Stockholms stad

Bilaga 11

GDPR Årsrapport

2024

Norra innerstadens stadsdelsnämnd

GDPR årsrapport
Januari 2025

Dnr: NI 2025/97
Utgivningsdatum: 2025-01-15
Kontaktperson: Marju Stenudd

1 Bakgrund

Dataskyddsförordningen trädde i kraft som lag i Sverige den 25 maj 2018. Syftet med förordningen var att skapa enhetliga dataskyddsregler inom EU avseende respekt för privatlivet och rätten till skydd av personuppgifter enligt artikel 7 och 8 i Europeiska unionens stadga om de grundläggande rättigheterna. Dataskyddsförordningen syftar även till att säkerställa det fria flödet av personuppgifter mellan medlemsstaterna i EU.

Enligt dataskyddsförordningen är varje nämnd och bolagsstyrelse inom Stockholms stad ansvarig för att verksamheten följer dataskyddslagstiftningen vid hantering av personuppgifter. Det innebär att nämnd och bolagsstyrelse behöver informera sig, styra och följa upp sin verksamhet avseende behandlingen av personuppgifter.

Varje nämnd och bolagsstyrelse i Stockholms stad har i enlighet med dataskyddsförordningen utnämnt ett Dataskyddsombud (”DSO”). DSO:n har till uppgift att övervaka verksamhetens integritets- och dataskyddsregelefterlevnad samt att ge rekommendationer och rapportera direkt till högsta förvaltningsnivå.

Denna årsrapport är således ett medel för nämnd och styrelse att ta emot de råd och rekommendationer som DSO:n är skyldig att ge till ansvarig enligt dataskyddsförordningen samt för att få insyn i vad DSO:ns granskande arbete av verksamhetens status avseende integritet och dataskydd visar. Årsrapporten syftar till att nämnd/bolagsstyrelse ska kunna fatta beslut om prioriteringar, resurser och initiativ framåt. Detta samspel resulterar i att det blir enklare för ansvarig nämnd/bolagsstyrelse att visa hur de som personuppgiftsansvarig efterlever dataskyddslagstiftningen.

Dataskyddsförordningen bygger på grundläggande principer och en av dessa principer är ansvarsskyldigheten. Den innebär att nämnd eller bolagsstyrelse ska kunna *visa* att verksamheten efterlever dataskyddsförordningen. Årsrapporten är en mycket viktig del av denna *dokumenteringsskyldighe*t. Årsrapporten är även ett medel för nämnds/bolagsstyrelsens uppföljning och styrning av verksamhetens systematiska integritets- och dataskyddsarbete.

Innehåll

2 Sammanfattning

I egenskap av nämndens utsedda dataskyddsombud lämnar jag följande årsrapport.

Förvaltningens systematiska dataskyddsarbete har utvecklats i jämförelse med föregående år. En organisation för informationssäkerhet och dataskydd har bildats med representanter från varje avdelning samt IT-enheten som fungerat som resurser i dataskyddsarbetet. En avdelnings representant har avsagt sitt uppdrag under hösten och behöver ersättas. DSO föreslår även att nätverket utökas med representanter från inköp och upphandling samt arkiv och registratur för att skapa en helhetssyn i arbetet med dataskydd.

Antalet påbörjade informationsklassningar har ökat markant under året vilket skapar bättre förutsättningar för att tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar har identifierats vilket ökar säkerheten i hanteringen av personuppgifter. Dock saknas tydlighet i vilka steg som genomförts i enlighet med klassningsverktyget KLASSA samt om prioritering av klassningar skett baserat på personuppgiftsbehandlingar som omfattats utifrån känslighet, mängden personuppgifter och antalet personer vars personuppgifter behandlas.

Inga konsekvensbedömningar har genomförts vilket är en kvarvarande allvarlig risk från föregående år.

Revidering och justeringar har skett av registerförteckning av behandlade personuppgifter samt rutin för personuppgiftsincidenter. I granskning har förbättringsområden identifierats i flera styrdokument som ligger till grund för ett systematiskt dataskyddsarbete. Främst bör prioriteras att revidera rutin samt komplettera med process avseende att tillgodose de registrerades rättigheter i enlighet med dataskyddsförordningens artiklar 15-22.

I rapporten framgår DSO:s förslag till aktiviteter att fatta beslut om för ett förbättrat dataskyddsarbete under 2025.

3 Obligatoriska rapporteringsområden

Denna årsrapport spänner över sex obligatoriska rapporteringsområden som Personuppgiftsansvarig (”PUA”) 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 nämndens eller bolagets status och DSO:ns slutsatser samt rekommendationer gällande de obligatoriska rapporteringsområdena efter DSO:ns genomförda uppföljning och granskning.

3.1 Registerförteckning

3.1.1 Sammanfattning

Fråga/kontroll	Svar
Antal behandlingar som är registrerade?	329
Har nödvändiga uppdateringar gjorts?	Till största del
Bedöms registerförteckningen vara fullständig?	Delvis
Har verksamheten lämpliga rutiner för registerföring?	Delvis

3.1.2 Syfte

Dataskyddsförordningen ställer krav på att myndigheten behöver ha en registerförteckning över de personuppgifter som be. handlas. Med att *behandla* menas exempelvis insamla, registrera, eller lagra.

Om förvaltningen arbetar utifrån principen att ha *dataskydd som standard* säkerställs att endast personuppgifter behandlas som är nödvändiga för det specifika ändamålet och att det finns en rättslig grund som stödjer detta.

En väl underhållen registerförteckning resulterar i en god överblick över vilka personuppgifter som behandlas och om tillräckliga skyddsåtgärder vidtagits när mer integritetskänsliga uppgifter behandlas. Det underlättar även hanteringen då en registrerad gör en begäran enligt dataskyddsförordningens artiklar 15-22 om att exempelvis få tillgång till vilka personuppgifter som behandlas avseende denne.

I enlighet med dataskyddsförordningen ska registerförteckningen innefatta, förutom namn och kontaktuppgifter för den personuppgiftsansvarige samt DSO, även:

- Ändamål med behandlingen
- Beskrivning av kategorier av registrerade
- Beskrivning av kategorier av personuppgifter
- Kategorier av mottagare av personuppgifterna

- Beskrivningar av eventuella överföringar till tredjeland samt vidtagna skyddsåtgärder
- Tidsfrister för radering av personuppgifter om det är möjligt
- Beskrivning av tekniska och organisatoriska åtgärder där det är möjligt

Registerförteckningen ska hållas aktuell genom att den uppdateras när behandlingar tillkommer eller om det sker förändringar i arbetssätt som gör att uppgifterna i förteckningen inte längre är giltiga.

Syftet med denna del av granskningen har varit att se hur väl förvaltningens registerförteckning uppfyller kraven enligt dataskyddsförordningen. Vidare har syftet varit att granska nuvarande arbetsmetod för att hålla den aktuell.

3.1.3 Resultat

DSO kontrollerar hur många behandlingar som registrerats

I förvaltningens registerförteckning finns efter årets revidering 329 behandlingar registrerade. Det är marginellt färre än föregående år vilket anses som en rimlig förändring i samband med en revidering.

DSO kontrollerar om nödvändiga uppdateringar gjorts

Under våren initierade DSO en revidering av registerförteckningen som slutfördes under sommaren.

Avdelningarnas dataskyddshandläggare har ansvarat för att för sin avdelning kontrollera riktigheten och vid behov uppdatera uppgifterna. Där de saknat sakkunskap har de tagit stöd av kollegor i verksamheten med rätt kompetens.

Vid granskning har DSO uppmärksammat dataskyddshandläggarna på uppgifter där instruktionerna tolkats felaktigt och behövt justeras:

- Beskrivning av kategorier av personuppgifter:

Med *kategorier av personuppgifter* avses exempelvis *namn, kontaktuppgifter* eller *personnummer.* Vissa har dock tolkat kategorier som graden av känslighet och uppgett *harmlösa* eller *känsliga.*

Felaktigheterna har till största del justerats.

- Kategorier av mottagare av personuppgifterna

Syftet med denna information är att uppge vilka som mottar informationen som exempelvis en specifik myndighet eller mottagargrupp som *anhörig* eller *klient*. Rubriken har dock i vissa fall tolkats som att det endast efterfrågas om mottagaren finns *internt* eller *externt.* Detta har till största del justerats men det finns fortsatt behandlingar som behöver justeras avseende detta.

Övriga behov av justeringar som upptäckts i samband med DSO:s granskning av registerförteckning och som kvarstår att hanteras presenteras nedan.

DSO bedömer hur fullständig registerförteckningen är

Granskningen har gjorts utifrån de uppgifter som Dataskyddsförordningen beskriver att registerförteckningen ska innehålla. Förbättringsområden har identifierats i de flesta fall men i varierande omfattning och allvarlighetsgrad:

- Ändamål med behandlingen

När ändamålet för behandlingen beskrivs ska det gå att förstå det avgränsade, berättigade syftet med den specifika behandlingen av personuppgifter.

Ett flertal behandlingar har ett alltför brett och vagt formulerat ändamål vilket skapar en risk för att personuppgifter behandlas felaktigt.

- Beskrivning av kategorier av registrerade

I kolumnen för kategorier av registrerade ges exempel på vad en kategori kan vara. Exemplen är inte heltäckande vilket resulterat i att olika begrepp använts för samma sak vilket skapar otydlighet.

En behandling kan även innehålla flera olika kategorier av registrerade som exempelvis både klienter och anhöriga och det bedöms osäkert om informationen med kategorier av registrerade är komplett.

- Beskrivningar av eventuella överföringar till tredjeland samt vidtagna skyddsåtgärder

I behandlingsregistret har det för samtliga behandlingar fyllts i att det inte sker några tredjelandsöverföringar.

För att säkerställa att detta stämmer krävs dock en omfattande inventering av befintliga system, vilka leverantörer som fungerar som personuppgiftsbiträden, om aktuellt PUB-avtal finns upprättat med uppgifter på underbiträden och till vilka länder personuppgifterna då överförs.

- Tidsfrister för radering av personuppgifter om det är möjligt

För vissa behandlingar har det under kolumnen *Vidtagna skyddsåtgärder* uppgivits gallringsregler men informationen saknas för de flesta behandlingar.

Det behöver göras en koppling mellan registerförteckningens behandlingar och förvaltningens övergripande hanteringsanvisningar där gallringsregler framgår samt en komplettering där verksamheterna behöver ansvara för att personuppgifterna raderas.

- Beskrivning av tekniska och organisatoriska åtgärder där det är möjligt

Informationen om genomförda informationsklassningar av system är endast uppdaterad avseende om protokoll har genomförts och är därmed bristfällig. Detta beskrivs vidare under avsnitt 3.3.

- Övrig information i registerförteckningen

Rättslig grund för behandling

Det är att rekommendera att för varje behandling även uppge vilken rättslig grund utifrån dataskyddsförordningens definitioner som stödjer rätten att behandla personuppgifter. Det skapar förutsättningar för verksamheterna att göra genomtänka överväganden inför behandling av personuppgifter.

I förvaltningens registerförteckning finns rättslig grund uppgiven för samtliga behandlingar. I ett flertal behandlingar har fler än en rättslig grund uppgivits vilket kan tyda på en osäkerhet av vad den egentliga rättsliga grunden är.

DSO bedömer om verksamheten har lämpliga rutiner för registerföring

Förvaltningens registerförteckning består av ett exceldokument med en flik för förvaltningsövergripande behandlingar och en flik för varje avdelnings behandlingar. Behandlingarna är sorterade utifrån vilka processer och delprocesser de utförs inom. Processtrukturen

utgår från *Stadsdelsförvaltningarnas hanteringsanvisningar för informationshantering och arkiv*.

Grundstrukturen i registerförteckningen bedöms fungera väl. Uppdelningen per avdelning skapar en tydlig avgränsning för varje dataskyddshandläggares ansvarsområde. Det bedöms vara rimligt årligen göra en granskning av att alla uppgifter är korrekta.

Excel kan upplevas som ett trubbigt format för ett så stort material och det finns förbättringsområden för att förtydliga vilka uppgifter som efterfrågas i registret. Parallellt med att mallen förtydligas bör alternativ utforskas som gör det mer användarvänligt att både revidera och granska materialet.

3.1.4 DSO anger hur allvarliga bristerna är på en skala

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
x	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
	Inga brister av nämnvärd betydelse identifierade

3.1.5 DSO ger råd och rekommendationer till PUA

Utifrån ovanstående resultat rekommenderar DSO att beslut fattas om följande aktiviteter för 2025:

- Kompetenshöjande insatser för medarbetare så de förstår de olika beståndsdelarna och hur en korrekt registerförteckning bidrar till en säker hantering av de registrerades personuppgifter
- Revidering av mallen utifrån de förbättringsområden som identifierats ovan
- Utforska möjligheten till ett verktyg för att föra registerförteckning i som är användarvänligt både för den som ska underhålla förteckningen och den som ska granska. I första hand bör verktyg som används inom Stockholms stad utvärderas som tilläggsmodul i Stratsys eller VisAlfa

- Inkludera hänvisning till gallringsregler i hanteringsanvisning samt vilka andra gallringsrutiner som gäller där hanteringsanvisningarna inte gäller

3.2 Styrdokument

3.2.1 Sammanfattning

Fråga/kontroll	Svar
Finns lämplig styrande dokumentation på plats?	Delvis
Håller innehållet i de existerande dokumenten lämplig kvalitet?	Till största del
Är dokumenten pedagogiska och ger de ett tillräckligt stöd?	Till största del
Är dokumenten uppdaterade?	Delvis
Finns ägare till dokumenten utpekade, så att uppdateringar kan bli gjorda vid behov?	Ja

3.2.2 Syfte

Förvaltningen ska bedriva ett systematiskt dataskyddsarbete genom att ha ett arbetssätt som uppfyller *dataskydd som standard*. Det förutsätter uppdaterade och tydliga styrdokument som omfattar ett systematiskt dataskyddsarbete och tydliggör ansvarsfördelning för olika roller i verksamheten.

I granskningen har förekomsten av styrande dokumentation och kvaliteten av dess utformning och innehåll bedömts.

3.2.3 Resultat

Finns lämplig styrande dokumentation på plats?

DSO bedömer att följande styrande dokument behöver finnas på förvaltningen för att ett systematiskt dataskyddsarbete ska kunna bedrivas:

- **Lokal anvisning för arbete med informationssäkerhet och dataskydd**
- **Registerförteckning över behandling av personuppgifter**
- Rutin för revidering av registerförteckning
- **Rutin för anmälan av personuppgiftsincidenter**

- **Sammanställning och uppföljning av anmälda personuppgiftsincidenter**
- **Rutin för att tillgodose de registrerades rättigheter**
- Årshjul för DSO:s arbete

De som är markerade med fet stil finns framtagna, övriga saknas.

DSO bedömer om innehållet i existerande dokument håller lämplig kvalitet

Lokal anvisning för arbete med informationssäkerhet och dataskydd:

Förvaltningens lokala anvisning är framtaget med utgångspunkt från Stockholms stads tillämpningsanvisningar för arbete med informationssäkerhet och fastställdes i april 2024.

Anvisningen är i behov av revidering då delar inte är överensstämmande med hur arbetssätt implementerats under året. Den hänvisar även till arbetssätt och roller i enlighet med förvaltningsmodellen pm3 som ännu inte implementerats inom förvaltningen.

En översyn behöver även göras av om uppdateringar är nödvändiga till följd av att Stockholms stads tillämpningsanvisningar reviderats i november 2024.

Registerförteckning över behandling av personuppgifter:

DSO:s rekommendationer avseende kvalitetsförbättringar av förvaltningens registerförteckning framgår under avsnitt 3.1.

Rutin för revidering av registerförteckning:

En skriftlig rutin för årliga revideringar av registerförteckningen skulle tydliggöra arbetsgång och ansvarsfördelningar.

Rutin för anmälan av personuppgiftsincidenter:

Rutinen har reviderats under året och följer bestämmelserna enligt dataskyddsförordningen.

Sammanställning och uppföljning av anmälda personuppgiftsincidenter:

Dokumentet följer kraven i enlighet med dataskyddsförordningen men bör revideras för att tydligare följa processen för

incidenthantering samt underlätta uppföljning av inkomna incidenter.

Rutinen bör även kompletteras med en skriftlig processbeskrivning för att förtydliga arbetsgång och ansvarsfördelning mellan olika roller i hanteringen.

Rutin för att tillgodose de registrerades rättigheter:

Rutinen behöver kompletteras för att omfatta alla rättigheter i enlighet med dataskyddsförordningens artiklar 15-22 och förtydliga vilka ställningstaganden vi som myndighet behöver göra när en begäran inkommer från en registrerad. Den behöver även utvecklas för att säkerställa att den information som lämnas ut är komplett då personuppgiftsbehandling sker inom flera verksamheter inom förvaltningen.

Rutinen bör kompletteras med en skriftlig processbeskrivning för att förtydliga arbetsgång och ansvarsfördelning mellan olika roller i hanteringen.

Årshjul för DSO:s arbete:

För att uppnå ett systematiskt dataskyddsarbete behöver DSO upprätta ett årshjul med inplanerade aktiviteter för verksamhetsåret. Aktiviteterna ska bestå av kontroller som bör ske årligen som exempelvis att granska att rutiner och processer fortfarande är giltiga och att granska registerförteckning över behandlade personuppgifter.

Till detta ska aktiviteter läggas in som grundar sig på identifierade risker och som personuppgiftsansvarig fattat beslut om ska prioriteras i arbetet med dataskydd under det aktuella året.

3.2.4 DSO anger hur allvarliga bristerna är på en skala

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
X	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
	Inga brister av nämnvärd betydelse identifierade

3.2.5 DSO ger råd och rekommendationer till PUA

Utifrån ovanstående resultat rekommenderar DSO att beslut fattas om följande aktiviteter för 2025:

- Revidering av rutiner i enlighet med ovan
- Kommunicering och implementering av de reviderade rutinerna med stöd av dataskyddshandläggarna
- Upprättande av årshjul för DSO:s arbete enligt beskrivning ovan.

3.3 Tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar

3.3.1 Sammanfattning

Fråga/kontroll	Svar
Hur många av personuppgiftsbehandlingarna som finns i verksamheten har informationsklassats?	116
Är klassade personuppgiftsbehandlingar aktuella?	Ja

3.3.2 Syfte

Stockholm stads riktlinjer för informationssäkerhet föreskriver att alla informationstillgångar inom förvaltningen ska informationsklassas med stöd av SKR:s verktyg KLASSA.

Om stegen enligt verktyget följs, och rätt kompetenser deltar under klassningsarbetet, skapas förutsättningar för att identifiera åtgärder för att skydda informationstillgångarna och utse ansvariga för att genomföra åtgärderna. Lämpliga tekniska och organisatoriska åtgärder kan då antas ha vidtagits.

Syftet med denna granskning har varit att undersöka hur många av förvaltningens behandlingar av personuppgifter som är informationsklassade samt hur arbetet med informationsklassningar är strukturerat.

3.3.3 Resultat

Som underlag för detta resultat har endast inkluderats informationsklassningar som genomförts efter att Norra innerstadens stadsdelsförvaltning bildades.

Som *genomfört* har räknats de informationsklassningar där protokoll finns, det vill säga det första steget av fyra i informationsklassningen.

Av de 329 behandlingar av personuppgifter som finns upptagna i registerförteckningen är det 116 som är informationsklassade. Den stora andelen klassade behandlingar beror på att system som

omfattar en stor mängd behandlingar har klassats under föregående år som eDok, Agresso och ILS.

Inom förvaltningen är det informationssäkerhetssamordnaren som själv, eller gemensamt med berörd dataskyddshandläggare, har bestämt prioritetsordning för system som ska informationsklassas. Informationssäkerhetssamordnare alternativt informationssäkerhetshandläggare har varit klassningsledare för de system som används inom flera av förvaltningens avdelningar. Där användarna begränsats inom en avdelning har det i första hand varit dataskyddshandläggare som lett klassningen. Den som är klassningsledare har bjudit in berörda avdelningars dataskyddshandläggare. Dataskyddshandläggare har ansvarat för att bjuda in personer med verksamhetskunskap och erfarenhet av det berörda systemet. Övriga deltagare på informationsklassningarna har varit representanter från IT-enheten samt DSO.

Vid granskning av den sammanställning som finns av genomförda informationsklassningar framgår att det behövs en tydligare struktur där det framgår vilka steg enligt KLASSA som genomförts samt kommentar om vad som är nästa steg i processen. Det behövs även en tydligare information om vad som ligger till grund för prioriteringar av klassningar och till vilken del det tagits hänsyn till vilken typ och mängd personuppgifter som behandlas.

3.3.4 DSO anger hur allvarliga bristerna är på en skala

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
X	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
	Inga brister av nämnvärd betydelse identifierade

3.3.5 DSO ger råd och rekommendationer till PUA

Utifrån ovanstående resultat rekommenderar DSO att beslut fattas om följande aktiviteter för 2025:

- Skapa en tydligare och mer överblickbar uppföljning av informationsklassningar där det framgår:

    - Datum för senaste informationsklassning
    - Vilket/-a steg som genomförts samt nästa steg i processen
    - Prioriteringsnivåer och kriterier som nivåerna baseras på
- Prioritet av informationsklassningar utifrån konsekvenser för de registrerade

3.4 Konsekvensbedömningar

3.4.1 Sammanfattning

Fråga/kontroll	Svar
Har man identifierat alla behandlingar som det borde göras konsekvensbedömningar av?	Nej
Har alla potentiella högriskbehandlingar konsekvensbedömts?	Nej
Är de genomförda bedömningarna aktuella?	Nej

3.4.2 Syfte

Konsekvensbedömningar ska alltid genomföras inför att beslut fattas om behandling av särskilt riskfyllda behandlingar av personuppgifter för att skydda enskildas rättigheter och friheter. Integritetsskyddsmyndigheten (IMY) beskriver när en konsekvensbedömning ska eller bör göras.

En konsekvensbedömning är en process som innehåller:

- En systematisk beskrivning av en tänkt personuppgiftsbehandling
- En bedömning av om behandlingen är nödvändig och proportionell
- En riskanalys med utgångspunkt i fysiska personer rättigheter och friheter
- Planering av vilka åtgärder som ska vidtas för att eliminera eller mildra riskerna
- Beslut om att påbörja en behandling utifrån de nya/givna förutsättningarna och eventuellt inhämta förhandssamråd från IMY
- Kontinuerlig översyn

Vid tveksamheter är det att rekommendera att genomföra en konsekvensbedömning för att fatta välgrundade beslut inför behandling av personuppgifter.

I denna granskning har syftet varit att undersöka i vilken grad konsekvensbedömningar har genomförts och hur arbetet med konsekvensbedömningar struktureras.

3.4.3 Resultat

Har man identifierat alla behandlingar som det borde göras konsekvensbedömningar av?

Det saknas information om vilka system som det borde göras konsekvensbedömningar av i sammanställningen över planerade och genomförda informationsklassningar.

Har konsekvensbedömning gjorts för alla potentiella högriskbehandlingar av personuppgifter?

Inga konsekvensbedömningar har genomförts under året inom förvaltningen.

Är de genomförda konsekvensbedömningarna aktuella?

Se svar ovan.

3.4.4 DSO anger hur allvarliga bristerna är på en skala

X	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
	Inga brister av nämnvärd betydelse identifierade

3.4.5 DSO ger råd och rekommendationer till PUA

Utifrån ovanstående resultat rekommenderar DSO att beslut fattas om följande aktiviteter för 2025:

- Prioritera informationsklassningar utifrån konsekvenser för de registrerade
- Prioritera att genomföra konsekvensbedömningar för behandlingar som är särskilt skyddsvärda

3.5 Individens rättigheter

3.5.1 Sammanfattning

Fråga/kontroll	Svar
Hur många begäran (om registerutdrag, begränsning, radering etc.) har inkommit från registrerade personer?	3
Hur många av dessa begäran har hanterats av verksamheten inom 30 dagar?	3

3.5.2 Syfte

De registrerade har i enlighet med dataskyddsförordningen rättigheter att få insyn i vilka personuppgifter som behandlas och önska att verksamheten vidtar vissa åtgärder. I vår myndighetsutövning är det vissa av dessa rättigheter som inte kan tillgodoses som exempelvis rätten att få uppgifter raderade. Vi är dock skyldiga att besvara förfrågningar som inkommer och detta ska i regel ske inom 30 dagar.

Att tillgodose de registrerades rättigheter är centralt för arbetet med dataskydd och är den viktigaste principen att följa för att undvika sanktionsavgifter. Det är därför viktigt att det finns ett välfungerande arbetssätt för att tillgodose de registrerades rättigheter.

Syftet med denna granskning har varit att undersöka hur många begäran enligt artikel 15-22 som inkommit samt om de hanterats inom tidsfristen på 30 dagar.

3.5.3 Resultat

Har verksamheten förutsättningar att hantera registrerades rättigheter inom föreskriven tidsfrist?

Verksamheterna har förutsättningar att hantera de registrerades rättigheter inom tidsfristen utifrån det låga antalet förfrågningar.

En process behöver dock formuleras som tydliggör arbetsgång och ansvarsfördelning mellan olika roller för att säkerställa att tidsfristen hålls även om antalet förfrågningar skulle öka. Vidare behöver process och rutin säkerställa att alla personuppgiftsbehandlingar identifieras även när den registrerade är aktuell inom olika avdelningar på förvaltningen.

Se även resultat under avsnitt 3.2 avseende behov av justeringar av rutin vid begäran från registrerad.

3.5.4 DSO anger hur allvarliga bristerna är på en skala

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
X	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
	Inga brister av nämnvärd betydelse identifierade

3.5.5 DSO ger råd och rekommendationer till PUA

Utifrån resultat ovan rekommenderar DSO att beslut fattas om följande aktiviteter under 2025:

- Formulera process samt utveckla rutin för att hantera begäran från den registrerade i enlighet med artikel 15-22 i dataskyddsförordningen

3.6 Personuppgiftsincidenter

3.6.1 Sammanfattning

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	Främst av den som gör sig skyldig till incidenten.
Hur många personuppgiftsincidenter har dokumenterats?	24
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	Rapporterade till IMY: 8 Berörda informerade: 11
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	6

3.6.2 Syfte

Som myndighet behöver vi följa dataskyddsförordningens bestämmelser avseende behandling av personuppgifter. Som personuppgift avses uppgifter som direkt eller indirekt kan identifiera en person. Det kan exempelvis vara namn, personnummer eller adress men även bilder och ljudinspelningar. Inom förvaltningen behandlar vi ofta känsliga personuppgifter som exempelvis uppgifter om personers fysiska eller psykiska hälsa men även andra integritetskänsliga personuppgifter som exempelvis information om personen dömts för brott.

De individer vars personuppgifter vi behandlar kallas för *de registrerade*. På förvaltningen är detta exempelvis klienter, brukare, medarbetare, anhöriga och medborgare. De registrerade består ofta av sårbara grupper som barn och vuxna med olika stödbehov. Med behandling avses olika sorters hantering av personuppgifter som exempelvis insamling, registrering och gallring.

När obehöriga får tillgång till personuppgifter som vi ansvarar för, avsiktligt eller oavsiktligt, eller då vi inte kan få tillgång till personuppgifter med anledning av exempelvis ett tekniskt fel ska detta betraktas som en personuppgiftsincident som ska anmälas i incidenthanteringsverktyget IA samt utredas.

Process och ansvarsfördelning vid förekomst av en personuppgiftsincident beskrivs i den lokala rutinen *Anmälan av personuppgiftsincident – förvaltningsövergripande rutin.*

Anmälan ska göras skyndsamt och om det inte går att utesluta att incidenten kan leda till risk för den registrerades fri- och rättigheter ska incidenten även anmälas till tillsynsmyndigheten IMY inom 72 timmar från upptäckt. I dessa fall ska även ett övervägande göras om den eller de berörda personerna ska informeras om det inträffade.

DSO har som uppgift att stötta verksamheterna i hur de ska tolka bestämmelserna i dataskyddsförordningen men det är verksamheterna som fattar det slutgiltiga beslutet om anmälan till IMY görs.

3.6.3 Resultat

Hur väl förmår verksamheten att rapportera personuppgiftsincidenter i tid till Integritetsskyddsmyndigheten?

Av totalt 24 anmälda incidenter har elva bedömts så allvarliga att de även rapporterats till IMY. Åtta av dessa har även rapporterats till de berörda vilket bedöms rimligt.

Verksamheterna har anmält de flesta personuppgiftsincidenter i tid till Integritetsmyndigheten. I de fall det dröjt har det funnits en osäkerhet i hanteringen av incidenten och anmälan till IMY.

För de flesta incidenter som skett har den mänskliga faktorn uppgetts som skäl och förebyggande orsaker för att undvika att de inträffar igen blir därigenom något vaga.

Med tanke på antalet behandlingar är det väldigt få incidenter som rapporteras in vilket kan antas bero på okunskap om både vad som utgör en incident och när den bör anmälas. Ett mer strukturerat sätt att upptäcka incidenter bedöms även kunna öka antalet anmälda incidenter och därmed ett större material att analysera för att kunna förebygga att de inträffar.

3.6.4 DSO anger hur allvarliga bristerna är på en skala

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
X	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
	Inga brister av nämnvärd betydelse identifierade

3.6.5 DSO ger råd och rekommendationer till PUA

Utifrån ovanstående resultat rekommenderar DSO följande aktiviteter för 2025:

- Öka kunskaperna om vad som utgör personuppgiftsincidenter för att fler incidenter ska anmälas genom att:
    - Förtydliga chefsansvaret att följa upp vilka medarbetare som inte genomfört de obligatoriska e-utbildningarna i informationssäkerhet och dataskydd
    - Inför Informationssäkerhet och dataskydd som obligatoriskt tema i årshjulet för APT
- Öka det aktiva upptäckandet av incidenter genom att implementera en övergripande incidentprocess som inkluderar alla typer av incidenter som även kan resultera i en personuppgiftsincident

4 Genomförda granskningar under året

4.1 Sammanfattning

Genomförda granskning:

- *Organisation för informationssäkerhet och dataskydd*

4.2 Syfte

Förutom ovanstående obligatoriska rapporteringsområden kan DSO genomföra ytterligare granskningar av områden som visar verksamhetens efterlevnad av dataskyddsförordningen.

4.3 Genomförda granskningar och deras resultat

Granskning – Organisation för informationssäkerhet och dataskydd

Under hösten 2023 fattades beslut om att en prioriterad åtgärd för att åstadkomma ett strukturerat dataskyddsarbete var att tillsätta en organisation för arbete med informationssäkerhet och dataskydd.

Denna granskning syftar till att undersöka hur organisationen för informationssäkerhet och dataskydd har realiserats och hur väl den fungerar utifrån sitt syfte.

Under våren 2024 bildades ett dataskyddsnätverk som samordnas av förvaltningens ISAM och DSO. Varje avdelningschef har utsett en dataskyddshandläggare som fungerar som avdelningens representant i nätverket med syftet att fungera som ett stöd för chefer och medarbetare avseende dataskyddsfrågor och som en länk mellan nätverket och verksamheterna. Under sommaren rekryterades en informationssäkerhetshandläggare i syfte att stötta i arbetet med informationssäkerhet och dataskydd med fokus på informationsklassningar.

Under hösten kompletterades nätverket med representanter från IT-enheten då detta upplevdes som viktigt i det övergripande informationssäkerhetsarbetet. Äldreomsorgen har sedan hösten saknat dataskyddshandläggare.

Dataskyddsnätverket har haft sju möten under året där fokus har varit på kompetenshöjande insatser, stöd för

dataskyddshandläggarnas revidering av registerförteckning över behandlade personuppgifter och övriga aktuella frågor och aktiviteter inom informationssäkerhet och dataskydd.

Dataskyddhandläggarna har bjudits in till informationsklassningar av system som berör deras avdelning. De har i sin tur ansvarat för att bjuda in rätt kompetenser från verksamheterna för att kunna kvalitetssäkra resultatet av klassningarna utifrån ett verksamhetsperspektiv. Dataskyddshandläggaren inom äldreomsorgen har lett informationsklassningar för system som endast omfattar deras avdelning fram till att hen behövde avsäga sig uppdraget.

Organisationen för dataskydd har fungerat väl utifrån sitt syfte. Nätverksmötena kan förbättras genom en tydligare planering av innehållet för året och med fler kompetenshöjande inslag. En ersättare för tidigare dataskyddshandläggare för äldreomsorgen behöver utses.

Det skulle bidra till ett förbättrat systematiskt dataskyddsarbete med större helhetssyn om nätverket utökades med representanter från inköp och upphandling samt registratur och arkiv.

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
X	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
	Inga brister av nämnvärd betydelse identifierade

4.4 DSO ger råd och rekommendationer till PUA

Utifrån ovanstående resultat rekommenderar DSO att beslut fattas om följande aktiviteter för 2025:

- Utse en ny dataskyddshandläggare för äldreomsorgen
- Utse en representant från inköp och upphandling samt arkiv/registratur som ska ingå i dataskyddsnätverket

5 Risker inom dataskydd

5.1 Sammanfattning

Relevanta risker inom verksamheten:

- *Bristfälliga informationsklassningar*
- *Bristfälliga konsekvensbedömningar*
- *Bristande rutin och process för att tillgodogöra de registrerades rättigheter*

5.2 Syfte

Detta avsnitt lyfter fram de främsta risker för verksamheten inom dataskydd som identifierats i granskningarna i denna rapport. Inga ytterligare riskområden har identifierats.

För fördjupande information om riskerna, se för dessa separata avsnitt ovan.

5.3 Resultatet av riskkartläggningen

Risk 1 – Bristfälliga informationsklassningar

Sedan föregående årsrapport har antalet genomförda informationsklassningar ökat från två till 25 vilket är en markant ökning.

Utifrån ett dataskyddsperspektiv är det dock inte tydligt hur väl prioritering i planeringen av informationsklassningar görs utifrån konsekvenser för de registrerade vilket kan innebära att förvaltningen har bristfälliga tekniska och organisatoriska åtgärder.

Vidare är sammanställning av påbörjade och genomförda informationsklassningar otydliga genom att det är svårt att tyda vad som är genomfört och vad som är nästa steg i processen.

Ovanstående resultat bedöms kunna innebära en stor risk för de registrerade och därmed ge konsekvenser även för verksamheten vid en eventuell tillsyn.

X	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
	Inga brister av nämnvärd betydelse identifierade

Risk 2 – Bristfälliga konsekvensbedömningar

Konsekvensbedömningar ska alltid genomföras inför att beslut fattas om behandling av särskilt riskfyllda behandlingar av personuppgifter för att skydda enskildas rättigheter och friheter. IMY beskriver för vilka kriterier det alltid ska genomföras konsekvensbedömningar. Vid tveksamheter är det dock alltid att rekommendera att genomföra en konsekvensbedömning för att fatta välgrundade beslut inför behandling av personuppgifter.

Inga konsekvensbedömningar har genomförts under året inom förvaltningen. Det har inte heller skett någon översyn av för vilka behandlingar som det behöver göras en konsekvensbedömning.

X	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
	Inga brister av nämnvärd betydelse identifierade

Risk 3 – Bristande rutin och process för att tillgodogöra de registrerades rättigheter

Artikel 15-22 i dataskyddsförordningen beskriver de registrerades rättigheter kopplade till de personuppgifter avseende dem som behandlas. Det är centralt i dataskyddsarbetet att ha ett fungerande

arbetssätt för att tillgodose dessa rättigheter och kunna säkerställa att den information som delges är korrekt och komplett.

Förvaltningen har under året endast fått tre förfrågningar kopplade till de registrerades rättigheter. Dessa bedöms ha hanterats korrekt och inom den tidsfrist som IMY beslutat om.

Den rutin och process som finns framtagen bedöms vara bristfällig då den inte inkluderar samtliga rättigheter enligt ovanstående artiklar. Det saknas också en tydlig process med olika rollers ansvar vilket skapar en risk för att samtliga personuppgifter som behandlas inte inhämtas för vidare information till den registrerade.

5.4 DSO ger råd och rekommendationer till PUA

Utifrån ovanstående resultat rekommenderar DSO att beslut fattas om följande aktiviteter för 2025:

- Justera underlag för översyn av informationsklassningar så det tydliggörs vad som är genomfört och vad som är nästa steg
- Prioritera informationsklassningarna utifrån konsekvenser för de som omfattas av behandling av personuppgifter
- Genomför en inventering av behandlade personuppgifter där en konsekvensbedömning ska göras och inkludera detta i prioritering av informationsklassningar
- Revidera rutin för att tillgodose de registrerades rättigheter och komplettera process med tydlig ansvarsfördelning mellan olika roller i processen

6 Planerade granskningar under det nya verksamhetsåret

6.1 Sammanfattning

- *PUB-avtal granskas i samband med informationsklassningar*
- *Konsekvensbedömningsprocess granskas*
- *Granskning av rutin och process för att tillgodose de registrerades rättigheter*

6.2 Syfte

Utifrån ovanstående resultat har tre områden för granskning valts ut för 2025. Områdena har valts utifrån allvarlighetsgrad och påverkan på de registrerade.

6.3 Planerade granskningar

Granskning 1 – PUB-avtal

De registrerade ska säkerställas en hög nivå av säkerhet kring hur deras personuppgifter behandlas oavsett om det sker inom förvaltningen eller av avtalad leverantör eller dennes underleverantör. För att kunna uppnå detta behöver PUB-avtal finnas för varje behandling som sker hos leverantör. PUB-avtalet beskriver ställda krav avseende behandling av personuppgifter samt ansvar när incidenter inträffar och regler för radering av personuppgifter.

Det saknas i dagsläget en tydlig överblick av i vilken grad det finns PUB-avtal och om uppgifterna avseende eventuella underleverantörer fortsatt är aktuell vilket är av stor vikt för att säkerställa att inga tredjelandsöverföringar sker.

Under 2025 kommer därför granskning av PUB-avtal ske genom att:

- Inventera behov och förekomst i påbörjade informationsklassningar
- Vid förekomst granska innehåll och vid otydligheter kontakta leverantör
- Vid varje ny informationsklassning som görs säkerställa att PUB-avtal upprättas där det uppstår ett personuppgiftsbiträdesförhållande

Granskning 2 - Konskevensbedömningsprocess

Konsekvensbedömningar ska alltid genomföras inför att beslut fattas om behandling av särskilt riskfyllda behandlingar av personuppgifter för att skydda enskildas rättigheter och friheter. Under 2024 har inga konsekvensbedömningar genomförts.

Under 2025 kommer därför granskning av konsekvensbedömningsprocessen ske genom att:

- Inventera behov av konsekvensbedömningar i påbörjade och genomförda informationsklassningar
- Påtala behovet av konsekvensbedömningar i kommande informationsklassningar

Granskning 3 – Granskning av process och rutin för att tillgodose de registrerades rättigheter

Artikel 15-22 i dataskyddsförordningen beskriver de registrerades rättigheter kopplade till de personuppgifter avseende dem som behandlas. Det är centralt i dataskyddsarbetet att ha ett fungerande arbetssätt för att tillgodose dessa rättigheter och kunna säkerställa att den information som delges är korrekt och komplett.

Den rutin och process som är framtagen är bristfällig och det finns en risk för att förvaltningen inte uppfyller kraven och lämnar inkomplett information.

Under 2025 kommer därför granskning ske av att:

- Rutin och process uppfyller dataskyddsförordningens krav
- Process tydligt beskriver olika rollers ansvar
- Rutin och process är implementerad genom dataskyddsnätverkets medlemmar