Stockholms stad

Bilaga 7

GDPR Årsrapport

2021

Stockholms stads kommunstyrelse

GDPR årsrapport
December 2021

Dnr: KS 2021/1557
Datum: 2021-12-20
Kontaktperson: Kommunstyrelsens dataskyddsombud

1 Bakgrund

Enligt dataskyddsförordningen är Stockholms stads kommunstyrelse ansvarig för att verksamheten tillhörande kommunstyrelsen följer gällande dataskyddslagstiftning vid hantering av personuppgifter. Det innebär att kommunstyrelsen behöver informera sig, styra och följa upp verksamheten avseende behandlingen av personuppgifter.

En myndighet eller offentligt organ ska enligt dataskyddsförordningen utnämna ett dataskyddsombud. Dataskyddsombudets ställning och uppgifter är definierade och angivna i förordningen. Enligt dataskyddsförordningen ska dataskyddsombudet informera och ge råd till kommunstyrelsen och de anställda som behandlar personuppgifter om skyldigheterna enligt gällande dataskyddslagstiftning. Ett dataskyddsombud ska även oberoende övervaka integritets- och dataskyddsefterlevnaden, strategin för skydd av personuppgifter och ansvarstilldelningen. I förordningen anges även att dataskyddsombudet i sitt uppdrag ska rapportera direkt till högsta förvaltningsnivå.

Dataskyddsombudets årsrapport är ett medel för Stockholms stads kommunstyrelse att ta emot de råd som dataskyddsombudet är skyldig att ge till ansvarig enligt dataskyddsförordningen samt för att få insyn i vad dataskyddsombudets granskande arbete av verksamhetens status avseende integritet och dataskydd visar. Årsrapporten syftar vidare till att Stockholms stads kommunstyrelse ska kunna följa upp och styra verksamhetens systematiska integritets- och dataskyddsarbete samt kunna fatta beslut om prioriteringar, resurser och aktiviteter för 2022. Detta samspel bör resultera i ett av flera verktyg för Stockholms stads kommunstyrelse att kunna visa hur de som personuppgiftsansvarig och personuppgiftsbiträde efterlever dataskyddslagstiftningen.

Dataskyddslagstiftningen och skyddet för individens personliga integritet har sin grund i de mänskliga rättigheterna i Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna, Europakonventionen. Den mänskliga rättighet som avses är individens rätt till respekt för sitt privat- och familjeliv, sitt hem och sin korrespondens. Individen ska inte behöva utsättas för godtyckliga eller olagliga inskränkningar i sitt privatliv.

Europiska unionen har antagit EU-stadgan om de grundläggande rättigheterna. Skyddet för individens personliga integritet föreskrivs i rättigheten att var och en har rätt till respekt för sitt privatliv och familjeliv, sin bostad och sina kommunikationer. EU-stadgan innehåller även individens rätt till skydd för personuppgifter.

Dataskyddsförordningen och kompletterande lagstiftning trädde i kraft den 25 maj 2018. Dataskyddsförordningen skyddar fysiska personers grundläggande rättigheter och friheter, särskilt individens rätt till skydd av personuppgifter. Förordningen säkerställer enhetliga dataskyddsregler inom EU och det fria flödet av personuppgifter inom unionen.

I egenskap av kommunstyrelsens dataskyddsombud lämnar jag följande årsrapport.

.

Innehåll

1 Bakgrund ... 3

2 Sammanfattning ... 6

2.1 Resultat av granskning och dataskyddsombudets råd ... 7

3 Obligatoriska rapporteringsområden ... 9

3.1 Registerförteckning ... 10

3.2 Styrdokument avseende dataskydd ... 13

3.3 Tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar ... 17

3.4 Konsekvensbedömningar ... 20

3.5 Individens rättigheter ... 22

3.6 Personuppgiftsincidenter ... 23

4 Genomförda granskningar under året ... 27

5 Risker inom dataskydd ... 28

5.1 Riskanalys ... 28

5.2 Dataskyddsombudets råd till kommunstyrelsen ... 30

6 Planerade granskningar under det nya verksamhetsåret ... 31

6.1 Planerad granskning ... 31

7 Övrigt att rapportera ... 33

7.1 Utbildning avseende dataskydd ... 33

7.2 Inhämtning av GDPR-årsrapporter ... 33

2 Sammanfattning

Stockholms stads mål om en modern, hållbar och innovativ storstad förutsätter ett systematiskt dataskyddsarbete för att skydda stockholmarnas personliga integritet och värna om stockholmarnas rättigheter och friheter.

I kommunstyrelsens dataskyddsombuds rapport kommer ni att få läsa om dataskyddsregelverket, utvecklande av praxis, kommunstyrelsens dataskyddsarbete och kommunstyrelsens dataskyddsombuds råd till kommunstyrelsen för att höja mognadsgraden avseende dataskydd i verksamheten.

I årets rapport kommer skyldigheterna nedan att beskrivas;

- att föra ett behandlingsregister,
- att ta fram styrdokument, rutiner och instruktioner avseende hur personuppgifter får behandlas,
- att implementera tekniska och organisatoriska skyddsåtgärder för personuppgifter,
- att utföra konsekvensbedömning avseende dataskydd,
- att kunna ta emot och hantera individens rättigheter,
- att ha förmåga att upptäcka, hantera och förebygga personuppgiftsincidenter.

I rapporten kommer även de grundläggande principerna beröras, även principerna om inbyggt dataskydd och dataskydd som standard. Vidare beskrivs risker inom dataskydd och behov av att utföra riskanalyser med individen och personuppgiftsbehandlingen i fokus. Genomförda granskningar under året och planerade granskningar för 2022 rapporteras om samt obligatorisk e-utbildning avseende dataskydd och informationssäkerhet. Årsrapporten kommer även behandla EU-domstolens Schrems II-dom och dess konsekvenser. Slutligen kommer även kommunstyrelsens inhämtning av samtliga Stockholms stads nämnders och bolagsstyrelsers dataskyddsombuds GDPR-årsrapport omnämnas och vad aktiviteten har för syfte.

Då gällande dataskyddslagstiftning ålägger ett omfattande ansvar på kommunstyrelsen avseende dataskydd behöver årsrapporten därför ge råd om aktiviteter som behöver planeras för och utföras under 2022.

2.1 Resultat av granskning och dataskyddsombudets råd

2.1.1 Registerförteckning

Ett omfattande arbete har gjorts gällande kommunstyrelsens registerförteckning, vilket ökat mognadsgraden avseende dataskydd. Under 2022 bör registerförteckningen kompletteras enligt plan och med den systematik som tagits fram. Kvalitetsgranskningar kommer även utföras av dataskyddsombudet under 2022.

2.1.2 Implementera tekniska och organisatoriska skyddsåtgärder för personuppgifter och hantering av personuppgiftsincidenter

Kommunstyrelsens ansvar att tillhandahålla stadsgemensam it medför att informationsklassning och implementering av informationsklassning behöver prioriteras, då det är vid klassningen behov av tekniska och organisatoriska skyddsåtgärder identifieras som behöver implementeras. Tillhandahållandet av gemensam it innebär också att verksamheten behöver förbättra sin förmåga att identifiera, dokumentera och hantera personuppgiftsincidenter. Generellt är dessa förmågor idag inte fullt ut tillfredsställande.

Dataskyddsombudet ser även att verksamheten behöver utbildas gällande informationsklassning och personuppgiftsincidenter för att förbättra regelefterlevnaden avseende dataskydd.

2.1.3 Individens rättigheter

Dataskyddsombudet bedömer att mognadsgraden avseende hanteringen av registrerades rättigheter är hög och att hanteringen efterlever gällande lagstiftning.

2.1.4 Styrdokument avseende dataskydd

I och med registerförteckningsarbetet har kunskap om och behov av samt implementering av styrdokument, rutiner och instruktioner för hur personuppgifter får behandlas ökat. Fler skriftliga instruktioner behöver emellertid tas fram. Vilka instruktioner som behöver prioriteras bör samrådas med dataskyddsombudet.

2.1.5 Konsekvensbedömning avseende dataskydd

Metoden för konsekvensbedömning avseende dataskydd används idag. Här är det emellertid viktigt att verksamheten klargör om nämnd är personuppgiftsansvarig för personuppgiftsbehandlingen eller är personuppgiftsbiträde till annan nämnd eller bolagsstyrelse inom Stockholms stad. Skyldigheten att utföra konsekvensbedömning åligger personuppgiftsansvarig nämnd eller bolagsstyrelse inom Stockholm stad och ska utgå från personuppgiftsbehandlingen. Användandet av metoden för konsekvensbedömning avseende dataskydd behöver öka.

Mot bakgrund av granskningens resultat och dataskyddsombudets råd bör kommunstyrelsen tillse att aktiviteter utförs, där förbättringsmöjligheter finns enligt ovan.

Avslutningsvis framhålls i rapporten risker inom dataskydd och vikten av att utföra riskanalyser avseende dataskydd.

3 Obligatoriska rapporteringsområden

Denna årsrapport spänner över sex obligatoriska rapporteringsområden som Stockholms stads kommunstyrelse som personuppgiftsansvarig och personuppgiftsbiträde som ett minimum ska informera sig om årligen för att kunna anses leda och styra dataskyddsarbetet så som dataskyddsförordningen avser.

De obligatoriska rapporteringsområdena är registerförteckning, styrdokument, tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar, konsekvensbedömningar, individens rättigheter och personuppgiftsincidenter.

Nedan redogörs för gällande dataskyddslagstiftning, utveckling av praxis och Stockholms stads kommunstyrelses arbete med dataskydd och dataskyddsombudets råd gällande de obligatoriska rapporteringsområdena.

Innan redogörelse av de obligatoriska rapporteringsområdena nedan ska de grundläggande principerna i dataskyddsförordningen som ska genomsyra all personuppgiftsbehandling kort beröras.

Principer för behandling av personuppgifter

De grundläggande principerna är laglighet, korrekthet och öppenhet, ändamålsbegränsning, uppgifts- och lagringsminimering, riktighet, integritet och konfidentialitet samt ansvarsskyldighet.

Principerna innebär i korthet följande. Den personuppgiftsansvariga måste ha stöd i dataskyddsförordningen för att få behandla personuppgifter. Personuppgifter får bara samlas in för specifika, särskilt angivna och berättigade ändamål och fler personuppgifter får inte behandlas än vad som behövs för ändamålen. Personuppgifterna ska vara riktiga och personuppgifter som inte behövs ska raderas[1]. Personuppgifterna ska skyddas så att inte obehöriga får tillgång till dem eller att de förvanskas, förloras eller förstörs. Den personuppgiftsansvarige ska även visa att den efterlever och hur den efterlever dataskyddsförordningen.

[1] Observera rätten till allmän handling och dess begränsning av radering.

3.1 Registerförteckning

3.1.1 Gällande lagstiftning

Enligt dataskyddsförordningen ska kommunstyrelsen i egenskap av personuppgiftsansvarig[2] och personuppgiftsbiträde[3] föra ett register över behandling[4] som utförs under dess ansvar. I förordningen anges även uttömmande vad behandlingsregistret ska innehålla.

I skälen i dataskyddsförordningen anges att ansvarig för att påvisa att förordningen följs ska föra ett register över behandling som sker under dess ansvar och registret ska på tillsynsmyndighetens begäran göras tillgängligt för tillsynsmyndighetens granskning och övervakning.

3.1.2 Kommunstyrelsens arbete

Den 22 oktober 2020 beslutade stadsdirektören om ett projektdirektiv för kommunstyrelsens dataskyddsarbete. Ett av syftena var att registerförteckningen skulle vara enhetlig och digitaliserad för att ledningen enklare ska kunna styra och följa upp förvaltningens dataskyddsarbete och säkerställa regelefterlevnad inom dataskydd.

Verksamheten har utfört en omfattande digitalisering av registerförteckningen under projektdirektivet och beaktat att nu gällande dataskyddslagstiftning omfattar både strukturerad och ostrukturerad behandling av personuppgifter genom att använda sig av de processbaserade hanteringsanvisningarna för kommunstyrelsen/ stadsledningskontoret, dokumenthanteringsplan, i arbetet. Eftersom hanteringsanvisningarna använts som stöd i arbetet behöver dessa vara fullständiga avseende de personuppgiftsbehandlingar som utförs om inte verksamheten själv

[2] 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; 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

[3] en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning

[4] 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

identifierar att någon personuppgiftsbehandling saknas i hanteringsanvisningarna.

Kommunstyrelsens dataskyddsombud har tillgång till kommunstyrelsen registerförteckning och har även under 2021 gjort kontroller gentemot upprättade hanteringsanvisningar och registerförteckning och förmedlat granskningen till verksamheten. Verksamheten har löpande kompletterat ramen för registerförteckningen och kompletteringsarbetet fortgår.

Verksamheten har även tillsammans med dataskyddsombudet identifierat personuppgiftsbehandlingar som behöver registerförtecknas 2022, då ny behandling av personuppgifter ska påbörjas. Stadsledningskontorets dataskyddshandläggare har skapat en systematik för att fånga upp personuppgiftsbehandlingar som behöver registerförtecknas och säkerställa att registerförteckning utförs av ansvarig. Dataskyddshandläggare har även tagit fram en rutin för registerförteckning i det digitala verktyg som används.

Under projektdirektivet har en ansvarig för varje personuppgiftsbehandling utsetts och angetts i behandlingsregistret, vilket underlättar att hålla kommunstyrelsens registerförteckning korrekt och uppdaterad. Det är medarbetare som dagligen hanterar personuppgifter som vet hur de behandlas, som bör delta vid upprättandet av behandlingsregistret. Ett nära samarbete mellan ansvarig för behandlingsregistret och dataskyddshandläggare, informationssäkerhetssamordnare och dataskyddsombud har etablerats.

3.1.3 Utveckling av praxis

Sveriges tillsynsmyndighet, Integritetsskyddsmyndigheten, förmedlar att en tydlig, komplett och väl utformad förteckning är viktig för personuppgiftsansvariges och personuppgiftsbiträdets interna arbete med att säkerställa att verksamheten följer reglerna i dataskyddslagstiftningen. Ett behandlingsregister över personuppgiftsbehandlingar behöver även löpande ses över allteftersom förutsättningarna hos en verksamhet förändras. Ovan har framkommit bland annat när Integritetsskyddsmyndigheten granskat några brottsbekämpande myndigheters förteckning över personuppgiftsbehandlingar enligt brottsdatalagen. Observera att tillsynen avsåg brottsdatalagen och inte dataskyddsförordningen, men slutsatserna borde även gälla dataskyddsförordningen.

3.1.4 Dataskyddsombudets råd till kommunstyrelsen

Att ha en korrekt och uppdaterad registerförteckning är nödvändigt. Det underlättar och utgör underlag för det systematiska och löpande dataskyddsarbetet inom kommunstyrelsens ansvarsområde.

3.1.4.1 Fortsatt systematisk inventering av personuppgifter

Dataskyddsombudet rekommenderar att verksamheten fortsätter att löpande inventera vilka personuppgiftsbehandlingar som utförs, då personuppgiftsbehandling är rörlig över tid på grund av exempelvis nya uppdrag och förändrade förutsättningar. Det är även viktigt att behandlingsregistret kompletteras med personuppgiftsbehandlingar om/när verksamheten identifierar att en personuppgiftsbehandling inte finns i behandlingsregistret.

3.1.4.2 Fortsatt systematisk uppdatering av dokumenthanteringsplanen

Det är av särskild vikt att hanteringsanvisningarna innefattar personuppgiftsbehandlingen som utförs av kommunstyrelsen och detta blir särskilt viktigt för avdelningarnas arkivredogörare att beakta när de medverkar vid upprättande och aktualisering av dokumenthanteringsplanen.

3.1.4.3 Fortsatt granskning av registret 2022

Då digitalisering och förändring av behandlingsregistret till ett processbaserat register gjorts under 2021 kommer kvalitén i behandlingsregistret och dess fullständighet granskas under 2022 av dataskyddsombudet tillsammans med verksamheten för att verksamheten enklare ska kunna uppdatera registret om och när behov identifieras under granskningen.

3.2 Styrdokument avseende dataskydd

3.2.1 Gällande lagstiftning

I detta avsnitt avses med styrdokument framförallt de rutiner och instruktioner som verksamheten är skyldig att ta fram och införa enligt gällande dataskyddslagstiftning.

3.2.1.1 Principerna om ansvarsskyldighet, *integritet och konfidentialitet*

Enligt den grundläggande principen om ansvarsskyldighet i dataskyddsförordningen ska personuppgiftsansvarig *visa* att denne efterlever förordningen. Principen om integritet och konfidentialitet innebär att personuppgifter ska behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder.

I de grundläggande principerna om ansvarsskyldighet och integritet och konfidentialitet, ingår att dokumentera och ge instruktioner gällande personuppgiftsbehandling och att vidta lämpliga organisatoriska åtgärder för att säkerställa säkerhetsnivån för personuppgiftsbehandlingen. I organisatoriska skyddsåtgärder ingår att ta fram exempelvis riktlinjer/anvisningar, rutiner, instruktioner och beslut om dataskydd.

3.2.1.2 Skyldigheten att ge instruktioner

I artikel 29 anges att personuppgiftsbiträdet och personer som utför arbete under den personuppgiftsansvariges eller personuppgiftsbiträdets överinseende, och som får tillgång till personuppgifter, får endast behandla dessa på instruktion från den personuppgiftsansvarige, såvida han eller hon inte är skyldig att göra det enligt unionsrätten eller medlemsstaternas nationella rätt.

3.2.1.3 Inbyggt dataskydd och dataskydd som standard

I dataskyddsförordningen har även principerna inbyggt *dataskydd* och *dataskydd som standard* kodifierats. Inbyggt dataskydd innebär att verksamheten ska ta hänsyn till integritetsskyddsreglerna redan när it-tjänst/system och *rutiner* utformas. Det är ett effektivt sätt

säkerställa att kraven i dataskyddsförordningen uppfylls och att individens personliga integritet skyddas. Dataskydd som standard innebär i korthet att verksamheten som behandlar personuppgifter ska säkerställa att personuppgifter i standardfallet inte behandlas i onödan, exempelvis genom att förvalda inställningar i en tjänst är satta så att inte mer information än nödvändigt samlas in, delas eller visas.

3.2.2 Kommunstyrelsens arbete

Nedan beskrivs kommunstyrelsens arbete och hur dataskydd är organiserat inom Stockholms stad och kommunstyrelsen.

3.2.2.1 Stadsövergripande funktion för informationssäkerhet och dataskydd

Stockholm stad har en stadsövergripande funktion för informationssäkerhet och dataskydd som är placerad på kommunstyrelsens förvaltning, stadsledningskontoret. I funktionen för stadsövergripande informationssäkerhet och dataskydd ingår att styra och följa upp det stadsövergripande informationssäkerhets- och dataskyddsarbetet inom Stockholms stad. I det styrande uppdraget ingår att ansvara för framtagande av riktlinjer och anvisningar avseende informationssäkerhet och dataskydd.

Funktionen för stadsövergripande informationssäkerhet och dataskydd tar även fram metodstöd, handböcker, mallar, utbildningsmaterial och liknande som ger stöd för olika analyser och aktiviteter som ska utföras i nämnder och bolagsstyrelser i Stockholms stad.

3.2.2.2 Operativa informationssäkerhets- och dataskyddsutföraransvaret

Det operativa informationssäkerhets- och dataskyddsutföraransvaret åligger respektive nämnd och bolagsstyrelse i Stockholms stad. Som stöd till verksamheten i kommunstyrelsens dataskyddsutföraransvar finns idag en informationssäkerhetssamordnare och dataskyddshandläggare.

3.2.2.3 Riktlinje för informationssäkerhet

En ny riktlinje för informationssäkerhet i Stockholms stad som anger kommunfullmäktiges direktiv för stadens informationssäkerhetsarbete är framtagen och ska inom kort beslutas av kommunfullmäktige. Riktlinjen kompletteras med tillämpningsanvisningar som detaljerar krav för olika delområden i informationssäkerhetsarbetet, exempelvis informationsklassning och behörighetshantering.

I den nya riktlinjen för informationssäkerhet beskrivs även behov av lokalt framtagna styrdokument, såsom anvisning som beskriver hur de övergripande reglerna för informationssäkerhets- och dataskyddsarbetet tillämpas i den egna verksamheten innefattande exempelvis hur den lokala informationssäkerhetsorganisationen ser ut, dess mandat och resurser, vem som ansvarar för att ta fram lokala styrdokument, hur arbetet följs upp med mera. Kommunstyrelsen ansvarar för att de lokala styrdokumenten upprättas för den egna verksamheten.

3.2.2.4 Stadsledningskontorets dataskyddsråd

Då kommunstyrelsen har både en stadsövergripande funktion för dataskydd samt en lokal stödfunktion för dataskydd har stadsledningskontorets dataskyddsråd upprättats för att funktionerna ska kunna effektivt samarbeta och internt sortera de aktuella dataskyddsfrågor som inkommer till funktionerna. Dataskyddsombudet ingår i stadsledningskontorets dataskyddsråd.

3.2.2.5 Kommunstyrelsens rutiner och instruktioner avseende personuppgiftsbehandling

I samband med registerförteckningen har chefers och medarbetares kunskap om ett lokalt behov av anvisningar, rutiner, instruktioner och metodstöd avseende dataskydd och personlig integritet ökat. Framtagande av styrdokument har inte ingått i projektdirektivet, men direktivet har som en positiv effekt genererat i att nya rutiner och instruktioner avseende dataskydd tagits fram, exempelvis en rutin för kommunstyrelsen fritextfält, flertalet särskilda informationstexter om personuppgiftsbehandling och instruktion gällande publicering av personuppgifter inom Stockholm webb.

Informationssäkerhetssamordnare och dataskyddshandläggare kommer under 2022 samla all information om lokal informationssäkerhet och dataskydd på en ny intranätssida, där styrdokument, anvisningar, rutiner, instruktioner, metodstöd och checklistor avseende dataskydd exempelvis kan finnas eller länkas till som kan utgöra stöd till verksamheten. Ett kartläggningsarbete har även påbörjats gällande vilka rutiner och instruktioner avseende dataskydd som finns på plats och vilka som behöver kompletteras med på lokal nivå i samråd med dataskyddsombudet.

3.2.3 Utveckling av praxis

Integritetsskyddsmyndigheten tillsynsbeslut och samrådssvar visar på vikten av att ha styrdokument implementerade i verksamheten. I tillsynsbeslut framgår även vikten av att medarbetare och personuppgiftsbiträden får kännedom om och utbildning i de styrdokument, anvisningar, rutiner, instruktioner och beslut avseende dataskydd som har tagits fram.

Att ha organisatoriska åtgärder såsom instruktioner på plats för att säkerställa en säkerhetsnivå som är lämplig är något som är av särskild vikt och Integritetskyddsmyndigheten har även tilldelat personuppgiftsansvarig verksamhet sanktioner när det saknats skriftliga rutiner och instruktioner till medarbetare för behandling av personuppgifter eller dessa inte följts på grund av bristande kännedom.

3.2.4 Dataskyddsombudets råd till kommunstyrelsen

Lagstiftningens krav på specifika rutiner och instruktioner avseende dataskydd gör att dataskyddsombudet rekommenderar att kommunstyrelsens verksamhet under 2022 prioriterar framtagandet av ytterligare rutiner och instruktioner gällande hur personuppgifter får behandlas.

Det är även viktigt att medarbetare och personuppgiftsbiträden får kännedom om dessa rutiner och instruktioner. Den kartläggning som redan görs kan fungera som ett stöd och det fortsatta arbetet rekommenderas att samrådas med dataskyddsombudet. En instruktion som särskilt bör prioriteras är hur personuppgifter får hanteras i e-post internt och externt.

3.3 Tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar

3.3.1 Gällande lagstiftning

Kärnan i dataskyddsförordningen är att skydda individens personliga integritet och värna individens rättigheter och friheter. Detta görs med hjälp av tekniska och organisatoriska åtgärder.

I Artikel 32 i dataskyddsförordningen anges;
Med beaktande av den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige och personuppgiftsbiträdet vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken, inbegripet, när det är lämpligt
- pseudonymisering och kryptering av personuppgifter,
- förmågan att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingssystemen och behandlingstjänsterna,
- förmågan att återställa tillgängligheten och tillgången till personuppgifter i rimlig tid vid en fysisk eller teknisk incident,
- ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet.

Personuppgifter som enligt lag definieras som särskilda kategorier av personuppgifter det vill säga känsliga personuppgifter och integritetskänsliga personuppgifter kräver en högre säkerhetsnivå. Andra personuppgifter kan även beroende på sin art, omfattning, sammanhang och ändamål kräva en högre säkerhetsnivå.

Känsliga personuppgifter är uppgifter som avslöjar etniskt ursprung, politiska åsikter, religiös övertygelse eller filosofisk övertygelse eller medlemskap i fackförening och behandling av genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning.

Integritetskänsliga personuppgifter är exempelvis löneuppgifter, uppgifter om lagöverträdelser, värderande uppgifter, exempelvis uppgifter från utvecklingssamtal, uppgifter om resultat från personlighetstester eller personlighetsprofiler, information som rör någons privata sfär och uppgifter om sociala förhållanden.

Överföring av personuppgifter till tredjeländer och internationella organisationer kräver om, inte adekvansbeslut av EU-kommissionen finns, även kompletterande tekniska och organisatoriska skyddsåtgärder om tredjeland inte kan garantera ett likvärdigt skydd för individ såsom under vår gällande dataskyddslagstiftning inom EU/EES.

Organisatoriska åtgärder har redogjorts för ovan under kapitel 3.2 Styrdokument avseende dataskydd.

3.3.2 Kommunstyrelsens dataskyddsroll och arbete

3.3.2.1 Kommunstyrelsens ansvar för stadsgemensam it

Enligt reglementet för kommunstyrelsen, Kfs 2021:5, ansvarar kommunstyrelsen för att leda, strategiskt utveckla och samordna stadens gemensamma it- och digitaliseringsfrågor och att vara systemägare för vissa stadsövergripande system.

När kommunstyrelsen behandlar personuppgifter för annan nämnds och bolags räkning inom Stockholms stad är kommunstyrelsen personuppgiftsbiträde. Enligt dataskyddsförordningen har numera personuppgiftsbiträdet utökade skyldigheter och ett eget ansvar för personuppgiftsbehandlingen, exempelvis att föra register över behandlingar och att säkerställa en lämplig säkerhetsnivå. Ett personuppgiftsbiträde kan även påföras administrativ sanktionsavgift.

Mot bakgrund av att kommunstyrelsen är systemägare till stadsövergripande system och tillhandahåller stadsgemensamma it-infrastrukturen är det viktigt att beakta att kommunstyrelsen har ett eget ansvar gällande de tekniska åtgärderna och behöver säkerställa en säkerhetsnivå som är lämplig för faktisk personuppgiftsbehandling som sker i dessa system eller tjänster.

3.3.2.2 Informationsklassning av personuppgiftsbehandling

Stockholms stads informationstillgångar ska informationsklassas enligt gällande riktlinjer för informationssäkerhet. Ett omfattande kartläggningsarbete pågår av nytillträdd informationssäkerhetssamordnare avseende vilka informationstillgångar/tjänster/system som är informationsklassade och vad som kvarstår. Verksamheten uppdaterar och utför idag

löpande informationsklassningar, men flera klassningar återstår att genomföra och implementera.

Då gällande lagstiftningen kräver en adekvat skyddsnivå beroende på personuppgiftsbehandlingens art, omfattning, sammanhang och ändamål är det ur ett dataskyddsperspektiv viktig att tillse att de tekniska och organisatoriska åtgärderna faktiskt är implementerade för att informationsägare och tillika personuppgiftsansvarig ska kunna behandla sina personuppgifter på ett lagenligt och säkert sätt.

3.3.3 Utveckling av praxis

Integritetsskyddsmyndighetens och andra EU/EES-tillsynsmyndigheters tillsynsbeslut påvisar vad som utgör brister avseende organisatoriska och tekniska skyddsåtgärder för att säkerställa en lämplig säkerhetsnivå för personuppgiftsbehandling.

Advokatbyrån DLA Piper analyserar årligen dataskydds-överträdelser och administrativa sanktionsavgifter och i deras årliga analys för 2020 framkom att brister i det organisatoriska och tekniska säkerhetsskyddet har utmynnat i bland de högsta administrativa sanktionsavgifterna.

3.3.4 Dataskyddsombudets råd till kommunstyrelsen

Dataskyddsombudet rekommenderar att informationsklassningar prioriteras och implementeringen av de i klassningen kravställda skyddsåtgärderna. Det kommunstyrelsens verksamhet särskilt ska fokusera på är således att säkerställa att tekniska och organisatoriska skyddsåtgärder faktiskt är implementerade i linje med gällande lagstiftning.

Generellt behöver förmågan att informationsklassa och implementera informationsklassningen förbättras och processen fungerar idag inte fullt ut tillfredsställande. Medarbetare behöver även utbildas gällande informationsklassning och dataskydd.

Dataskyddsombudet ser emellertid positivt på att det i ny riktlinje för informationssäkerhet i Stockholms stad ges en ökad tydlighet kring ansvar och roller, vilket kommer att bidra till förstärkt dataskydd på sikt.

3.4 Konsekvensbedömningar

3.4.1 Gällande lagstiftning

I dataskyddslagstiftningen finns det numera en skyldighet att genomföra en konsekvensbedömning avseende dataskydd.

> *Om en typ av behandling, särskilt med användning av ny teknik och med beaktande av dess art, omfattning, sammanhang och ändamål, sannolikt leder till en hög risk för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige före behandlingen utföra en bedömning av den planerade behandlingens konsekvenser för skyddet av personuppgifter. En enda bedömning kan omfatta en serie liknande behandlingar som medför liknande höga risker.*

Hög risk kan enligt Integritetsskyddsmyndigheten exempelvis vara att det saknas tillräckliga säkerhetsåtgärder, så att "fel" personer får tillgång till personlig eller känslig information, till exempel uppgifter som kan leda till risker för individ, såsom diskriminering, identitetsstöld, bedrägeri, ekonomisk förlust eller skadat anseende.

Integritetsskyddsmyndigheten beskriver konsekvensbedömning som en process för att ta reda på vilka risker som finns med att behandla personuppgifter, ta fram rutiner och åtgärder för att bemöta dessa risker och visa att personuppgiftsansvarig uppfyller dataskyddsförordningens krav. Syftet med konsekvensbedömning avseende dataskydd är således att förebygga risker för individ innan de uppkommer.

Kravet att utföra en konsekvensbedömning föreligger *innan* en personuppgiftsbehandling påbörjas, om risken med en pågående behandling ändras och för pågående behandlingar om konsekvensbedömning inte utförts tidigare.

Integritetsskyddsmyndigheten har enligt gällande lagstiftning antagit en förteckning över när en konsekvensbedömning ska utföras. Förteckningen finns publicerad på Integritetsskydds-myndighetens webbplats[5].

[5] Förteckning över när en konsekvensbedömning ska göras | IMY.

3.4.2 Kommunstyrelsens arbete

Kommunstyrelsen har idag en rutin och ett metodstöd för att utföra konsekvensbedömningar avseende dataskydd. Rutin och metodstöd ses nu över och uppdateras av funktionen informationssäkerhet centralt tillsammans med juridiska avdelningen med hänsyn till den utveckling av praxis som skett.

Ett arbete pågår även av informationssäkerhetssamordnare tillsammans med dataskyddsombudet för att klargöra sambanden mellan registerförteckning, informationsklassning, tekniska och organisatoriska skyddsåtgärder, riskanalys och konsekvensbedömning avseende dataskydd. Arbetet syftar bland annat till att öka förståelsen för konsekvensbedömning avseende dataskydd och när en konsekvensbedömning behöver utföras av kommunstyrelsen.

Då kommunstyrelsen enligt dataskyddsförordningen kan inneha både ansvarsrollen personuppgiftsansvarig och personuppgiftsbiträde innebär i detta hänseende att ansvarsrollen för kommunstyrelsen initialt behöver fastställas, då det är den personuppgiftsansvarige som ska utföra konsekvensbedömningen och personuppgiftsbiträdet ska bistå den personuppgiftsansvarige med att tillse att skyldigheten fullgörs.

Kommunstyrelsens verksamhet är således skyldig att identifiera behovet och utföra eller bistå vid konsekvensbedömningar. Dataskyddshandläggare och informationssäkerhetssamordnare i samråd med dataskyddsombudet sammanställer nu, till stöd för verksamheten, vilka personuppgiftsbehandlingar som behöver konsekvensbedömas för att öka förståelsen och främja utförandet av konsekvensbedömningar.

3.4.3 Utveckling av praxis

Konsekvensbedömning avseende dataskydd är enligt lagstiftningen en metod och process för att förebygga risker avseende personlig integritet innan de uppkommer.

I tillsynsbeslut avseende personuppgiftsincidenter synliggörs att konsekvensbedömningar avseende dataskydd vanligtvis inte har utförts, vilket är en försvårade omständighet för personuppgiftsansvarig och är i sig sanktionsgrundande.

3.4.4 Dataskyddsombudets råd till kommunstyrelsen

Dataskyddsombudet är positiv till att informationssäkerhet centralt tillsammans med juridiska avdelningen uppdaterar metodstödet för konsekvensbedömning för Stockholms stads nämnder och bolagsstyrelser, så det är korrekt, enkelt, relevant och väl kommunicerat, vilket i sig kan öka användandet av metodstödet.

Ett medskick från dataskyddsombud till kommunstyrelsen och dess medarbetare i detta sammanhang är att konsekvensbedömningen avseende dataskydd alltid ska utgå från personuppgiftsbehandlingen, då det är risker för individ och hur dessa risker ska omhändertas som ska vara i fokus.

3.5 Individens rättigheter

3.5.1 Gällande lagstiftning

Individens, den registrerades, rättigheter beskrivs i dataskyddsförordningen. Individen har rätt till specifikt angiven information om hur personuppgifterna behandlas, rätt till tillgång till sina personuppgifter som behandlas, registerutdrag. Individen har i vissa fall avseende kommunstyrelsens behandling rätt till rättelse och radering samt rätt till dataportabilitet av sina personuppgifter. Individen har även rätt att begära begränsning av sin personuppgiftsbehandling och att invända mot personuppgiftsbehandlingen.

När den personuppgiftsansvarige hanterar rättigheterna, ska informationen vara tydlig och i lätt tillgänglig form med användning av ett klart och tydligt språk.

3.5.2 Kommunstyrelsens arbete

KF/KS Kansli hanterar för kommunstyrelsens del alla frågor som rör individens rättigheter enligt dataskyddsförordningen. Det innebär att KF/KS Kansli samordnar och säkerställer att berörd individs begäran avseende dataskyddsförordningens rättigheter behandlas och ger svar och beslut till individen.

KF/KS Kansli samarbetar med dataskyddsombudet vid hantering av rättigheterna och vid uppdatering av rutin och metodstöd för hur rättigheterna ska hanteras av kommunstyrelsen.

Alla frågor och individs begäran om rättighet som har inkommit till kommunstyrelsen har hanterats inom föreskriven lagstadgad tidsram om trettio dagar. Årligen hanteras fyra till fem stycken inkomna begäranden avseende den registrerades rättigheter som avser kommunstyrelsen behandling av personuppgifter som personuppgiftsansvarig.

3.5.3 Utveckling av praxis

Gällande lagstiftning ska värna om individen och skyddet för den personliga integriteten. EU-domstolen har därför särskilt pekat på att tillsynsmyndigheterna ska utreda de individuella klagomål som inkommer till tillsynsmyndigheterna.

Det innebär att Integritetsskyddsmyndigheten inte längre helt fullt kan välja vilka ärenden som den ska prioritera samt att flera riktade tillsynsärenden kan förväntas för att värna den specifika individens rättigheter. Integritetsskyddsmyndighetens tillsynspolicy och tillsynsplan innefattar nu ett övergripande fokus på att utreda klagomål från enskilda, där tillsynsmyndigheten i klagomålshanteringen utför en fördjupad bedömning av samtliga klagomål.

3.5.4 Dataskyddsombudets råd till kommunstyrelsen

Dataskyddsombudets råd är att utveckla det arbete som görs gällande hantering av individens rättigheter och att beakta att inflödet av inkomna frågor och begäranden avseende individens rättigheter kan öka.

Om klagomål från individ avseende dataskydd inkommer bör verksamheten involvera dataskyddsombudet.

3.6 Personuppgiftsincidenter

3.6.1 Gällande lagstiftning

En personuppgiftsincident inträffar när de personuppgifter som kommunstyrelsen behandlar och ansvarar för drabbas av en säkerhetsincident som resulterar i ett brott mot konfidentialitet, tillgänglighet eller riktighet avseende individens personuppgifter.

Vid en personuppgiftsincident[6]ska den personuppgiftsansvarige utan onödigt dröjsmål och, om så är möjligt, inte senare än 72 timmar efter att ha fått vetskap om den, anmäla personuppgiftsincidenten till den tillsynsmyndighet som är behörig, såvida det inte är osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter.

Personuppgiftsbiträdet ska underrätta den personuppgiftsansvarige utan onödigt dröjsmål efter att ha fått vetskap om en personuppgiftsincident.

Den personuppgiftsansvarige ska dokumentera alla personuppgiftsincidenter, inbegripet omständigheterna kring personuppgiftsincidenten, dess effekter och de korrigerande åtgärder som vidtagits. Dokumentationen ska göra det möjligt för tillsynsmyndigheten att kontrollera efterlevnaden.

Om personuppgiftsincidenten sannolikt leder till en hög risk för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige utan onödigt dröjsmål informera den registrerade om personuppgiftsincidenten.

Tillsynsmyndigheterna i EU/EES samarbetar och tar fram riktlinjer avseende dataskydd. Riktlinjer finns om anmälan av personuppgiftsincidenter enligt förordning (EU) 2016/679, WP250 rev.01[7]. Enligt gällande dataskyddslagstiftning måste alla lämpliga tekniska skyddsåtgärder och organisatoriska åtgärder ha vidtagits för att omedelbart kunna fastställa om en personuppgiftsincident har ägt rum. I detta ingår att ha förmåga att upptäcka, åtgärda, förebygga och rapportera personuppgiftsincidenter för att förhindra konsekvenser som exempelvis diskriminering, identitetsstöld, bedrägeri, förlorat anseende och ekonomisk förlust för individ.

I ovan nämnd riktlinje anges att personuppgiftsansvarige bör ha interna rutiner för att upptäcka och åtgärda en incident. I riktlinjen anges även att ”För att hitta oriktigheter i databehandlingen kan den personuppgiftsansvarige eller personuppgiftsbiträdet använda vissa tekniska åtgärder som dataflödes- och logganalysinstrument. Med hjälp av dessa kan man definiera händelser och varningar genom att korrelera loggdata”[8].

[6] en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.
[7] wp250rev_en (imy.se)
[8] Observera att loggdata kan klassificeras som personuppgifter och ska hanteras enligt gällande dataskyddslagstiftning.

3.6.2 Kommunstyrelsens arbete

Kommunstyrelsen har rutiner för att hantera personuppgifts-incidenter. Potentiella personuppgiftsincidenter utreds och systemägare och förvaltningsledare tar ofta kontakt med dataskyddsombudet vid utredning av en potentiell personuppgiftsincident.

3.6.2.1 Anmälda personuppgiftsincidenter till tillsynsmyndigheten

I kommunstyrelsen diarium finns idag tre personuppgiftsincidenter som avser kommunstyrelsens verksamhet, i egenskap av personuppgiftsansvarig, som anmälts till IMY. En av dessa anmälningar har återkallats, då kompletterande utredning visade att händelsen inte utgjorde en personuppgiftsincident. Om personuppgiftsincident upptäcks som ska anmälas till Integritetsskyddsmyndigheten har anmälan inom 72 timmar efter vetskap gjorts. De berörda individerna av personuppgiftsincidenten har kontaktats i två av de tre diarieförda personuppgiftsincidenterna.

3.6.2.2 Förmåga att upptäcka och identifiera personuppgiftsincidenter

Under 2022 ska arbete påbörjas med att etablera en CERT, Computer Emergency Response Team. En CERT avser förmågan att upptäcka, hantera och förebygga it-säkerhetsincidenter. Att ha förmåga att upptäcka, hantera och förebygga it-säkerhetsincidenter kommer att öka förmågan att upptäcka, åtgärda och förebygga även personuppgiftsincidenter.

3.6.2.3 Informationsplikt som personuppgiftsbiträde

Ovan har under 3.3.2.1 kommunstyrelsens ansvar för stadsgemensam it redogjorts för kommunstyrelsens ansvarsroller både som personuppgiftsansvarig och personuppgiftsbiträde. Då kommunstyrelsen kan vara personuppgiftsbiträde till annan nämnd och bolagsstyrelse inom Stockholms stad behöver kommunstyrelsen även iaktta skyldigheterna som ett personuppgiftsbiträde har att uppfylla. Personuppgiftsbiträdet ska underrätta personuppgiftsansvarig, utan onödigt dröjsmål, efter att ha fått vetskap om en personuppgiftsincident och tillhandahålla i lag

specificerad information till personuppgiftsansvarig för att ansvarig ska kunna uppfylla sina skyldigheter och utreda om anmälan till tillsynsmyndighet behöver ges in och om berörd individ ska informeras om personuppgiftsincidenten.

3.6.2.4 Dokumentationsskyldigheten

En skyldighet att dokumentera alla personuppgiftsincidenter föreligger oavsett om de anmälts eller inte till Integritetsskyddsmyndigheten. Enligt kommunstyrelsen rutin ska alla personuppgiftsincidenter dokumenteras i ett i rutinen angivet system. Detta system utreds för närvarande för att fastställa huruvida systemet omhändertar de verksamhetsbehov som ställs eller inte.

I den granskande rollen ser även dataskyddsombudet att det till viss del finns personuppgiftsincidenter dokumenterade i systemet, men att samtliga kategorier av incidenter behöver kontrolleras för att få fram informationen. Det saknas således ett enkelt och tydligt register över kommunstyrelsens personuppgiftsincidenter som dataskyddsombudet kan ta del av och granska. Integritetsskyddsmyndigheten kan i sin tillsynsroll även komma att begära att få ta del av kommunstyrelsens personuppgiftsincidentregister för att granska och kontrollera regelefterlevnad.

3.6.3 Utveckling av praxis

Integritetsskyddsmyndigheten sammanställer varje år en rapport avseende anmälda personuppgiftsincidenter, se exempelvis Anmälda personuppgiftsincidenter 2020 | IMY. Syftet med rapporten är att bidra till en kunskapshöjning om integritet och dataskydd.

I rapporten framkommer att den vanligaste incidenten år 2020 och 2019 är felskickade mejl eller brev, obehörigt röjande. Den vanligaste orsaken till att en personuppgiftsincident uppkommer är den mänskliga faktorn, vilket belyser vikten av att ha fungerande styrdokument, tekniska skyddsåtgärder, rutiner och instruktioner avseende personuppgiftsbehandling på plats.

Efter felskickade mejl och brev är obehörig åtkomst den näst största kategorin av anmälda personuppgiftsincidenter. Obehörig åtkomst

innebär att någon olovligen berett sig tillgång till personuppgifter, exempelvis till följd av att behörigheter till ett it-system har tilldelats för generellt eller felaktigt. Den tredje största kategorin anmälda personuppgiftsincidenter avser obehörigt röjande. Obehörigt röjande innebär att den personuppgiftsansvarige behandlat personuppgifter på ett vis så att personuppgifterna kommit obehöriga till kännedom, på grund av exempelvis tekniska brister i en it-tjänst eller it-system.

3.6.4 Dataskyddsombudets råd till kommunstyrelsen

Framtagna personuppgiftsincidentrutiner måste fungera i praktiken när en personuppgiftsincident uppkommer. Det innebär att rutinerna måste testas och övas av verksamheten. Vid testning och övning bör rutinerna vid behov justeras för att främja skyddet för individ och regelefterlevnad.

Vid framtagande av CERT bör effektivitetsvinster och samband mellan it-säkerhetsincidenter och personuppgiftsincidenter inte gå förlorade, utan fångas upp där det är möjligt. Detta för att öka kommunstyrelsen förmåga att upptäcka personuppgiftsincidenter och för att skydda individs personliga integritet.

Medarbetare och andra som behandlar personuppgifter behöver löpande utbildas för att deras kunskap och medvetande avseende personuppgiftsincidenter ska öka. Tidsramen som är inbyggd i dataskyddsförordningen kräver att ansvariga och medarbetare som hanterar personuppgiftsincidenter är insatta i regelverket och rutinen samt att de i förväg övat in rutinen. Tidsramen kräver även att i förväg utpekade ansvariga utsetts och att dataskyddsombudet omgående involveras.

Generellt är förmågan att hantera personuppgifter idag inte fullt ut tillfredsställande och det är av vikt att aktiviteter enligt ovan utförs.

4 Genomförda granskningar under året

Dataskyddsombudet har under 2021 gjort riktade granskningar kopplade till projektdirektivet avseende kommunstyrelsens dataskyddsarbete.

Råden och rekommendationerna avseende granskningarna har omhändertagits av verksamheten och bland annat resulterat i framtagande av en systematik för att hantera en enhetlig digitaliserad registerförteckning, att öka utförandet och implementering av informationsklassning samt att förståelsen att tillämpa metoden konsekvensbedömning avseende dataskydd ökat bland medarbetare. I granskningarna har även ytterligare behov av organisatoriska skyddsåtgärder synliggjorts och instruktioner upprättats. Framtagande av instruktioner avseende personuppgiftsbehandling behöver fortsätta och en enligt dataskyddsombudet prioriterad instruktion avser personuppgiftsbehandling i intern och extern e-post, där tjänsten säkra meddelanden kan lyftas och spridas information om.

5 Risker inom dataskydd

Innan en personuppgiftsbehandling påbörjas och utförs ska den personuppgiftsansvarige alltid bedöma de risker som är förenade med behandlingen.

Dataskyddsförordningen är uppbyggd på så vis att riskanalyser avseende dataskydd ska utföras, uppdateras och dokumenteras av personuppgiftsansvarig. Det innebär att kommunstyrelsen behöver utföra riskanalyser avseende dataskydd.

Nedan följer en kort beskrivning av riskanalys av dataskydd och kommunstyrelsens dataskyddsansvar utifrån ansvarsrollerna i dataskyddsförordningen. Kapitlet avslutas med generella råd från kommunstyrelsens dataskyddsombud.

5.1 Riskanalys

En riskanalys avseende dataskydd ska utföras med individen i fokus, det vill säga den personuppgiftsansvarige ska bedöma om behandlingen kan äventyra den registrerades friheter och rättigheter, särskilt personuppgifter, och om personuppgiftsbehandlingen kan orsaka den registrerade fysisk, materiell eller immateriell skada.

I riskanalysen identifieras de åtgärder som den personuppgifts-ansvarige ska genomföra för att omhänderta riskerna och trygga en korrekt, proportionell och säker personuppgiftsbehandling. En riskminimerande åtgärd är att beakta de grundläggande principerna

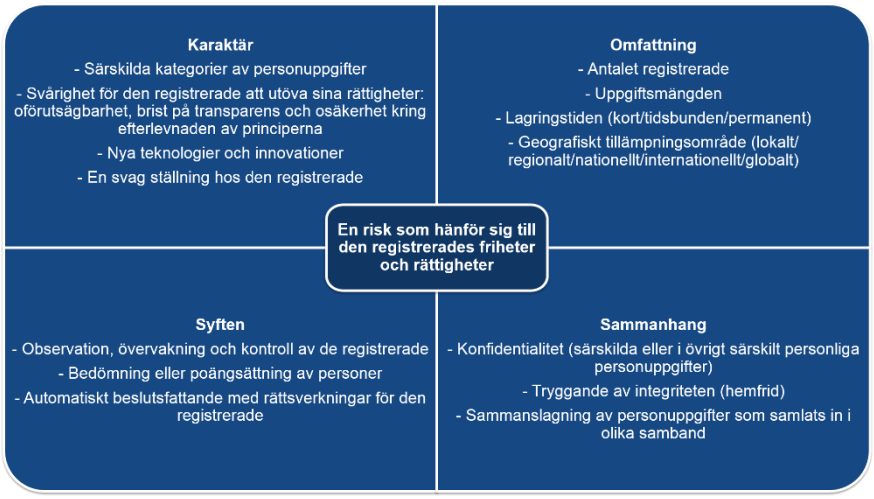
och att laglig grund bedöms innan en personuppgiftsbehandling påbörjas. De grundläggande principerna har redogjorts för ovan i kapitel 3 Obligatoriska rapporteringsområden.

I riskanalysen avseende dataskydd ska även sannolikheten för att risken realiseras och allvaret och olägenheten för individ om risken realiseras bedömas.

5.1.1 Personuppgiftsansvarigs ansvar

Personuppgiftsansvarig ska utifrån personuppgiftsbehandlings art (karaktär), omfattning, sammanhang, ändamål (syften) och riskerna för fysiska personers rättigheter och friheter genomföra lämpliga tekniska och organisatoriska åtgärder.

Den finska tillsynsmyndigheten har tagit fram bilden nedan för att beskriva karaktär, omfattning, syften och sammanhang i samband med riskanalys avseende dataskydd.



5.1.2 Personuppgiftsbiträdets ansvar

Utifrån att kommunstyrelsen ansvarar för stadsgemensam it och innehar ett sanktionsgrundande eget ansvar som personuppgiftsbiträde enligt dataskyddsförordningen för de tekniska och organisatoriska åtgärderna blir det särskilt viktigt att säkerställa att tekniska och organisatoriska skyddsåtgärder är implementerade och att inhämta en instruktion från personuppgiftsansvarig nämnd och bolagsstyrelse inom Stockholms stad avseende personuppgiftsbehandlingen. I instruktionen ska bland annat

personuppgiftsbehandlingen specificeras, typ av personuppgifter och kategori av registrerade framgå, vilket underlättar hanteringen för kommunstyrelsen och att rätt skyddsåtgärder implementeras.

Ovan innebär att även systemägare och förvaltningsledare[9] behöver ha god kännedom om dataskyddslagstiftningen och vad de specifikt behöver utföra eller inhämta från informationsägare tillika personuppgiftsansvarig gällande dataskydd. Det rekommenderas att systemägare och förvaltningsledare på stadsledningskontoret tar del av upprättad GDPR-årsrapport – Stockholms stads kommunstyrelse.

Systemägare och förvaltningsledare behöver även ha god kunskap om och utbildning i hantering av personuppgiftsincidenter.

5.1.3 Inbyggt dataskydd och dataskydd som standard

Vid riskanalys avseende dataskydd behöver även beaktas att pandemin har gjort oss än mer digitala, att omvärldsbevakning visar på en kraftigt ökande hotbild avseende it-attacker och att innovation av IoT-lösningar och AI ökar digitaliseringens komplexitet, vilket påverkar individens rätt till och behov av skydd för sin personliga integritet. Att tillämpa och implementera inbyggt dataskydd och dataskydd som standard enligt dataskyddsförordningen är en riskminimerande åtgärd i detta sammanhang.

5.2 Dataskyddsombudets råd till kommunstyrelsen

Dataskyddsförordningen och kompletterande lagstiftning uppställer omfattande krav som behöver efterlevas för att individens personliga integritet ska skyddas och individens friheter och skyldigheter ska värnas.

I den praxis som nu utvecklas genom tillsynsbeslut med administrativa sanktionsavgifter framgår vad som krävs av den personuppgiftsansvarige och personuppgiftsbiträdet för att efterleva gällande dataskyddslagstiftning.

Att efterleva dataskyddsförordningen kräver att dataskydds-processerna i verksamheten är definierade, kända och proaktiva. Processer som är oförutsägbara, reaktiva och saknar uppföljning

[9] Rollerna får en annan benämning enligt styr- och samverkansmodell pm³. Detta beaktas i GDPR-årsrapporten för 2022.

resulterar i att dataskyddsarbetet bedrivs ad hoc och att riskerna för individ ökar.

Kommunstyrelsen behöver säkerställa att det faktiska dataskyddsarbetet är definierat, känt och proaktivt för att därefter säkerställa att processer, rutiner och instruktioner efterlevs, utvecklas och motsvarar gällande dataskyddslagstiftning. Kommunstyrelsens dataskyddsombud och stödfunktionerna såsom informationssäkerhetssamordnare och dataskyddshandläggare kan bistå i detta arbete.

Avsikten med råden i denna rapport är att öka mognadsgraden avseende dataskydd och att minska dataskyddsriskerna samt arbeta mot en utvecklad och proaktiv regelefterlevnad. Dataskyddsombudet välkomnar att dataskyddsombudets råd omhändertas av stadsledningsledningskontoret för implementering och om dataskyddsombudets råd beaktats och implementerats kommer att granskas av dataskyddsombudet och beskrivas i årsrapporten för 2022.

Vikten av att dataskydd ska in tidigt i processerna kan inte nog betonas och ställer även krav på att dataskydd omhändertas vid upphandling. Att tillse att dataskyddsombudet deltar i planeringsstadiet inför personuppgiftsbehandling och ges möjlighet att granska dataskyddsstrategin i kommunstyrelsens roll som personuppgiftsansvarig och personuppgiftsbiträde höjer även mognadsgraden och är linje med dataskyddsombudets lagreglerade ställning och uppgifter.

6 Planerade granskningar under det nya verksamhetsåret

6.1 Planerad granskning

I dataskyddsombudets lagreglerade uppgifter ingår bland annat att övervaka verksamhetens efterlevnad av dataskyddsförordningen och kompletterande lagstiftning, strategin för skydd av personuppgifter och ansvarstilldelning.

Dataskyddsombudet kommer under 2022 granska hur dataskyddsombudets råd i denna rapport har hanterats. Vidare kommer även kvalitén och fullständigheten av kommunstyrelsens registerförteckning granskas tillsammans med verksamheten. Ett

annat område som dataskyddsombudet kommer att granska är om tredjelandsöverföringar hanteras enligt gällande EU-vägledningar[10]. Andra granskningar och rådgivning, gällande exempelvis AI och IoT-lösningar, kan även företas i samråd med verksamheten.

6.1.1 EU-domstolens Schrems II-dom

Stockholms stads kommunstyrelse har bedrivit ett omfattande arbete i samråd med dataskyddsombudet med anledning av EU-domstolens dom, Schrems II-domen, meddelad den 16 juli 2020. EU-domstolen ogiltigförklarade Privacy-Shield-avtalet mellan EU och USA, då avtalet inte gav ett tillräckligt skydd för personuppgifter när dessa fördes över till eller gavs åtkomst till mottagare i USA.

Ogiltigförklarandet har sin grund i de ingrepp som amerikansk underrättelseverksamhet kan vidta med stöd i den amerikanska lagstiftningen. Ingreppen ansågs av EU-domstolen inte vara proportionerliga och att ett icke väsentligt likvärdigt dataskydd i jämförelse med dataskyddsförordningen saknades vid tredjelandsöverföring till USA.

EU-domstolen ogiltigförklarade däremot inte EU-kommissionens beslut om standardavtalsklausuler och dessa klausuler kan fortsatt användas vid överföring till länder utanför EU/EES. Vid användandet av standardavtalsklausuler kan emellertid ytterligare tekniska och organisatoriska skyddsåtgärder behöva implementeras, om tredjelands lagstiftning eller praxis inte kan anses tillförsäkra en i allt väsentligt likvärdig skyddsnivå för personuppgifterna som inom EU/EES.[11]

[10] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data Version 2.0 Adopted on 18 June 2021, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data | European Data Protection Board (europa.eu)
Rekommendationer 02/2020 om europeiska nödvändiga garantier för övervakningsåtgärder Antagna den 10 november 2020, edpb_recommendations_202002_europeanessentialguaranteessurveillance_sv.pdf (europa.eu)

[11] Se fotnot 10 för vägledningar som tillkommit efter EU-domen, Shrems-II domen.

6.1.2 Inhämtning av dataskyddsombudets råd

Stockholms stads kommunstyrelses dataskyddsombuds rekommendationer har inhämtats med anledning av Schrems II-domen. Dataskyddsombudet har lämnat råd om kartläggning, leverantörskontroller, riskvärdering och konsekvensbedömning avseende dataskydd.

Dataskyddsombudets granskning av tredjelandsöverföring syftar till att utreda om verksamheten arbetar likartat med frågorna, om lärdomar kan dras internt av arbetet och hur arbetet står sig i jämförelse med dataskyddsförordningen och uppdaterad EU-vägledning.

7 Övrigt att rapportera

7.1 Utbildning avseende dataskydd

Dataskyddsombudet vill i samband med årets rapport synliggöra att dataskydds- och informationssäkerhetsutbildningar finns på Stockholms stads utbildningsplattform[12]. Idag har Stockholms stad en obligatorisk grundkurs i dataskydd och en i informationssäkerhet för medarbetare i staden. Svarsfrekvensen för kommunstyrelsens medarbetare avseende dessa obligatoriska utbildningar följs upp och redovisas månadsvis. För den intresserade finns även fördjupningskurser i dataskydd och informationssäkerhet på Stockholms stads utbildningsplattform.

7.2 Inhämtning av GDPR-årsrapporter

Årets GDPR-årsrapporter kommer att inhämtas av funktionen informationssäkerhet centralt från samtliga nämnder och bolagsstyrelser, som ett led i att utveckla och följa upp Stockholms stads dataskyddsarbete och förmågan att efterleva dataskyddsförordningen och kompletterande lagstiftning.

Samtliga GDPR-årsrapporter kan även fungera som ett stöd för att identifiera behov av utbildningsinsatser, såsom till exempel betydelsen av att implementera utförd informationsklassning och

[12] https://utbildning.stockholm.se/

vad som utgör en personuppgiftsincident enligt gällande dataskyddslagstiftning.