-drift. Utredaren ska vidare bedöma förslagens konsekvenser i enlighet med kommittéförordningen (1998:1474) och förordningen om konsekvensutredning vid regelgivning (2007:1244). I detta ingår att redogöra för ekonomiska konsekvenser för de enskilda myndigheter som direkt berörs av utredarens förslag. Om förslag lämnas som innebär en verksamhetsövergång eller avveckling av verksamhet, t.ex. för myndigheter som är direkt berörda av etableringen och tillhandahållandet av samordnad it-drift, ska de budgetära och verksamhetsmässiga konsekvenserna för detta särskilt analyseras. Vidare ska utredaren särskilt redogöra för even-

tuella marknadseffekter och konkurrenspåverkan för det privata näringslivet i förhållande till de potentiella samordningsvinster som kan uppnås av samordnad it-drift för hela eller delar av den statliga förvaltningen.

Kontakter och redovisning av uppdraget

Utredaren ska hålla Regeringskansliet (Infrastrukturdepartementet) informerat om det löpande arbetet.

Uppdraget ska utföras i nära dialog med Försäkringskassan och Myndigheten för digital förvaltning. Utredaren ska samråda med Myndigheten för samhällsskydd och beredskap, Försvarsmakten/MUST, Försvarets radioanstalt och Säkerhetspolisen när det gäller informationssäkerhetsfrågor och med Säkerhetspolisen, Försvarsmakten och Fortifikationsverket beträffande säkerhetsskydd och andra säkerhetsaspekter som t.ex. kan följa av centralisering av statliga myndigheters it-drift. I frågor som rör dataskydd ska utredaren samråda med Datainspektionen. Vidare ska utredaren samråda med de statliga myndigheter som är direkt berörda av utredningens förslag, t.ex. om förslagen omfattar verksamhetsövergång eller på annat sätt mer specifikt berör en enskild myndighet. I relevanta delar ska utredaren inhämta synpunkter från privata it-driftsleverantörer, it-branschen och Sveriges Kommuner och Landsting.

Utredaren ska under arbetets gång ta hänsyn och förhålla sig till det fortsatta arbetet med betänkandena Kompletteringar till den nya säkerhetsskyddslagen (SOU 2018:82) och Juridik som stöd för förvaltningens digitalisering (SOU 2018:25). Vidare ska utredaren särskilt beakta det arbete som bedrivs inom Utredningen om näringslivets roll inom totalförsvaret samt försörjningstrygghet i fråga om försvarsmateriel (dir. 2018:64) och inom Utredningen om samordning av statliga utbetalningar från välfärdssystemen (dir. 2018:50).

Uppdragen att kartlägga och analysera statliga myndigheters behov av it-drift och den offentliga fö1valtningens rättsliga förutsättningar för utkontraktering ska redovisas senast den 31 augusti 2020. I delredovisningen ska utredaren redogöra för förslag till inriktning för det fortsatta utredningsarbetet när det gäller samordnad statlig it-drift. Uppdraget att förslå mer varaktiga former för samordnad statlig it-drift ska redovisas senast den 31 maj 2021.

(Infrastrukturdepartementet)

Kommittédirektiv 2020:73

Tilläggsdirektiv till It-driftsutredningen (I 2019:03)

Beslut vid regeringssammanträde den 2 juli 2020

Förlängd tid för uppdraget

Regeringen beslutade den 26 september 2019 kommittédirektiv om att ge en särskild utredare i uppdrag att utreda förutsättningarna för den offentliga förvaltningen att få tillgång till säker och kostnadseffektiv it-drift (dir. 2019:64). Enligt de ursprungliga direktiven skulle uppdragen att kartlägga och analysera statliga myndigheters it-drift och den offentliga förvaltningens rättsliga förutsättningar för utkontraktering med bibehållen säkerhet, inklusive eventuella författningsförslag, redovisas senast den 31 augusti 2020. Uppdraget att föreslå mer varaktiga former för samordnad statlig it-drift skulle redovisas senast den 31 maj 2021.

Utredningstiden förlängs. Uppdragen att kartlägga och analysera statliga myndigheters it-drift och den offentliga förvaltningens rättsliga förutsättningar för utkontraktering med bibehållen säkerhet, inklusive eventuella författningsförslag, ska i stället redovisas senast den 15 januari 2021. Uppdraget att föreslå mer varaktiga former för samordnad statlig it-drift ska i stället redovisas senast den 15 oktober 2021.

(Infrastrukturdepartementet)

STATENS OFFENTLIGA UTREDNINGAR

Utredningen om säker och kostnadseffektiv it-drift för den offentliga förvaltningen
I 2019:03

Enkät om säker och kostnadseffektiv it-drift

Den 29 september 2019 fattade regeringen beslut om att ge en särskild utredare i uppdrag att utreda förutsättningarna för den offentliga förvaltningen att få tillgång till säker och kostnadseffektiv it-drift. I oktober utnämndes Annelie Roswall Ljunggren, generaldirektör för Statskontoret, som särskild utredare. För närmare information om utredningens uppdrag se direktiv: https://www.regeringen.se/rattsliga-dokument/kommittedirektiv/2019/09/dir.-201964/

En viktig del i utredningens uppdrag är att kartlägga och analysera statliga myndigheters behov av säker och kostnadseffektiv it-drift. Genom enkäten vill vi på ett bättre sätt förstå hur behoven och förutsättningarna ser ut inom myndigheterna idag och framåt. Detta för att få ett bra underlag att utgå från i utredningens fortsatta arbete.

Enkäten är indelad i sex delar

Kapitel 1 berör säkerhet på myndigheten och i vilken utsträckning myndigheten är i behov av säkerhetsskydd utifrån myndighetens verksamhet och den information som myndigheten hanterar.

Kapitel 2 handlar om hur myndigheten hanterar sin it-drift idag. Frågorna syftar till att ge en bild av om myndigheten har egna datacenter, använder molntjänster och/eller samordnar sin it-drift med en annan myndighet. Frågorna syftar även till att fastställa ifall myndigheten utkontrakterar vissa närliggande tjänster till privata leverantörer alternativt samordnar dessa med en annan myndighet.

Kapitel 3 handlar om uppskattade kostnader för myndighetens egna datacenter, för molntjänster samt för samordnad it-drift mellan myndigheter. Frågorna kan vara svåra att svara på då definitioner och beräkningskonventioner varierar. Vi ber er därför att försöka uppskatta genomsnittliga årliga kostnader.

Kapitel 4 syftar till att identifiera hinder mot och bristande förutsättningar för säker och kostnadseffektiv it-drift. Utveckla gärna resonemang i fritext under de svarsalternativ som är relevanta för er.

Kapitel 5 syftar till att kartlägga framtida intresse för och behov av samordnad it-drift i staten.

Kapitel 6 ges myndigheten möjlighet att förtydliga vissa svar eller ge andra medskick till utredningen.

Enkäten kräver att flera kompetenser involveras

Frågorna i enkäten behöver besvaras av flera personer med olika kompetens inom er myndighet, till exempel juridisk och teknisk kompetens. Vi rekommenderar därför att ni hittar ett lämpligt tillvägagångssätt för att säkerställa att ni kan lämna ett så väl förankrat svar för myndigheten som möjligt.

Enkätsvaren skyddas

Eftersom myndighetens enkätsvar kan innehålla känslig information bör den ifyllda enkäten kommuniceras till utredningen på ett säkert sätt. Responderande myndighet ska e-posta den ifyllda enkäten som en krypterad bilaga med stöd av signalskyddssystem till Regeringskansliets informationsförmedling fa.ja.informationsformedling@regeringskansliet.se. För tekniska instruktioner kontakta Regeringskansliets informationsförmedling på angiven e-postadress eller Regeringskansliets bitr. signalskyddschef på 08-405 54 00 eller 08-405 59 21. Uppge ”Svar på enkät till Utredning I 2019:03” i ämnesraden när ni mejlar den ifyllda enkäten. I den fortsatta hanteringen av enkätsvaren följer utredningen tillämplig reglering i bl.a. säkerhetsskyddslagen (2018:585) och offentlighets- och sekretesslagen (2009:400).

Vänligen tänk på att inte i fritextsvar ange uppgifter som rör specifika leverantörer eller detaljerad information om eventuella säkerhetsbrister på myndigheten.

Svarstid

Vi önskar få era svar senast **den 31 mars 2020.**

Vid frågor om enkäten

Ni är välkomna att kontakta sekretariatet vid eventuella frågor.

Tina J Nilsson
tina.nilsson@regeringskansliet.se
072-227 90 76

Sofia Allansson
sofia.allansson@regeringskansliet.se
073-078 27 89

Kapitel 1 Säkerhet på myndigheten

Detta kapitel berör *säkerhet på myndigheten* och i vilken utsträckning myndigheten är i behov av säkerhetsskydd utifrån myndighetens verksamhet och den information som myndigheten hanterar.

Fråga 1a. Bedriver myndigheten verksamhet som kan bedömas vara samhällsviktig?

Samhällsviktig verksamhet är ett samlingsbegrepp som omfattar de verksamheter, anläggningar, noder, infrastrukturer och tjänster som är av avgörande betydelse för att upprätthålla viktiga samhällsfunktioner inom en samhällssektor. Med samhällsviktig verksamhet menas dels verksamhet som måste fungera för att inte dess bortfall ska leda till en samhällsstörning, dels verksamhet som måste finnas för att hantera en samhällsstörning när den väl inträffar.

Myndigheten för samhällsskydd och beredskap (MSB) har tagit fram en vägledning som ett stöd i arbetet med att identifiera samhällsviktig verksamhet: https://www.msb.se/contentassets/d8fca23b124c4686a629970fd2c1aa31/vagledning-for-identifiering-av-samhallsviktig-verksamhet-msb1408---juni-2019.pdf

[Välj ett svarsalternativ]

☐ Ja, gå vidare till **fråga 1b**
☐ Nej, gå vidare till **fråga 2a**
☐ Vet ej

Om ja, Fråga 1b. Inom vilka av följande samhällssektorer ingår den samhällsviktiga verksamheten?

Myndigheten för samhällsskydd och beredskap (MSB) har tagit fram en vägledningen som ett stöd i arbetet med att identifiera samhällsviktig verksamhet: https://www.msb.se/contentassets/d8fca23b124c4686a629970fd2c1aa31/vagledning-for-identifiering-av-samhallsviktig-verksamhet-msb1408---juni-2019.pdf

[Flervalsalternativ]

☐ Energiförsörjning
Exempel: Produktion och distribution el, produktion och distribution av fjärrvärme, produktion och distribution av bränslen och drivmedel.

☐ Finansiella tjänster
Exempel: Betalningar, tillgång till kontanter, centrala betalningssystemet, värdepappershandel.

☐ Handel och industri
Exempel: Bygg- och entreprenadverksamhet, detaljhandel, tillverkningsindustri.

☐ Hälso- och sjukvård samt omsorg
Exempel: Akutsjukvård, läkemedels- och materielförsörjning, omsorg om barn, funktionshindrade och äldre, primärvård, psykiatri, socialtjänst, smittskydd för djur och människor.

☐ Information och kommunikation
Exempel: Telefoni (mobil och fast), internet, radiokommunikation, distribution av post, produktion och distribution av dagstidningar, webbaserad information, sociala medier.

☐ Kommunalteknisk försörjning
Exempel: Dricksvattenförsörjning, avloppshantering, renhållning, väghållning.

☐ Livsmedel
Exempel: Distribution av livsmedel, primärproduktion av livsmedel, kontroll av livsmedel, tillverkning av livsmedel.

☐ Offentlig förvaltning
Exempel: Lokal ledning, regional ledning, nationell ledning, begravningsverksamhet, diplomatisk och konsulär verksamhet.

☐ Skydd och säkerhet
Exempel: Domstolsväsendet, åklagarverksamhet, militärt försvar, kriminalvård, kustbevakning, polis, räddningstjänst, alarmeringstjänst, tullkontroll, gränsskydd och immigrationskontroll, bevaknings- och säkerhetsverksamhet.

☐ Socialförsäkringar
Exempel: Allmänna pensionssystemet, sjuk- och arbetslöshetsförsäkringen.

☐ Transporter
Exempel: Flygtransport, järnvägstransport, sjötransport, vägtransport, kollektivtrafik.

☐ Annan; ange vad

☐ Vet ej

Fråga 2a. Hanterar myndigheten säkerhetsskyddsklassificerade uppgifter?

I säkerhetsskydd ingår att skydda uppgifter som rör säkerhetskänslig verksamhet och som därför omfattas av sekretess enligt offentlighets- och sekretesslagen, eller som skulle ha omfattats av den lagen om den varit tillämplig. De kallas säkerhetsskyddsklassificerade uppgifter och delas in i fyra säkerhetsskyddsklasser utifrån vilken skada för Sveriges säkerhet som kan uppstå om de röjs: kvalificerat hemlig, hemlig, konfidentiell, begränsat hemlig. För mer information om säkerhetsskyddsklassificerade uppgifter se Säkerhetspolisens vägledning: https://www.sakerhetspolisen.se/download/18.7acd465e16b4e0e54c64d/1560777315837/Vagledning-Introduktion-till-sakerhetsskydd.pdf

[Välj ett svarsalternativ]
☐ Ja, gå vidare till **fråga 2b**
☐ Nej, gå vidare till **fråga 3**
☐ Vet ej

Om ja, Fråga 2b. Vilken/vilka säkerhetsskyddsklasser ingår uppgifterna inom?

[Du kan välja flera svarsalternativ]

☐ Kvalificerat hemlig
☐ Hemlig
☐ Konfidentiell
☐ Begränsat hemlig
☐ Vet ej

Fråga 3. Hanterar myndigheten i sin **kärnverksamhet** uppgifter som är sekretessreglerade enligt offentlighets- och sekretesslagen?

Med kärnverksamhet avses myndighetens instruktionsenliga uppgifter.

När en sekretessbestämmelse inte ställer upp några särskilda villkor för sekretess, är sekretessen för en uppgift absolut. De flesta sekretessbestämmelser innehåller däremot som krav för att sekretess ska gälla att något speciellt villkor är uppfyllt, ett så kallat skaderekvisit. Det finns två huvudtyper av skaderekvisit, raka och omvända. För mer information om skaderekvisit se s. 29 i följande dokument: https://www.regeringen.se/4adad2/contentassets/e9c8b1b5a6224a26a0add9ae62db9413/offentlighetsprincipen-och-sekretess--kortfattat-om-lagstiftningen

[Du kan välja flera svarsalternativ]

☐ Ja, uppgifter med rakt skaderekvisit (presumtion för offentlighet)
☐ Ja, uppgifter med omvänt skaderekvisit (presumtion för sekretess)
☐ Ja, uppgifter med absolut sekretess
☐ Nej
☐ Vet ej

Fråga 4. Hanterar myndigheten i sin **kärnverksamhet** känsliga personuppgifter?

Med kärnverksamhet avses myndighetens instruktionsenliga uppgifter.

Enligt dataskyddsförordningen är följande kategorier av personuppgifter känsliga:

- *etniskt ursprung*
- *politiska åsikter*
- *religiös eller filosofisk övertygelse*
- *medlemskap i en fackförening*
- *hälsa (inkluderar även uppgifter om sexualliv eller sexuell läggning och genetiska uppgifter)*
- *biometriska uppgifter som entydigt identifierar en fysisk person.*

För mer information om känsliga personuppgifter se Datainspektionens hemsida: https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/kansliga-personuppgifter/

[Välj ett svarsalternativ]

☐ Ja
☐ Nej
☐ Vet ej

Fråga 5. Hur långt har myndigheten kommit i arbetet med informationssäkerhet?

Enligt MSB:s föreskrifter (MSBFS) 2016:1 ska myndigheter ha kontroll över all den information som organisationen ansvarar för och se till att:

- *Endast behöriga personer kan ta del av den (konfidentialitet)*
- *Vi kan lita på att den är korrekt och inte manipulerad (riktighet)*
- *Den alltid finns när vi behöver den (tillgänglighet)*

Du kan läsa mer i MSBFS 2016:1: https://www.msb.se/siteassets/dokument/regler/rs/b74a7b16-36a5-4de8-8f15-1297c37f1324.pdf

[Välj ett svarsalternativ]

☐ Vi har inte påbörjat ett systematiskt informationssäkerhetsarbete enligt MSBFS 2016:1.

☐ Vi har påbörjat arbetet genom att ha utsett en ansvarig att leda arbetet och börja analysera hur föreskrifterna MSBFS 2016:1 ska införas i myndigheten.

☐ Vi har tagit fram informationssäkerhetspolicy och påbörjat arbetet med styrande interna regelverk. Ledningen har beslutat om informationssäkerhetspolicyn och vi har beslutade styrande interna regelverk för allt informationssäkerhetsarbete enligt MSBFS 2016:1.

☐ Vi har förutom av ledningen beslutad informationssäkerhetspolicy och styrande interna regelverk, arbetssätt i delar av organisationen som säkerställer att vi genomför informationsklassning och riskbedömning samt inför säkerhetsåtgärder utifrån dessa underlag.

☐ Vi har förutom av ledningen beslutad informationssäkerhetspolicy och styrande interna regelverk, arbetssätt i hela organisationen som säkerställer att vi genomför informationsklassning och riskbedömning samt inför säkerhetsåtgärder utifrån dessa underlag.

☐ Allt informationssäkerhetsarbete i hela organisationen sker systematiskt enligt framtaget arbetssätt dokumenterat i interna regler och stöd. Arbetet och de interna regelverken och stöden utvärderas och vidareutvecklas regelbundet.

Fråga 6. Utgår myndigheten från en standard/modell som stöd för ett systematiskt informationssäkerhetsarbete?

[Välj ett svarsalternativ]

☐ Ja, ISO 27001
☐ Ja, BITS (Basnivå för informationssäkerhet, KBM 2006:1)
☐ Ja, COSO
☐ Ja, COBIT
☐ Ja, NIST (FISMA)
☐ Ja, ange vilken:
☐ Nej
☐ Vet ej

Fråga 7. Har myndigheten en kravkatalog med säkerhetskrav vid it-upphandling?

[Välj ett svarsalternativ]

☐ Vi har inte reflekterat över frågan på myndigheten.
☐ Vi har påbörjat diskussion om att vi behöver en kravkatalog med säkerhetskrav att utgå ifrån.
☐ Vi har en säkerhetskravkatalog som vi använder oss av vid upphandling.

Fråga 8. Har myndigheten ett etablerat arbetssätt för att verifiera säkerhetskrav i anbudssvar vid it-upphandling?

[Välj ett svarsalternativ]

☐ Vi har inte reflekterat över frågan på myndigheten
☐ Vi har ett *påbörjat* arbetssätt att verifiera säkerhetskraven i **anbudssvar**
☐ Vi har ett *etablerat* arbetssätt att verifiera säkerhetskraven i **anbudssvar**

Fråga 9. Har myndigheten ett etablerat arbetssätt att verifiera säkerhetskraven i leverans/acceptanstest/driftsättning (eller motsvarande)?

[Välj ett svarsalternativ]

☐ Vi har inte reflekterat över frågan på myndigheten
☐ Vi har ett *påbörjat* arbetssätt att verifiera säkerhetskraven i **leverans/acceptanstest/driftsättning (eller motsvarande)**
☐ Vi har ett *etablerat* arbetssätt att verifiera säkerhetskraven i **leverans/acceptanstest/driftsättning (eller motsvarande)**

Fråga 10. Har myndigheten ett etablerat arbetssätt att verifiera säkerhetskraven under avtalets/kontraktets giltighetstid?

[Välj ett svarsalternativ]

☐ Vi har inte reflekterat över frågan på myndigheten
☐ Vi har ett *påbörjat* arbetssätt att verifiera säkerhetskraven under **avtalets/kontraktets giltighetstid**
☐ Vi har ett *etablerat* arbetssätt att verifiera säkerhetskraven under **avtalets/kontraktets giltighetstid**

Kapitel 2 Myndighetens nuvarande hantering av it-drift och närliggande tjänster

Detta kapitel handlar om *hur myndigheten hanterar sin it-drift idag*. Frågorna syftar till att ge en bild av om myndigheten har egna datacenter, använder molntjänster och/eller samordnar sin it-drift med en annan myndighet. Frågorna syftar även till att fastställa ifall myndigheten utkontrakterar vissa *närliggande tjänster* till privata leverantörer alternativt samordnar dessa med en annan myndighet.

Datacenter i egen regi

Fråga 11. Har er myndighet egna datacenter i egna lokaler där ni äger utrustningen?

Med datacenter avses ett fysiskt utrymme där hela eller merparten av er utrustning för servrar, lagring- och kommunikationsutrustning finns. Utrymmet kan vara anpassat med avseende på t.ex. kylsystem, elförsörjning, brand- och skalskydd.

☐ Ja. Om flera, hur många?
☐ Nej

Fråga 12. Hur många fysiska servrar äger myndigheten?

Med servrar avses datorsystem med anpassad hårdvara som syftar till att betjäna andra system.

Antal
☐ Inga
☐ Vet ej

Fråga 13. Hur många virtuella servrar använder myndigheten?

Med virtuell server avses en virtuell instans av ett operativsystem som kan köras isolerat från och parallellt med liknande instanser på samma fysiska server.

Antal
☐ Inga
☐ Vet ej

Användning av molntjänster från privata leverantörer

Fråga 14. Använder myndigheten molntjänster som tillhandahålls av privata leverantörer?

En vanligt förekommande kategorisering av it-driftsrelaterade tjänster är Infrastructure as a service (IaaS), Platform as a Service (PaaS) och Software as a Service (SaaS).[1]

	Ja	Nej	Vet ej
IaaS *kan beskrivas som tjänster där användaren får tillgång till processorkapacitet, lagring, nätverk, servrar och andra fundamentala resurser och som möjliggör för användaren att köra godtycklig mjukvara inklusive operativsystem och applikationer.*	☐	☐	☐
PaaS *kan beskrivas som tjänster där användaren får tillgång till utvecklingsmiljöer, bibliotek och verktyg som möjliggör driftsättning av applikationer. Användaren kontrollerar inte underliggande nätverk, servrar, operativsystem eller lagring men applikationer som driftas i miljön.*	☐	☐	☐
SaaS *kan beskrivas som tjänster där användaren genom en klient får tillgång till en viss applikation utan att kontrollera underliggande infrastruktur såsom nätverk, servrar, lagring, operativsystem.*	☐	☐	☐

[1] Definitionen av de tre kategorierna är baserade på National Institute of Standards and Technology (NIST) SP 800-145 (https://csrc.nist.gov/publications/detail/sp/800-145/final).

Fråga 15. Om myndigheten använder SaaS-tjänster från privata leverantörer, vilka funktioner fyller dessa tjänster?

[Du kan välja flera svarsalternativ]

☐ HR/lön
☐ Kontorsstöd
☐ Diarium
☐ Ärendehanteringssystem
☐ Webbplats
☐ Enkätverktyg
☐ Ekonomisystem
☐ Andra, ange vilka:

Fråga 16. Hyr myndigheten in sig i en privat leverantörs datacenter (så kallade samlokaliserings- eller co-locationtjänster)?

☐ Ja
☐ Nej

Samordnad it-drift mellan myndigheter

Flera myndigheter samordnar i dag sin it-drift på olika sätt. Försäkringskassan fick 2017 i uppdrag av regeringen att tillhandahålla samordnad och säker it-drift till vissa myndigheter. Försäkringskassan erbjuder allt från ett helhetsåtagande kring it-drift, för myndigheter som har små resurser för it-drift, till enstaka it-tjänster för myndigheter som sköter det mesta av sin it-drift i egen regi.

Fråga 17a. Har myndigheten samordnat sin it-drift med annan/andra myndigheter?

Ja, en annan myndighet hanterar vår it-drift, gå vidare till **fråga 17b**	☐	Vilken myndighet?
Ja, myndigheten hanterar en annan/andra myndigheters it-drift, gå vidare till **fråga 17c**	☐	Vilken/vilka myndigheter?
Nej, gå vidare till **fråga 18**	☐	

Fråga 17b. Om myndighetens it-drift hanteras av en annan myndighet, vilka tjänster eller leveranser omfattas?

Ange vad:	

Fråga 17c. Om myndigheten hanterar it-drift åt en annan myndighet, vilka tjänster eller leveranser omfattas?

Ange vad:	

Närliggande tjänster

Fråga 18. Tillhandahåller privata leverantörer eller en annan myndighet följande närliggande it-tjänster till myndigheten?

	Utkontrakterad till privat leverantör	Tillhandahålls av annan myndighet	Ej aktuell
It-arbetsplats *Administration, underhåll och leverans av paketerad stationära eller bärbara arbetsdatorer med tillbehör och programvara.*	☐	☐	☐

Stödtjänster *Helpdesk, stöd och support till myndighetens personal.*	☐	☐	☐

Kapitel 3 Kostnader för it-drift

Detta kapitel handlar om uppskattade kostnader för myndighetens egna datacenter, för molntjänster samt för samordnad it-drift mellan myndigheter. Frågorna kan vara svåra att svara på då definitioner och beräkningskonventioner varierar. Vi ber er därför att försöka uppskatta genomsnittliga årliga kostnader.

Kostnader för datacenter

Fråga 19. Om myndigheten har egna datacenter, vad är de genomsnittliga årliga platsbundna kostnaderna, i tusentals kronor, för myndighetens samtliga datacenter?

Med platsbundna kostnader för datacentret avses summan av kostnader för lokaler, el, kylsystem, larm, skal- och brandskydd. Dvs. kostnaden för alla tillgångar som är knutna till den fysiska platsen för datacentret. Som exempel skulle dessa platsbundna kostnader kunna sparas in om innehållet i datacentret (servrar, nätverksutrustning etc.) flyttades till ett annat externt datacenter. Däremot ingår inte icke platsbundna kostnader, se nästa fråga.

Ange belopp:	(i tusentals kronor)

Fråga 20. Om myndigheten har egna datacenter, vad är den genomsnittliga årliga icke platsbundna kostnaderna, i tusentals kronor, för myndighetens datacenter?

Med icke platsbundna kostnader avses summan av kostnader för servrar, nätverksutrustning, lagring kringutrustning etc. som potentiellt kan flyttas till ett nytt datacenter.

Ange belopp:	(i tusentals kronor)

Fråga 21. Hur många årsarbetskrafter arbetar uppskattningsvis med att drifta myndighetens datacenter på myndigheten?

Med årsarbetskrafter avses summan av arbetstid för anställd och inhyrd personal som inte varit nödvändig om it-driften varit helt utkontrakterad. Arbetsuppgifter som typiskt omfattas är sådant som rör hantering av kyla, kablage, larm, rack, fysiska servrar, nätverksutrustning, lagringsnätverk, blocklagring, operativsystem och virtualiseringslager. Applikationer och applikationsdrift omfattas inte. Arbetstid för anställd och inhyrd personal på myndigheten för utveckling och förvaltning ska inte räknas med.

Ange antal årsarbetskrafter:	

Kostnader för molntjänster från privata leverantörer

Fråga 22. Om myndigheten använder IaaS-tjänster (se definition fråga 14), vad är de genomsnittliga årliga kostnaderna för dessa tjänster? (i tusentals kronor)

Ange belopp:	(i tusentals kronor)

Fråga 23. Om myndigheten använder PaaS-tjänster (se definition fråga 14), vad är de genomsnittliga årliga kostnaderna för dessa tjänster? (i tusentals kronor)

Ange belopp:	(i tusentals kronor)

Fråga 24. Om myndigheten använder SaaS-tjänster (se definition fråga 14), vad är de genomsnittliga årliga kostnaderna för dessa tjänster? (i tusentals kronor)

Ange belopp:	(i tusentals kronor)

Kostnader för samordnad it-drift mellan myndigheter

Fråga 25. Om er it-drift tillhandahålls av en annan myndighet genom överenskommelse, vad är de genomsnittliga årliga kostnaderna för detta? (i tusentals kronor)

Ange belopp:	(i tusentals kronor)

Kapitel 4 Hinder mot säker och kostnadseffektiv it-drift

Detta kapitel syftar till att identifiera hinder mot och bristande förutsättningar för säker och kostnadseffektiv it-drift. Utveckla gärna resonemang i fritext under de svarsalternativ som är relevanta för er.

Fråga 26. Vilka hinder ser myndigheten att upprätthålla en säker it-drift?

Med säker it-drift avses att myndighetens it-drift lever upp till rättsliga och säkerhetsmässiga krav, exempelvis krav på säkerhetsskydd och informationssäkerhet samt skyddet för den personliga integriteten.

[Du kan välja flera svarsalternativ]

☐ Avsaknad av relevant kompetens inom verksamheten

Ange varför:

☐ Svårigheter att tolka lagstiftning (t.ex. upphandling, avtal, sekretess, dataskydd, säkerhetsskydd, arkivering)

Ange varför:

☐ Bristande informationsklassificering

Ange varför:

☐ Hög kostnad för de lösningar som verksamheten kräver

Ange varför:

☐ Svårigheter att hitta lösningar som möter verksamhetens krav

Ange varför:

☐ Annat

Ange vilka och varför:

Fråga 27. Vilka hinder ser myndigheten att upprätthålla en kostnads-effektiv it-drift?

Med kostnadseffektivitet avses att myndigheten utifrån sitt uppdrag har tillgång till en ändamålsenlig it-drift till en rimlig kostnad.

[Du kan välja flera svarsalternativ]

☐ Avsaknad av relevant kompetens inom verksamheten

Ange varför:

☐ Låg kostnadskontroll

Ange varför:

☐ Svårigheter att formulera ändamålsenliga krav på it-drift (t.ex. funktionella, icke-funktionella och tekniska krav)

Ange varför:

☐ Leverantörsberoende eller andra inlåsningseffekter

Ange varför:

☐ Höga krav på säkerhet

Ange varför:

☐ Annat

Ange vilka och varför:

Kapitel 5 Myndighetens framtida behov och intresse av samordnad it-drift

Utredningen har i uppgift att utvärdera Försäkringskassans uppdrag att tillhandahålla säker och samordnad it-drift. Utredningen ska även lämna eventuella förslag på organisering och finansiering av en säker och kostnadseffektiv samordnad it-drift. Detta kapitel syftar till att kartlägga framtida intresse för och behov av samordnad it-drift i staten.

Fråga 28. Beskriv hur myndighetens behov av it-drift ser ut under de kommande 5 åren?

Vänligen tänk på att inte ange uppgifter som rör specifika leverantörer eller detaljerad information om eventuella säkerhetsbrister på myndigheten.

Beskriv:	

Fråga 29a. Har myndigheten intresse/behov av att i framtiden ansluta sig till en samordnad statlig it-drift?

[Välj ett svarsalternativ]

☐ Ja, gå vidare till **fråga 29b**
☐ Nej, gå vidare till **fråga 30a**
☐ Vet ej

Fråga 29b. Om myndigheten har intresse/behov av att ansluta sig till en samordnad statlig it-drift, vilka delar av it-driften vill myndigheten överlåta?

Ange vad:	

Fråga 29c. Om myndigheten har intresse/behov av att ansluta sig till en samordnad statlig it-drift, vad är de huvudsakliga skälen till detta?

[Du kan välja flera svarsalternativ]

☐ Kostnadsbesparingar
☐ Förbättrad säkerhet
☐ Förenklad digital samverkan mellan myndigheter
☐ Annat, beskriv:

Fråga 30a. Har myndigheten intresse av att i framtiden erbjuda it-drift till andra myndigheter?

[Välj ett svarsalternativ]

☐ Ja, gå vidare till **fråga 30b**
☐ Nej, gå vidare till **fråga 31**
☐ Vet ej

Fråga 30b. Om myndigheten har intresse av att i framtiden erbjuda it-drift till andra myndigheter, vilka tjänster kan myndigheten erbjuda?

Ange vad:	

Fråga 30c. Vilka förutsättningar behöver myndigheten för att kunna erbjuda it-drift till andra myndigheter?

Ange vad:	

Kapitel 6 Avslut

Fråga 31. Finns det något ytterligare ni skulle vilja tillägga eller förtydliga när det gäller era svar?

Beskriv:	

Tack för er medverkan!

Statens offentliga utredningar 2021

Kronologisk förteckning

1. Säker och kostnadseffektiv it-drift – rättsliga förutsättningar för utkontraktering. I.

Statens offentliga utredningar 2021

Systematisk förteckning

Infrastrukturdepartementet

Säker och kostnadseffektiv it-drift
– rättsliga förutsättningar för
utkontraktering. [1]