Stockholms stad

Bilaga 7
Dnr KS 2023/1238

Dataskyddsombudets GDPR årsrapport 2023

Kommunstyrelsen

GDPR årsrapport
December 2023

Dnr: KS 2023/1238
Datum: 2023-12-22
Kontaktperson: Kommunstyrelsens dataskyddsombud

1 Bakgrund

Dataskyddsombudet, DSO, lämnar härmed årsrapport för 2023.
I år har Europeiska dataskyddstyrelsen initierat en samordnad åtgärd för att undersöka dataskyddsombudens roll och ställning, vilket medfört att vår svenska tillsynsmyndighet har en pågående tillsyn i offentlig och privat sektor av dataskyddsombudets lagstadgade roll. I tillsynen ingår tillsyn om dataskyddsombudet har tilldelats resurser, förmåga att utföra sin roll och om dataskydds-ombudet har den oberoende ställning som lagen kräver och om denne ges insyn för att utföra sina lagstadgade uppgifter. I och med pågående tillsyn blir detta ett av fokusområdena för årets rapport.

Ett annat fokusområde för rapporten är att kommunstyrelsen, genom stadsledningskontoret, SLK, bör fortsatt prioritera att implementera ett ändamålsenligt och systematiskt integritetsskydd, som följer gällande lagkrav när kommunstyrelsen i sin ledning och samordning av den kommunala förvaltningen fattar beslut och utför uppgifter som påverkar och innebär behandling av personuppgifter inom staden. Det ändamålsenliga och systematiska integritets-skyddet ska införlivas i kommunstyrelsens strategi och följa de lagstadgade ansvarsrollerna personuppgiftsansvarig och personuppgiftsbiträde.

I år har även Europeiska dataskyddsstyrelsen publicerat att en samordnad en insats 2024 för samtliga europeiska dataskydds-myndigheter gällande individens, den registrerades, rätt till tillgång, vilket även det blir ett fokusområde i årets rapport.

I tidigare årsrapporter har bakgrund och gällande dataskydds-lagstiftning, inklusive dataskyddsförordningen[1], och dess syfte att värna individens integritet beskrivits. Detta kommer således inte att beskrivas i samma omfattning i årets rapport. I denna del hänvisas till GDPR årsrapport 2022 för kommunstyrelsen, diarienummer KS 2022/1278. I årets årsrapport, kommer även åtgärder rekommenderas utifrån risk- och granskningsperspektivet som kan fungera väl att omsätta till avdelningsspecifika aktiviteter för verksamhetsplan (VP-aktiviteter) att hantera befintliga integritetsrisker. Att hantera integritetsfrågor och risker är idag väsentligt för att värna stockholmares och anställdas integritet.

[1] EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning)

Innehåll

1 Bakgrund ... 3
2 Sammanfattning ... 5
3 Dataskyddsombudets roll och ställning ... 6
3.2 Samordnad åtgärd avseende dataskyddsombudsrollen ... 7
3.3 Dataskyddsombudets rekommendationer ... 8
4 Ett ändamålsenligt och systematiskt integritetsskydd ... 8
4.1 Integritetsskyddsanalys och dess processer ... 9
4.2 Individens, den registrerades, rättigheter ... 13
4.3 Dataskyddsombudets rekommendationer ... 15
4.4 Register för behandling, s.k. registerförteckning ... 16
4.5 Dataskyddsombudets rekommendationer ... 17
4.6 Styrning och styrdokument avseende dataskydd ... 18
4.7 Dataskyddsombudets rekommendationer ... 19
4.8 Informationssäkerhet och dataskydd bör vara integrerade ... 20
4.9 Dataskyddsombudets rekommendationer ... 23
4.10 Konsekvensbedömning avseende dataskydd ... 24
4.11 Dataskyddsombudets rekommendationer ... 25
4.12 Hantering av personuppgiftsincidenter ... 26
4.13 Dataskyddsombudets rekommendationer ... 28
4.14 Tredjelandsöverföring ... 29
4.15 Dataskyddsombudets årshjul ... 30
4.16 Dataskyddsorganisationens årshjul ... 31
5 Risk och dataskydd ... 32
5.1 Dataskyddsombudets rekommendation ... 32
6 Genomförda granskningar ... 33
7 Övrigt att rapportera ... 34
7.1 Analys av dataskyddsombudens årsrapporter ... 34

2 Sammanfattning

Att värna individs, stockholmarens, kommunmedlemmens, och anställds integritet när personuppgifter behandlas är idag en fråga om förtroende och om regelefterlevnad. Regelverket är omfattande och EU-domstolens förtydligar regelverket löpande. Detta driver på komplexiteten och kräver att systematiska integritetsprocesser förfinas eller tas fram, samt att dessa är väl förankrade i verksamhetens kärnverksamhet och redan framtagna processer.

Vid digitalisering, innovation, automatiskt beslutsfattande och användande av AI behöver ledning och verksamhet ha kunskap om hur dataskyddslagstiftningen[2] utvecklas och hur ett ändamålsenligt och systematiskt integritetsskydd bör införlivas i en verksamhet.

Årets GDPR-årsrapport 2023 beskriver därför vad en integritets-skyddsanalys behöver innehålla för att ett ändamålsenligt och systematiskt integritetsskydd ska kunna långsiktigt införlivas.

Rapporten kommer att beröra Europeiska dataskyddsstyrelsens samordnade åtgärder 2023 om dataskyddsombudets roll och ställning. Europeiska dataskyddstyrelsens aviserade samordnade åtgärder för 2024, den registrerades rätt till tillgång till personuppgifterna och tillhörande information, kommer även beröras.

De obligatoriska områdena individens, den registrerades, rättigheter registerförteckning, styrdokument, implementerade tekniska och organisatoriska åtgärder för personuppgiftsbehandling, konsekvens-bedömning avseende dataskydd och hantering av personuppgifts-incidenter kommer att belysas med tillhörande rekommendationer utifrån dataskyddsombudets rådgivning och granskning.

Tredjelandsöverföringsbedömningar utförs fortsatt regelbundet och behöver därför informeras om. Integritetsrisk och hantering av integritetsrisk utifrån individs rättigheter och friheter kommer mot bakgrund av dess legala betydelse åter kort beröras i årets rapport.

Avslutningsvis lyfts att rekommendationen om behov av analys av trender och integritetsrisker utifrån samtliga stadens dataskydds-ombuds årsrapporter kvarstår.

[2] Så hänger lagarna ihop | IMY.

3 Dataskyddsombudets roll och ställning

Dataskyddsombud är en lagstadgad roll. I dataskyddsförordningen regleras hur ett dataskyddsombud utnämns, dess ställning och uppgifter[3].

I tidigare årsrapport har informerats om att enligt dataskydds-förordningen ska utnämnt dataskyddsombud oberoende rapportera direkt till högsta förvaltningsnivå avseende verksamhetens efterlevnad av dataskyddslagstiftningen, d.v.s. kommunstyrelsen. Dataskyddsombudet ska även ge kommunstyrelsen och dess stadsledningskontor regelbundet råd avseende de skyldigheter som lagstiftningen uppställer avseende integritetsskydd.

Kommunstyrelsen ska i sin tur säkerställa att dataskyddsombudet oberoende, på ett korrekt sätt, och i god tid deltar i alla frågor som hanteras på kommunstyrelsens uppdrag som rör skyddet av personuppgifter. Detta inbegriper strategin för skydd av personuppgifter och ansvarstilldelningen. Detta innebär att dataskyddsombudet ska involveras i alla personuppgiftsfrågor där kommunstyrelsens agerar lokalt och stadenövergripande i ansvarsrollerna personuppgiftsansvarig och personuppgiftsbiträde.

Tillsynsmyndigheten beskriver dataskyddsombudets roll på följande vis. Dataskyddsombudets roll är att kontrollera att dataskydds-lagstiftningen följs inom organisationen genom att till ex. utföra kontroller och information- och utbildningsinsatser. Den övergripande och viktigaste uppgiften för dataskyddsombudet är att övervaka att organisationen följer lagstiftningen. Det innebär bl.a. att samla in information om hur organisationen behandlar personuppgifter, kontrollera att organisationen följer bestämmelser och interna styrdokument samt informera och ge råd inom organisationen.

Tillsynsmyndigheten lyfter även att dataskyddsombudet inte är ansvarig för hur en organisation följer lagstiftningen. Det ansvaret ligger alltid på kommunstyrelsen som styr personuppgiftsstrategin och genom att stadsledningskontoret agerar i ansvarsrollerna personuppgiftsansvarig och personuppgiftsbiträde.

[3] Artikel 37-39, skäl 97 och riktlinjer om dataskyddsombud Riktlinjer om dataskyddsombud - Vägledning från 29-gruppen - Datainspektionen (imy.se)

Tillsynsmyndigheten lyfter även särskilt att dataskyddsombudet ska känna till organisationens kärnverksamhet, hur organisationen behandlar personuppgifter samt veta hur organisationens informationsteknik och it-säkerhet fungerar för att ha förmåga att sprida information och en integritetskultur inom organisationen.

Dataskyddsombudet är således en roll som bistår organisationen med information och utbildning för att skapa en integritetskultur som är förenlig med gällande lagstiftning. Dataskyddsombudets granskning bidrar även den som verktyg för att kommunstyrelsen, genom dess stadsledningskontor, kan prioritera och omsätta dataskyddsombudets rekommendationer till faktiska aktiviteter som värnar stockholmarnas och de anställdas mänskliga rättighet till integritet vid personuppgiftsbehandling.

3.2 Samordnad åtgärd avseende dataskyddsombudsrollen

I år inledde Europiska dataskyddstyrelsen en riktad insats för att undersöka om organisationer runt om i EU följer dataskydds-förordningens regelverk om dataskyddsombudets roll och ställning[4].

Tillsynsmyndigheten i Sverige valde att initiera en tillsyn över olika personuppgiftsansvariga inom privat och offentlig sektor, varav en av Stockholms stads nämnder ingår[5]. Tillsynen avser att bedöma om dataskyddsombudet har den roll och ställning samt de resurser som förutsätts enligt dataskyddsförordningen. Frågor som ställts har således grund i dataskyddsombudets utnämning, kvalifikationer, uppgifter, resurser och ställning samt oberoende.

En delrapportering av IMY har skett till Europeiska dataskydds-styrelsen avseende vad tillsynerna hittills visat. Delrapporteringen innehåller information som bl.a. visar att organisationerna till viss del har olika uppfattningar om vad som ska ingå i dataskydds-ombudets uppdrag. IMY lyfter därför att behov av tydligare vägledning finns. Tillsynsmyndigheten lyfter även exempel om dataskyddsombudet innehar flera roller inom organisationen är det viktigt att det inte föreligger en intressekonflikt vid utförande av dataskyddsombudets uppgifter.

[4] Launch of coordinated enforcement on role of data protection officers | European Data Protection Board (europa.eu)
[5] IMY inleder bred granskning av dataskyddsombudens roll och ställning | IMY

Tillsynsmyndigheten har i några få fall gentemot utvalda personuppgiftsansvariga valt att ställt fördjupande frågor, vilket innebär att tillsynen fortfarande pågår per den 22 december 2023.

3.3 Dataskyddsombudets rekommendationer

Med anledning av den vägledning som kommer från tillsyns-myndigheten, i och med en tillsyn, behöver kommunstyrelsen, genom dess stadsledningskontor, se över och säkerställa dataskyddsombudet oberoende ställning, roll, resurser och uppgifter under 2024 i överenstämmelse med vägledningen.

Dataskyddsombudets rekommendationer är följande.

- Att bevaka ovan tillsyn av Integritetskyddsmyndigheten och kommande vägledning från Europeiska dataskydds-styrelsen.
- Att det systematiska integritetsskyddsarbetet säkerställer att dataskyddsombudet får lagstadgad *insyn och oberoende* kan utföra sina uppgifter såsom *rådgivning och granskning*, samt *utbilda* stadsledningskontoret om integritetsskydd i kontakt med bl.a. avdelningsspecifika dataskyddskontakter.
- Att *resurseffektivt systematisera integritetskyddsarbetet* över stadsledningskontoret. I förslagsvis ett årshjul med utnämnda dataskyddskontakter på varje avdelning i samverkan med dataskyddsombudet för att främja dataskyddsombudets oberoende, insyn och för att strukturera upp rådgivningen samt identifierade behov av *utbildnings-insatser*.

4 Ett ändamålsenligt och systematiskt integritetsskydd

Att värna stockholmarens och de anställdas integritet är idag av centralt värde för att följa lag men också för att skapa ett långsiktigt förtroende för den offentliga verksamhetens digitalisering och hantering av individens personuppgifter. Ett faktiskt ändamålsenligt och systematiskt integritetsskydd ska därför ha införlivats i befintliga processer och strukturer i en verksamhet.[6]

[6] https://digg.se/kunskap-och-stod/metodstod-for-dataskydd-vid-innovation

För att lyckas med sitt integritetsskydd behöver en dataskyddsorganisation finnas på plats som medvetandegör integritetsskyddsfrågorna. Om kunskap om integritetsskyddet inte finns eller om det inte hanteras riskerar det att personuppgifter behandlas på ett otillåtet vis, eller att rutiner och arbetssätt implementeras som omedvetet ökar risken för personuppgifts-incidenter.

I ett ändamålsenligt och systematiskt integritetsskydd involveras dataskyddsombudet proaktivt och inte reaktivt för att aktivt rådge och utbilda gällande integritetsskyddet.

Om befintlig process och struktur inte omhändertar integritets-skyddet ska integritetsskyddet aktivt implementeras i dessa. Behov av nya processer och strukturer kan även finnas utifrån de arbetsuppgifter som lag och ny praxis från EU-domstolen kräver och då bör dessa prioriteras i VP-aktiviteter.

4.1 Integritetsskyddsanalys och dess processer

Den integritetsskyddsanalys och integritetsprocess som behöver finnas på plats beskrivs översiktligt i detta avsnitt.

Vid all behandling av personuppgifter ska alltid de grundläggande principerna införlivas i personuppgiftsbehandlingen. Nedan angivna principer ska därför initialt ingå i en integritetskyddsanalys inför ny behandling och i befintlig behandling för att dataskyddsregelverket ska vara införlivat korrekt.

4.1.1 Hantering av de grundläggande principerna

- Har den specifika personuppgiftsbehandlingen stöd i dataskyddsförordningen och är personuppgiftsbehandlingen proportionerlig? (*principen om laglighet och korrekthet*)
- Har stockholmaren och den anställde, de registrerade, fått lagstadgad information om den specifika personuppgiftsbehandlingen? (*principen om öppenhet*)
- Har insamling och användning av personuppgifter skett för specifika, särskilt angivna och berättigade ändamål? (*principen om ändamålsbegränsning*)
- Innebär personuppgiftsbehandlingen att personuppgifter behandlas på ett sätt som är oförenligt med dessa specifika,

angivna och berättigade ändamål? (*principen om ändamålsbegränsning*)
- Behandlas fler personuppgifter än vad som behövs för ändamålen? (principen om uppgiftsminimering).
- Är personuppgifterna riktiga och om nödvändigt uppdaterade? (principen om riktighet)
- Raderas personuppgifterna när de inte längre behövs[7] (*principen om uppgiftsminimering*)
- Skyddas personuppgifterna, ex. så att inte obehöriga får tillgång till dem eller så att de inte förloras eller manipuleras? (*principen om integritet och konfidentialitet*) - informationssäkerhet
- Sker dokumentation för att visa hur dataskydds-förordningen efterlevs? *(principen om ansvarsskyldighet)*

4.1.2 Laglig personuppgiftsbehandling

Då laglig eller rättslig grund för behandling av personuppgifter är central för all behandling kommer detta att kort åter beröras i årets rapport. Laglig grund innebär att det måste finnas ett uttryckligt stöd för behandlingen i dataskyddsordningen och det åligger en verksamhet att säkerställa att en korrekt laglig grund finns och används för nya och befintliga personuppgiftsbehandlingar.

Dataskyddsförordningen anger olika lagliga grunder. De är samtycke, behandlingen är nödvändig för att fullgöra ett avtal eller innan ett avtal ingås, fullgöra en rättslig förpliktelse, skydda intressen som är av grundläggande betydelse för den registrerade eller för en annan fysisk person, att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning samt intresseavvägning. Den rättsliga grunden intresseavvägning får inte användas av offentliga myndigheter när de fullgör sina uppgifter.

För att kunna använda den rättsliga grunden samtycke krävs att maktförhållandet är jämlikt. Det innebär att det ofta är olämpligt att använda samtycke i förhållandet myndighet – kommunmedlem och arbetsgivare – arbetstagare.

Behandling av integritetskänsliga personuppgifter som ex. personnummer och uppgift om brott samt känsliga personuppgifter har dessutom specialreglering i dataskyddsförordningen och

[7] Rätten till allmänna handlingar kan medföra begränsning i rätten till radering,

dataskyddslagen[8] avseende när dessa uppgifter får behandlas, vilket behöver beaktas i all personuppgiftsbehandling.

Vid behandling av känsliga personuppgifter är det viktigt att beakta att indirekta personuppgifter också kan utgöra känsliga personuppgifter, vilket EU-domstolen bl.a. lyft i mål C-184/20 Vyriausioji tarnybinés etikos komisija. Uppgifter om för- och efternamn på make/maka/sambo/partner konstaterades utgöra känsliga personuppgifter, då dessa indirekt kan avslöja uppgifter om individs sexualliv eller sexuella läggning.

4.1.3 Registrerades rättigheter

Dataskyddsförordningen är en rättighetslagstiftning som har sin grund i Europeiska konventionen om skydd för de mänskliga rättigheterna och EU-stadgan om de grundläggande rättigheterna.

Idag är det således centralt att hantera individens rättigheter korrekt. Rättigheterna är följande.

- Rätt till specifikt angiven information om hur individens personuppgifter behandlas
- Rätt till tillgång till personuppgifter som behandlas
- Rätt till rättelse och radering i vissa fall
- Rätt till dataportabilitet, överföring av personuppgifter, när förutsättningarna är uppfyllda
- Rätt att begära begränsning av personuppgiftsbehandling
- Rätt att invända mot personuppgiftsbehandling
- Rätt att i vissa fall inte omfattas av automatiserat individuellt beslutsfattande, inbegripet profilering

Under 2023 har tillsynsärenden avseende de registrerades rättigheter fortsatt att öka. Tillsynsmyndigheten har även behövt anpassa sig till att den legala kontexten sätts av EU-domstolen. Detta har resulterat i att tillsynsmyndigheten nu behöver utreda individuella klagomål i större utsträckning än tidigare. Den registrerade har idag även en större möjlighet att få sina klagomål prövade i sak i svensk domstol.[9]

Flertalet tillsynsbeslut avseende den registrerade rättigheter, visar nu att verksamheter som behandlar personuppgifter för egen och

[8] Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning
[9] Högsta förvaltningsdomstolens mål nr 6193-22, 3691-22

annans räkning behöver ha implementerat fungerande processer för att hantera rättigheterna.

I denna rapport berörs specifikt rätten till tillgång som fokusområde under avsnitt 4.2 Individens, den registrerades, rättigheter. Redan i detta sammanhang kan betonas att utan en process för att hantera registrerades rättigheter ökar risken för bristande förtroende för hur personuppgifter behandlas och bristande regelefterlevnad.

4.1.4 Ansvarsrollerna inom integritets- & dataskydd

I en integritetsskyddsanalys ska även ingå att fastställa ansvarsrollerna personuppgiftsansvarig[10], personuppgiftsbiträde[11] eller om gemensamt personuppgiftsansvar föreligger för den specifika personuppgiftsbehandlingen.[12]

Det är viktigt att betona att om en verksamhet inom staden behandlar personuppgifter för annan nämnds eller bolags räkning kan ett ansvar enligt dataskyddsförordningen föreligga som *personuppgiftsbiträde.* Så är fallet när kommunstyrelsen tillhandahåller och hanterar it-tjänster till övriga nämnder/bolag inom staden. Det innebär att kommunstyrelsen även blir medansvarig för att säkerheten för personuppgiftsbehandlingen motsvarar dataskyddslagstiftningen, rättslig praxis samt har en lagstadgad informationsskyldighet gentemot övriga nämnder och bolag inom staden.

Ett personuppgiftsbiträde ska exempelvis:

- Vidta alla åtgärder som krävs enligt artikel 32 säkerhet i samband med personuppgiftsbehandlingen
- Hjälpa den personuppgiftsansvarige med tekniska och organisatoriska åtgärder så att den personuppgiftsansvarige kan fullgöra sina skyldighet att svara på begäran om utövande av den registrerades rättigheter

[10] *Personuppgiftsansvarig* är en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter; 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.

[11] *Personuppgiftsbiträde* är en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning.

[12] Riktlinjer 07/2020 angående begreppen personuppgiftsansvarig och personuppgiftsbiträde i GDPR | European Data Protection Board (europa.eu)

- Bistå den personuppgiftsansvarige med att fullgöra säkerheten i samband med behandlingen, personuppgifts-incidenthantering och konsekvensbedömning avseende dataskydd.

När kommunstyrelsen genom stadsledningskontoret anskaffar gemensamma it-tjänster bör idag inbyggt dataskydd och dataskydd som standard kravställs och avtalas om. Inbyggt dataskydd och dataskydd som standard har redogjorts för i årsrapport 2021 och 2022 och återges även i år, då det är ett resurseffektivt och ändamålsenligt tillvägagångsätt att införliva dataskydds-lagstiftningen proaktivt och skapa en långsiktigt hållbar integritetskyddskultur.

Inbyggt dataskydd innebär att kommunstyrelsen, genom stads-ledningskontoret, ska ta hänsyn till integritetsskyddsreglerna redan när it-tjänst/system anskaffas och riktlinjer, tillämpnings-anvisningar, rutiner och metodstöd utformas. Det är ett effektivt sätt säkerställa att kraven i dataskyddsförordningen införlivas och att individens personliga integritet skyddas. Dataskydd som standard innebär i korthet att kommunstyrelsen, genom stadsledningskontoret, vid personuppgiftsbehandling ska säkerställa att personuppgifter i standardfallet inte behandlas i onödan, exempelvis genom att förvalda inställningar i en it-tjänst är satta så att inte mer information än nödvändigt samlas in, delas eller visas.

Annat uttryckt innebär inbyggt dataskydd att tekniska och organisatoriska åtgärder ska vara implementerade som beaktar att de grundläggande dataskyddsprinciperna och att övrigt integritetsregelverk integreras i de tekniska och organisatoriska åtgärderna. Dataskydd som standard innebär att integritetsvänliga teknologier och designmönster väljs.

4.2 Individens, den registrerades, rättigheter

I avsnitt 4.1.3 har de registrerades rättigheter berörts. I detta avsnitt ska rätten till tillgång, s.k. registerutdrag, särskilt beröras då det vanligtvis är den rättigheten den registrerade begär gentemot kommunstyrelsen och Stockholms stad. I detta avsnitt ska även de registrerades allmänna rätt till information kort beröras.

Europeiska dataskyddstyrelsen har tagit fram en vägledning som beskriver rätten till tillgång utifrån tidigare EU-domstolspraxis[13]. EU-domstolen har även i år preciserat rätten till tillgång ytterligare. Några av årets EU-domar behöver därför omnämnas för att förtydliga komplexiteten i regelefterlevnaden. EU-domstolen slår i domen, C-154/21, fast att individ har rätt att få veta vem hans/hennes personuppgifter har lämnats ut till, d.v.s. den faktiska mottagaren ska kunna anges i ett s.k. registerutdrag. I domen C-487/21 klargör EU-domstolen att rätten att erhålla en kopia av personuppgifter innebär att den registrerade ska förses med en exakt och begriplig återgivning av samtliga personuppgifter som behandlas. Om detta inte kan utföras kan kopia på utdrag eller hela handlingar komma att behöva lämnas ut. I domen C-579/21 framkommer att den registrerade har rätt att få information om syftet med behandlingen, t.ex. läsning av dennes personuppgifter och datum för läsning. I domen C-307/22 slås fast att en patient har rätt att kostnadsfritt få ut en kopia av sin journal.

Tillsynsmyndigheten har även under 2023 påfört organisation administrativ sanktionsavgifter avseende rätten till tillgång.[14]

Mot bakgrund av ovan är det nödvändigt att Stockholms stad och kommunstyrelsen, genom stadsledningskontoret, ser över processen för att ge den registrerade rätt till tillgång till sina personuppgifter. Europeiska dataskyddsstyrelsen har även aviserat att rätten tillgång kommer att vara en av styrelsens fokusområde för samordnade åtgärder för EU:s tillsynsmyndigheter, likaså svenska tillsynsmyndigheten, under 2024.[15]

Klagomålshanteringen har nu fått ökat genomslag hos tillsyns-myndigheten. Även detta kräver en genomlysning av hur rätten till tillgång hanteras inom staden och av dess kommunstyrelse, genom stadsledningskontoret.

Juridiska avdelningen har initierat ett samarbete med avdelningen för it och digitalisering avseende rätten till tillgång. Dataskydds-ombudet har involverats och har lämnat rekommendation om att en process, gärna digital, behöver tas fram för mottagande och hantering av begäran av den registrerades rättigheter i enlighet med Europeiska dataskyddsstyrelsens vägledning Guidelines 01/2022 on data subject rights - Right of access, version 2.0. Processen behöver

[13] Guidelines 01/2022 on data subject rights - Right of access | European Data Protection Board (europa.eu)
[14] Sanktionsavgift mot Spotify | IMY, diarienummer DI-2019-6696
[15] EDPB picks topic for 2024 Coordinated Action | European Data Protection Board (europa.eu), ”the implementation of the right of access by controllers”

även beakta EU-domstolens vida tolkning av *personuppgift* och *behandling* av personuppgift.

Juridiska avdelningen har även i årets verksamhetsplans (VP) aktiviteter, för att förstärka dataskyddet inom staden haft som aktivitet att se över informationstexterna till de registrerade hur personuppgifter behandlas. Uppdatering utifrån förtydligande praxis från tillsynsmyndigheten pågår.[16] Det är en aktivitet som kommer att fortgå under 2024. Dataskyddsombudet har även varit behjälplig i denna aktivitet och ytterligare informationstexter har tagits fram under 2023.

4.3 Dataskyddsombudets rekommendationer

Även i år har dataskyddsombudet involverats och gett råd vid begäran om tillgång till personuppgifter, s.k. registerutdrag, när dessa hanterats av KF/KS Kansli för kommunstyrelsen.

Arbetet med att samla in information, sammanställa svar och ge individ tillgång till sina personuppgifter och hur de behandlas blir allt mer komplexa att hantera. Risker för bristande regelefterlevnad utifrån att individ inte får fullständig information har ökat vilket kan leda till minskat förtroende och i förlängningen risk för administrativ sanktionsavgift.

Dataskyddsombudet bedömer att lagstadgad tidsram efterlevs vid alla begäranden avseende rättigheterna och endast ett fåtal begäranden har inkommit som avsett kommunstyrelsens behandling av personuppgifter.

Dataskyddsombudets rekommendationer är följande.

- Ta fram en process, som beaktar personuppgifts- och behandlingsbegreppets vida tolkning, gärna digital, som följer Europeiska dataskyddsstyrelsens Guidelines 01/2022 on data subject rights - Right of access, version 2.0, se Guidelines 01/2022 on data subject rights - Right of access | European Data Protection Board (europa.eu).
- Processen behöver beakta att kommunstyrelsen inte bara agerar i ansvarsrollen personuppgiftsansvarig utan även personuppgiftsbiträde till övriga nämnder och bolag när kommunstyrelsen behandlar personuppgifter för annan nämnd/bolags räkning.

[16] Klarna Bank AB, bristande information (imy.se), diarienummer DI-2019-4062

- Processen behöver beakta att kommunstyrelsen hanterar avtal och kontakten med leverantörer som är personuppgiftsbiträde till samtliga nämnder och bolag inom staden.
- Metodstöd för registrerades rättigheter behöver ses över och uppdateras, utifrån ny domstolspraxis och Europeiska dataskyddsstyrelsens vägledning.
- Fortsätta det pågående arbetet med att uppdatera informationstexter till de registrerade hur personuppgifter behandlas inom kommunstyrelsen och att kartlägga behov av ytterligare informationstexter till de registrerade.

4.4 Register för behandling, s.k. registerförteckning

När en integritetsskyddsanalys för en personuppgiftsbehandling är utförd ska personuppgiftsbehandlingen föras in i ett register över behandling utifrån kraven för personuppgiftsansvarig och personuppgiftsbiträde. För befintliga behandlingar som redan är införda i registret behöver även en integritetsskyddsanalys enligt ovan ha utförts.

Ett register är upprättat över kommunstyrelsens personuppgifts-behandlingar. Behandlingsregistret är en grundförutsättning för integritetsskyddsarbetet. En korrekt, komplett och systematiskt uppdaterat register säkerställer regelefterlevnad av integritetsskyddet.

Registret över behandling är processbaserat och utgår från kommunstyrelsens/stadsledningskontorets hanteringsanvisningar, dokumenthanteringsplans klassificeringsstruktur. Metoden har valts för att dra nytta av redan befintlig informationskartläggning och informationsredovisning samt för att underlätta att efterleva principen om lagringsminimering. Metoden kräver emellertid att det finns en upprättad process på SLK som bidrar till att när hanteringsanvisningar uppdateras ska även behandlingsregistret uppdateras, eller tvärtom. Här är det viktigt att bygga bort processer i stuprör för att få ett resurseffektivt och ändamålsenligt integritetsskydds- och arkivredovisningsarbete.

Rekommenderad upprättad process, i form av en rutin, har under 2023 tagits fram av kommunikation och omvärldsavdelningen – årlig översyn över registerförteckningar i Draftit, vilken fungerar

som ett stöd till integritetsskyddsarbetet på avdelningen. Rutinen har även samrådts med dataskyddsombudet.

4.5 Dataskyddsombudets rekommendationer

Utifrån de frågor och utbildningsinsatser vid införande av behandlingsprocesser, samt den insyn som dataskyddsombudet ges rekommenderar dataskyddsombudet följande.

Att tidigare rekommendationer från 2021 och 2022 årsrapporter omhändertas i verksamhetsplanens aktiviteter, samt att arbetsinsatsen med register för behandling inte ges olika vikt och resurs per avdelning, utan utförs systematiskt och ändamålsenligt med utpekat ansvar.

Dataskyddsombudet rekommenderar följande.

- Att stadsledningskontoret tar fram en gemensam process för att säkerställa att kommunstyrelsens register för behandling uppdateras och att systematisk inventering av personuppgiftsbehandling fortgår i enlighet med lagkrav.
- En utsedd dataskyddskontakt per avdelning behövs för att dataskyddsombudet ska kunna rådge systematiskt och ändamålsenligt och utbilda avseende register för behandling
- Dataskyddsombudets granskning av behandlingsregistret och dess resultat kan ske i samverkan med dataskydds-kontakt.
- En insats per avdelning behövs för att säkerställa att samtliga personuppgiftsbehandlingar utifrån särskilt personuppgiftsbiträdes och personuppgiftsansvarigs krav finns införda i behandlingsregistret. Behandlingsregistret behöver omfatta hela kommunstyrelsens ansvarsområde och uppgifter.
- Tillse att alla personuppgiftsbehandlingar i system finns registerförtecknade. Idag finns en differens mellan KLASSA och registerförteckningen.
- Prioritera att föra in personuppgiftsbehandlingar som är kopplade till automatiserat beslutsfattande, IoT, AI och skyddade personuppgifter.

4.6 Styrning och styrdokument avseende dataskydd

För fördjupning avseende organisationen stadenövergripande funktion för informationssäkerhet och det operativa dataskydds-utföraransvaret hänvisas till dataskyddsombudets GDPR-årsrapport 2021, diarienummer KS 2021/1557. Gällande information om lokal anvisning som beskriver hur stadens övergripande ledningssystem för informationssäkerhet omhändertas av kommunstyrelsen hänvisas till dataskyddsombudets GDPR-årsrapport 2022, diarienummer KS 2022/1278.

I detta sammanhang ska emellertid framhållas att införliva ett integritetsskydd för kommunstyrelsens räkning gäller oavsett om stadsledningskontoret arbetar lokalt eller i stadenövergripande frågor. Integritetsskyddet ska alltid införlivas utifrån ansvarsrollerna personuppgiftsansvarig och personuppgiftsbiträde. Stadenövergripande funktion för informationssäkerhet behöver även i sin funktion säkerställa att strategi, styrdokument och aktiviteter omhändertar integritetsskyddet när informationssäkerhet och dataskydd hanteras under samma paraply.

Det är därför det är så viktigt att betona att kommunstyrelsens dataskyddsombud kommer in proaktivt i början av alla kommun-styrelsens årsaktiviteter avseende personuppgiftshantering, då kommunstyrelsens dataskyddsombuds lagstadgade uppdrag och ställning omfattar alla aktiviteter som faller inom kommunstyrelsens ansvarsområde och uppgifter, både stadenövergripande och lokala uppgifter. Införlivandet av integritetsskyddet är således inte idag en valbar aktivitet, utan ska appliceras i samtliga funktioner och avdelningar på stadsledningskontoret för att stockholmarna och de anställda ska erhålla ett rättighetsskydd som lagstiftning och praxis kräver. Det är även obligatoriskt att ge dataskyddsombudet oberoende insyn för att kunna rådge avseende gällande dataskyddslagstiftning. Att ge dataskyddsombudet lagstadgade förutsättningar är obligatoriskt och sanktionsgrundande när så inte görs, vilket medför att stadsledningskontoret behöver ta fram process som omhändertar dessa lagkrav.

För att öka förståelsen för integritetsskyddet i verksamheterna har stadens informationssäkerhetsansvarig och kommunstyrelsens dataskyddsombud samt juridiska avdelningen i samarbete uppdaterat styrdokumentet *tillämpningsanvisning till stadens*

riktlinje för informationssäkerhet tillhörande Stockholms stads kvalitetsprogram.

I uppdateringsarbetet har dataskyddsombudets rekommendationer utifrån 2022 års GDPR-årsrapport hörsammats och införlivats i styrdokumentet. Dataskyddsombudets involvering har bidragit med att proaktivt förtydliga och förstärka integritetsskyddet, samt att pedagogiskt synliggöra frågorna och utvecklingsområden för verksamheten. Det har varit ett av de viktigaste rådgivningsområdena under 2023 för kommunstyrelsens dataskyddsombud.

Juridiska avdelningen, i samråd med dataskyddsombudet, har även i årets verksamhetsplansaktiviteter förstärkt integritetsskyddet genom att ta fram en vägledning avseende ansvarsrollerna i dataskydd, med för staden specifika exempel, som kompletterar gällande tillämpningsanvisning till stadens riktlinje för informationssäkerhet. Vägledningen kommer att publiceras på intranätet under 2024.

Vägledningen syftar till att förenkla införlivningen av ett resurseffektivt och ändamålsenligt integritetsskydd genom att verksamheten enkelt kan identifiera utifrån vilken ansvarsroll uppgifter utförs som påverkar stadens personuppgiftsbehandling och/eller innebär en faktisk behandling av personuppgifter.

Såsom i 2022 års rapport lyfts även i årets rapport att dataskydds-lagstiftningen kräver att rutiner och instruktioner finns på plats som instruerar hur medarbetare och externa får behandla personuppgifter.

4.7 Dataskyddsombudets rekommendationer

I dag finns som tidigare omnämnts riktlinje för informations-säkerhet i Stockholms stad och tillämpningsanvisningar till stadens riktlinje för informationssäkerhet som berör integritets- och dataskydd på en övergripande nivå.

Utifrån dataskyddslagstiftningen behöver en verksamhet emellertid beakta att lagstiftningen kräver att specifika organisatoriska åtgärder i form av rutiner och instruktioner behöver tas fram om hur personuppgifter faktiskt får hanteras. Ett tidigare exempel på instruktion som lyfts i årsrapporterna är hur personuppgifter får hanteras i e-post. Ytterligare exempel på rutiner är

kamerabevakning och publicering av personuppgifter i publikt diarium.

Dataskyddsombudets rekommendationer är följande.

- Förstärkande insats gällande skriftliga rutiner och instruktioner är en aktivitet för stadsledningskontoret som fortsatt rekommenderas
- Använd intranätet för att publicera rutiner och instruktioner
- Slutför det pågående arbetet med framtagande av instruktion för hur personuppgifter får behandlas i intern och extern e-post och koppla gärna instruktionen till användandet av krypteringsfunktionen säkra meddelanden.
- Utse ansvariga för framtagande av rutiner och instruktioner

4.8 Informationssäkerhet och dataskydd bör vara integrerade

Integritetsskyddet och informationssäkerhet bör vara integrerade, då en verksamhet kan dra nytta av informationssäkerhetsarbetet i sitt integritetsskyddsarbete. Integrationen främjar skyddet för den personliga integriteten.

Samtidigt är det viktigt att framhålla att informationssäkerhet inte kan likställas med integritets- eller dataskydd. Informationssäkerhet ingår i integritets- och dataskyddslagstiftningen och lagstiftningen styr vilken informationssäkerhet som ska appliceras på de faktiska personuppgifterna och personuppgiftsbehandlingen. Detta beror på att lagstiftningen bl.a. reglerar vad som är integritetsrisker och vad som är höga integritetsrisker.

Tillsynsmyndigheten har varje år en DSO-konferens. På årets konferens lyftes vikten av samarbete mellan informationssäkerhets-ansvarig, informationssäkerhetssamordnare och dataskyddsombud. Att se över gemensamma mål och utmaningar, hur drar man nytta av varandras arbetssätt och att man bör ta ett helhetsgrepp om informationssäkerheten. Detta samarbete är väletablerat för kommunstyrelsen. Ett utvecklingsområde för 2024 är nu när resurserna ökat på den stadenövergripande funktionen för informationssäkerhet att dataskyddsombudet fortsatt i god tid får oberoende insyn för att rådge gällande dataskyddslagstiftningen och hur den bör införlivas.

När integritetsskyddsanalysen genomförts som beskrivits i avsnitt 4.1 ska personuppgiftsbehandlingen informationsklassas enligt

stadens riktlinjer och tillämpningsanvisningar för informations-säkerhet.

4.8.1 Tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar

Vid informationsklassning behöver, om integritets- och dataskyddet ska beaktas, tekniska och organisatoriska åtgärder implementeras för att säkerställa en säkerhetsnivå som är lämplig i förhållande till *risken för fysiska personers rättigheter och friheter*.

Vid informationsklassningen behöver både personuppgiftsansvarig och personuppgiftsbiträdet *utifrån personuppgiftsbehandlingens art, omfattning, sammanhang och ändamål* vidta tekniska och organisatoriska säkerhetsåtgärder i förhållande till risken för de registrerade. De säkerhetsåtgärder som lagstiftningen lyfter särskilt är:

- pseudonymisering och kryptering av personuppgifter
- förmågan att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingssystemen och –tjänsterna
- 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 personuppgiftsbehandlingens säkerhet.

När personuppgiftsbehandlingens skyddsvärde ska bestämmas ska skyddsvärdet sättas utifrån dataskyddsrättsliga regelverket och vid bedömning av säkerhetsnivån ska särskild hänsyn tas till de risker som personuppgiftsbehandlingen medför i synnerhet avseende 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.

Säkerhetsrisker och hot mot den personliga integriteten varierar beroende på personuppgiftsbehandlingens omfattning och komplexitet. En behandling med omfattande personuppgifter och individer i beroendeställning såsom anställda och elever kräver en annan skyddsnivå än kontaktuppgifter i form av e-post för ett frivilligt nyhetsbrev. Vidare behöver skyddsnivån vara högre när integritetskänsliga och känsliga personuppgifter behandlas. I det här

sammanhanget måste betonas att EU-domstolen har kommit med domar som förtydligar att indirekta känsliga uppgifter såsom namn och partnerskap är känslig personuppgift om sexuell läggning likaså att individ har förvaltare är en känslig uppgift om hälsa.

Behov av organisatoriska åtgärder har redogjorts för ovan under avsnitt 4.6 Styrning och styrdokument avseende dataskydd.

4.8.2 Identifierade risker utifrån deltagande vid informationsklassning

En av flera aktiviteter där dataskyddsombudet naturligt involverats under 2023 är vid informationsklassning av information.

Vid informationsklassningen ska integritetsriskerna vävas in och värderas med övriga informationstillgångar. Informations-klassningsprotokollet uppmuntrar till denna hantering, likaså klassningsverktyget KLASSA.

Uppbyggnaden av KLASSA försvårar emellertid införlivandet av integritetsskyddet, då frågorna om dataskydd och GDPR kommer först i slutet av en klassning. Om verksamheten däremot utför en integritetskyddsanalys initialt inför personuppgiftsbehandling och inför informationsklassning omhändertas integritetsskyddet korrekt.

Om verksamheten inte gjort en integritetsskyddsanalys inför informationsklassningen, där säkerheten för personuppgifts-behandlingen ska sättas, kan det medföra att integritetsskyddet inte har införlivats fullt ut. Med andra ord sätts en säkerhet för personuppgiftsbehandlingen, men ex. de grundläggande principerna har inte beaktats och införlivats i behandlingen. Detta kan resultera i att personuppgifter behandlas i för stor omfattning och lagstöd för hela behandlingen kan därför saknas.

Konsultstöd tas ofta in som klassningsledare, vilka har kunskap i informationssäkerhet och hur information värderas ur ett informationssäkerhetsperspektiv men inte alltid hur risk för individens rättigheter och friheter ska värderas, vilket gör att dataskyddsombudet har haft en viktig roll att fylla vid en informationsklassning för att utbilda kring integritetsskyddet. Utbildning omfattar exempelvis att vissa behandlingar av personuppgifter kräver krypteringsskydd. Att verksamheten inte kan värdera personuppgifterna efter vilken skada de själva bedömer att individ kan drabbas av vid förlust av konfidentialitet, riktighet och

tillgång, utan integritetsrisker utifrån dataskyddsförordningen behöver beaktas. Vid en informationsklassning kan även en sammanblandning av offentlighetsprincipen och integritetsskyddet uppkomma. Offentlighetsprincipen och integritetsskyddet kan inte likställas eller användas som måttstock för personuppgifters och personuppgiftsbehandlingars skyddsvärde.

4.9 Dataskyddsombudets rekommendationer

Med anledning av att identifierade integritets- och dataskyddsrisker kan förebyggas och hanteras *rekommenderar dataskyddsombudet följande*.

- En VP-aktivitet för juridiska avdelningens framtagande av vägledning avseende *integritetsskyddsanalys* planeras för 2024
- Ett *metodstöd* behöver tas fram som förenklar för verksamheten *att värdera integritetsrisk* korrekt utifrån risken för fysiska personers rättigheter och friheter
- Säkerställa att tillämpningsanvisningar för informationssäkerhet, handböcker och informationsklassningsprotokoll hänvisar till framtagen vägledning avseende integritetsskyddsanalys och metodstöd för att värdera integritetsrisk för att väva in ett ändamålsenligt och systematiskt integritetsskydd under informationssäkerhetsparaplyet.
- Dataskyddsombudet utbildar avseende integritets-skyddsanalys och värdering av integritetsrisker
- Säkerställ att lokal anvisning för informationssäkerhet vid stadsledningskontoret integrerar dataskyddet på motsvarande sätt som informationssäkerhet. Detsamma gäller ledningens genomgång av informationssäkerhet, annars kan omedvetna integritetsrisker uppkomma för verksamheten.
- Det är en risk när endast informationssäkerhetssamordnare och inte längre dataskyddsombuden innefattas i dagens förankringsprocess för stadenövergripande funktionen för informationssäkerhet. Säkerställ att dataskyddsombudet involveras.

4.10 Konsekvensbedömning avseende dataskydd

En konsekvensbedömning avseende dataskydd är en obligatorisk riskbedömning och riskhantering. Konsekvensbedömningen innefattar identifiering av skyddsåtgärder och en rättslig genomgång av personuppgiftsbehandlingen, inför att en personuppgifts-behandling ska påbörjas som innebär hög integritetsrisk.[17]

Den höga integritetsrisken värderas inte utifrån ett verksamhets-perspektiv utan integritetsrisken värderas utifrån ett lagstadgat integritetsperspektiv, Integritetsskyddsmyndighetens förteckning och Europeiska dataskyddsstyrelsen vägledning om konsekvens-bedömning.[18] En omfattande personuppgiftsbehandling av individer som är i beroendeställning såsom exempelvis elever kräver idag att en konsekvensbedömning avseende dataskydd utförts. Att identifiera integritetsrisker och hantera dem är en viktig del av ändamålsenligt och systematiskt integritetsskyddsarbete. Tillsynsmyndigheten har även i år utdömt administrativ sanktionsavgift när kommun inte utfört konsekvensbedömning innan it-tjänst infördes där elever och anställdas personuppgifter behandlades.[19]

Det finns stadenövergripande *metodstöd och mall för konsekvens-bedömning avseende dataskydd.* Metodstödet innefattar även tröskelanalys och råd gällande referenskonsekvensbedömning.

Dataskyddsombudet är en obligatorisk part, som ska rådfrågas och övervaka när en konsekvensbedömning avseende dataskydd ska genomföras. Det innebär att dataskyddsombudet har insyn i konsekvensbedömningar avseende dataskydd. Genomförande av konsekvensbedömningar avseende dataskydd behöver ske i större utsträckning än idag, likaså användandet av referenskonsekvens-bedömning. Kommunala myndigheter som inför ett it-tjänst kan utföra en enda konsekvensbedömning, referenskonsekvens-bedömning som omfattar personuppgiftsbehandlingen av dessa

[17] Digitalisering och innovation, såsom IoT, myndighets digitala plattformar som ger service till stockholmare, kräver att konsekvensbedömningar avseende dataskydd utförs, likaså bakgrundskontroll inför rekrytering och när kommun samlar in personuppgifter innefattande bland annat lokaliseringsuppgifter i syfte att använda dessa vid exempelvis stads- och trafikplanering.
[18] ARTICLE29 - Guidelines on Data Protection Impact Assessment (DPIA) (wp248rev.01) (europa.eu) och Förteckning över när en konsekvensbedömning ska göras | IMY
[19] Sanktionsavgift mot kommun som inte bedömt konsekvenser innan Google Workspace infördes (imy.se), diarienummer IMY-2023-1647

enskilda personuppgiftsansvariga. I reglemente för kommunstyrelsen, KFS 2022:18, anges att styrelsen ska ansvara för stadens strategiska innovationsarbete och kvalitetsutvecklingsfrågor, samt ska styrelsen ansvara för att leda, strategiskt utveckla och samordna stadens gemensamma it- och digitaliseringsfrågor och vara systemägare för vissa stadsövergripande system. När kommunstyrelsen tillhandahåller gemensam it, stadsövergripande system och innovativa tjänster till övriga nämnder och bolag inom staden behöver kommunstyrelsen, genom stadsledningskontoret, driva att konsekvensbedömningar avseende dataskydd utförs, själv utföra i egenskap av personuppgiftsansvarig och delta vid konsekvensbedömningar avseende dataskydd när kommunstyrelsen agerar som personuppgiftsbiträde. Kommunstyrelsen kan komma att agera personuppgiftsbiträde när stadsledningskontoret tillhandahåller och förvaltar exempelvis sociala system, säkra meddelanden och säkra möten. Att utföra gemensamma referenskonsekvensbedömningar avseende dataskydd inom staden är ett resurseffektivt och ändamålsenligt sätt att införliva ett brett dataskydd.

Tillsynsmyndigheten har även under årets DSO-konferens aviserat att konsekvensbedömning avseende dataskydd kommer att vara ett fokusområde för myndigheten, likaså bakgrundskontroller.

4.11 Dataskyddsombudets rekommendationer

Dataskyddsombudet rekommenderar följande.

- Framtagande av en dokumenterad process för att genomföra referenskonsekvensbedömning avseende dataskydd inom staden. Metodstöd bör således omhänderta hur konsekvensbedömning kan utföras inom Stockholms stad som består av flera personuppgiftsansvariga nämnder/bolag och som även kan bli interna personuppgiftsbiträden till varandra.
- Genomförandet av konsekvensbedömning avseende dataskydd behöver ske i större utsträckning på stadsledningskontoret för kommunstyrelsens räkning i syfte att värna stockholmarens, kommunmedlemmarnas, och de anställdas integritet
- Respektive avdelning på stadsledningskontoret behöver fortsätta att kartlägga behov av konsekvensbedömning avseende dataskydd, gärna i samråd med dataskyddsjurist och dataskyddsombud

4.12 Hantering av personuppgiftsincidenter

En korrekt och lagenlig personuppgiftshantering innebär att kommunstyrelsen, genom stadsledningskontoret, ska ha förmåga att förebygga, *upptäcka, identifiera, hantera* och *anmäla person-uppgiftsincidenter*[20] inom 72 timmar till tillsynsmyndigheten i enligt med dataskyddsförordningen.[21] Anmälan till tillsyns-myndigheten ska göras, såvida det inte är osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter. Dataskyddsförordningen innehåller även ett obligatoriskt krav att *dokumentera* samtliga personuppgiftsincidenter. Dokumenteringskravet anger vad som ska dokumenteras för att tillsynsmyndigheten ska kunna kontrollera regelefterlevnad vid förfrågan.[22] *Vid en sannolik hög risk för berörd individ, den registrerade, ska även denne, utan onödigt dröjsmål, informeras om personuppgiftsincidenten*. Här ska åter betonas att integritetsrisk bestäms utifrån dataskyddslagstiftningen.

Kommunstyrelsen ska således ha förmåga och en ändamålsenlig process implementerad för stadsledningskontoret för att kunna efterleva dagens regelverk avseende personuppgiftsincidenter, såsom *personuppgiftsansvarig*. För att hantera incidenter, inklusive personuppgiftsincidenter har stadsledningskontoret en *rutin för hantering av informationssäkerhetsincidenter*, som publicerats på intranätet. Rutinen bygger på att alla medarbetare ska kunna hantera informationssäkerhetsincidenter och dokumentera dessa i stadens incidentverktyg.

Kommunstyrelsen, genom stadsledningskontoret, behöver dessutom beakta att kommunstyrelsen agerar såsom *personuppgiftsbiträde* när stadsledningskontoret tillhandahåller stadsgemensamma it-infrastrukturen och stadsövergripande system och behöver således *skyndsamt informera* berörda nämnder och bolag om person-

[20] 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.

[21] wp250rev_en (imy.se) , Guidelines 01/2021 on Examples regarding Personal Data Breach Notification | European Data Protection Board (europa.eu) och edpb_guidelines_202209_personal_data_breach_notification_targetedupdate_en.pdf (europa.eu)

[22] I dataskyddsförordningen artikel 33.5 anges att 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 av artikel 33.

uppgiftsincidenter, så att personuppgiftsansvariga nämnder och bolag kan bedöma de sannolika konsekvenserna[23] för berörda individer och om incidenten ska anmälas till tillsynsmyndigheten. Den lagstadgade information som ska tillhandahållas är:

- personuppgiftsincidentens art
- de kategorier registrerade och det ungefärliga antalet registrerade som är berörda
- de kategorier personuppgiftsposter och det ungefärliga antalet personuppgiftsposter som är berörda
- beskrivning av de åtgärder som har vidtagits eller föreslagits för att åtgärda personuppgiftsincidenten, inbegripet åtgärder för att mildra incidentens potentiella negativa effekter för de registrerade.

Kommunstyrelsens stadsledningskontor hanterar även *personuppgiftsbiträdesavtal och leverantörskontakter* för stadens nämnder och bolags räkning, vilket gör att stadsledningskontoret behöver säkerställa att samtliga nämnder och bolag inom staden får den information som de behöver. Information som behövs från externa personuppgiftsbiträden anges i punktform ovan. Stockholms stads nämnder och bolag behöver informationen för att de ska kunna utföra sitt personuppgiftsansvar korrekt vid en personuppgiftsincident.

Juridiska avdelningen i samråd med dataskyddsombudet har även i årets uppdatering av mall för personuppgiftsbiträdesavtal med instruktion uppdaterat att leverantör, såsom personuppgiftsbiträde, ska uppfylla sin informationsskyldighet avseende personuppgifts-incidenter på nämnd- och bolagsnivå enligt punktformslistan ovan.

Initial kontakt har tagits med dataskyddsombudet för rådgivning gällande integritetsskyddet, dataskyddslagkrav, vid behovs-insamling gällande systemstöd för informationssäkerhets-incidenthanteringen. Därefter har en förstudie för incident-hanteringsprocess skickats till dataskyddsombudet för granskning under december 2023. Då dataskyddsombudets årsrapports upprättande ska slutföras under december 2023 kan årets rapport inte omfatta förstudien, men den kommer att hanteras och granskas under 2024.

[23] Ex. diskriminering, identitetsstöld, bedrägeri, förlorat anseende och ekonomisk förlust för individ.

I förra årets årsrapport berördes att CERT, Computer Emergency Response Team[24] etablerats. Dataskyddsombudet lyfter åter hur viktigt det är att dataskyddsombudet får lämna råd avseende dataskyddsregelverket för att främja kommunstyrelsens efterlevnad av regelverket för personuppgiftsincidenter. Det finns effektivitetsvinster om integritetsskyddet kan vävas in i redan befintliga processer.

4.13 Dataskyddsombudets rekommendationer

Här finns en utvecklingspotential och dataskyddsombudet välkomnar förstudien för incidenthanteringsprocess inom informationssäkerhet. Samtidigt behöver tidigare rekommendationer från 2021 och 2022 årsrapporter fortsatt beaktas och förmågan att hantera personuppgiftsincidenter fortsatt utvecklas i samråd med dataskyddsombudet.

Dataskyddsombudet kan i år inte följa upp och granska en sammanhållen dokumentering av personuppgiftsincidenter på stadsledningskontoret för 2023. Inga incidenter på stadsledningskontoret har klassificerats som personuppgiftsincidenter i stadens incidentverktyg. Av de incidenter som dokumenterats under andra kategorier såsom exempelvis säkerhet/egendom rör bluffmejl, som inte resulterat i en faktisk personuppgiftsincident. Dataskyddsombudet har inte tillgång till it-säkerhetsincidenter, vilket gör att några slutsatser därav inte kan dras. Personuppgiftsincidenter har även diarieförts tidigare år, men inte för personuppgiftsincidenter som uppkommit under 2023.

Någon personuppgiftsincident, där kommunstyrelsen är personuppgiftsansvarig har inte inrapporterats till Integritetsskyddsmyndigheten under 2023.

Dataskyddsombudet är enligt lagstadgat uppdrag behjälplig vid personuppgiftincidenter när dataskyddsombudet blir involverat enligt rutin. Dataskyddsombudet involveras dock inte i den omfattning som är nödvändig vid incidenter, vilket kan ha att göra med uppdelningen lokalt och stadenövergripande arbete, som inte beaktar att dataskyddsombudet är kommunstyrelsens dataskyddsombud som ska kopplas in både när kommunstyrelsen, genom

[24] CERT avser förmågan att upptäcka, hantera och förebygga it-säkerhetsincidenter.

stadsledningskontoret agerar som personuppgiftsansvarig och personuppgiftsbiträde i likväl lokala som stadenövergripande informationssäkerhetsincidenter som innefattar personuppgifter.

Dataskyddsombudet rekommenderar följande.

- Det pågående arbetet med incidenthanteringsprocess behöver fortsätta och juridiska avdelningen inklusive dataskyddsombudet behöver vävas in för att proaktivt omhänderta integritetsskyddet.
- Process avseende hur kommunstyrelsen ska agera vid personuppgiftsincidenter utifrån ansvarsrollerna *personuppgiftsansvarig* och *personuppgiftsbiträde* behöver tas fram för att kommunstyrelsen och övriga nämnder och bolag ska kunna efterleva exempelvis kort tidsram.
- Det är fortsatt viktigt att medarbetare och externa på stadsledningskontoret tar del av upprättad informations-säkerhetsincidentrutin och utbildas i vad som utgör en personuppgiftsincident och hur dessa ska hanteras under 2024
- Utse incidentledare i förväg som har dataskyddsombudet som naturlig samverkanspart för rådgivning
- Dokumentationsskyldigheten behöver säkerställas så att det vid var tid finns en stadsledningskontorsövergripande dokumentering över personuppgiftsincidenter enligt lagkrav.
- Dataskyddsombudet måste proaktivt och omgående involveras i all incidenthantering innefattande person-uppgifter, då dataskyddsombudet är den registrerades och tillsynsmyndighetens kontaktpunkt till kommunstyrelsen och dess stadsledningskontor.
- Framtagna processer och informationssäkerhetsincidentrutin ska testas och övas av verksamheten.

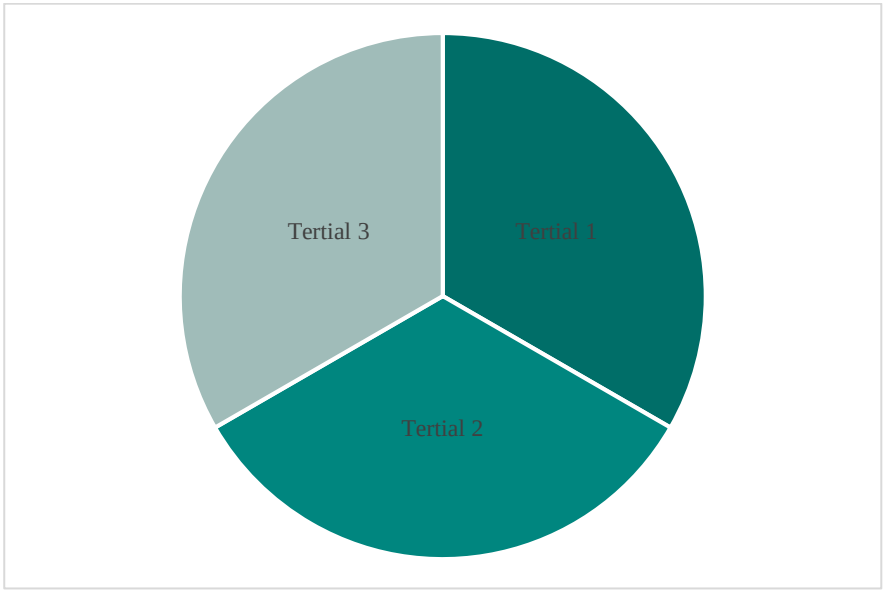
4.14 Tredjelandsöverföring

Under 2023 har avdelningarna inom stadsledningskontoret fortsatt att bedriva ett omfattande arbete i samråd med dataskyddsombudet och juridiska avdelningen avseende överföring av personuppgifter till tredjeländer. I arbetet har juridiska avdelningens *mall för tredjelandsöverföringsbedömning, Transfer Impact Assessment, och PM med vägledning vid användning av standardavtalsklausuler* använts.

I arbetet har dataskyddsombudet observerat att leverantör kan lämna uppgift om att tredjelandsöverföring inte förekommer men efter utredning framkommer att underbiträden används av leverantör som innebär att tredjelandsöverföring kan komma att ske. Leverantör kan även lämna uppgift om att personuppgifter inte behandlas när dessa behandlas pseudonymiserade, vilket innebär att ett fortsatt samråd behövs med juridiska avdelningen och dataskyddsombudet i dessa frågor för att höja *kunskapsnivån* generellt i dessa integritetsskyddsfrågor. Juridiska avdelningen har även i samråd med dataskyddsombudet en pågående VP-aktivitet över 2024 avseende *upphandling och dataskydd* där bl.a. tredjelands-överföringsfrågan adresseras för att förenkla och underlätta verksamhetens hantering av dessa frågor. Mall för personuppgifts-biträdesavtal med instruktion har även uppdaterats avseende tredjelandsöverföring.

Den 14 september 2023 fattade även stadsledningskontorets styrgrupp för informationssäkerhet ett reviderat inriktningsbeslut med anledning av EU-kommissionens beslut om adekvat skyddsnivå för USA[25]. Styrgruppen, som består av stadsjuristen, avdelningschef för säkerhetsavdelningen, utvecklingschef på personalstrategiska avdelningen samt företrädare för avdelningen för it och digitalisering, betonade behovet av fortsatt återhållsamhet avseende tredjelandsöverföring till USA, vilket välkomnas av dataskyddsombudet.

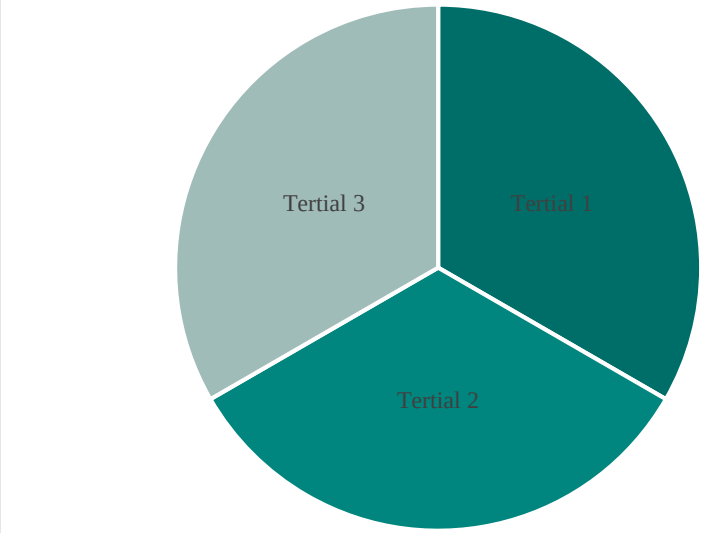
4.15 Dataskyddsombudets årshjul



[25] Diarienummer KS 2023/241

- Tertial 1 Dataskyddsombudet utbildar och rådger ex. avseende integritetsskyddsanalys, integritetsrisker och nödvändiga integritetsskyddsprocesser
- Tertial 2 Dataskyddsombudet utför systematiska kontroller, uppföljningar, rapporteringar av resultat och rekommendationer avseende integritetsskydd
- Tertial 3 – Dataskyddsombudet rådger utifrån resultat och rekommendationer avseende integritetsskyddsarbetet för att integritetsrisker ska kunna omhändertas av dataskyddsorganisationen.

4.16 Dataskyddsorganisationens årshjul



- Tertial 1 Dataskyddsorganisationen utför operativt arbete såsom integritetsskyddsanalys, registerförtecknar, tar fram rutin för personuppgiftsbehandling, värderar information i en informationsklassning och arbetar med handlingsplan, utför riskanalys avseende integritetsskydd och konsekvensbedömning avseende dataskydd vid behov etc. Dataskyddsorganisationen utbildas utifrån identifierade utbildningsbehov, ex. hantering av personuppgiftsincidenter, och rekommendationer av dataskyddsombudet
- Tertial 2 Dataskyddsorganisationen deltar vid dataskyddsombudets systematiska kontroller, uppföljningar och

rapporteringar av resultat och rekommendationer på avdelningsnivå
- Tertial 3 – Dataskyddsombudet rådger utifrån resultat och rekommendationer avseende integritetsskyddsarbetet för att identifierade integritetsrisker ska kunna omhändertas av dataskyddsorganisationen.

5 Risk och dataskydd

Integritetsskyddsarbete utifrån integritetsskyddsanalys främjar hantering av integritetsrisker. Det är viktigt att verksamhetens kunskap om integritetsrisk höjs i form av ex. utbildning. I tidigare GDPR-årsrapporter har risker inom dataskydd och att dataskydds-förordningen är uppbyggd utifrån risk beskrivits. Det innebär i praktiken att dokumenterade *riskanalyser* utifrån individens rättigheter och friheter ska utföras och att konsekvensbedömning avseende dataskydd ska utföras vid *hög risk* för individs rättigheter och friheter.

Riskanalys avseende dataskydd ska således utföras med individen i fokus och bedömningen ska baseras på om personuppgifts-behandlingen kan äventyra den registrerades friheter och rättigheter och om personuppgiftsbehandlingen kan orsaka den registrerade fysisk, materiell eller immateriell skada. Bedömningarna ska utföras utifrån dataskyddsregelverket, samt Europiska dataskyddsstyrelsen vägledningar, även tillsynspraxis finns som stöd för dessa bedömningar. *Riskbedömningarna ska ha sin grund i hur dataskyddsregelverket värderar behandlingens art, omfattning, sammanhang och ändamål.*

Dataskyddsombudet rekommenderar att *handbok för riskanalys och riskhantering vid SLK, inom området informationssäkerhet, inklusive integritets- och dataskydd* ses över 2024 och uppdateras i förenlighet med utveckling av dataskyddspraxis.

5.1 Dataskyddsombudets rekommendation

Stadsledningskontoret som helhet behöver under 2024 utifrån ett ledningsperspektiv säkerställa ett ändamålsenligt och systematiskt integritetsskydd. Där tydliga processer införlivas för att omsätta riktlinje för informationssäkerhet och dess tillämpningsanvisningar, där integritetsskyddet får ta sin rätta plats. Att metodstöd för integritetsskyddsanalys integreras i informationssäkerhetsmodellen

tydliggör det faktiska integritets- och dataskyddsarbetet. Det är vidare viktigt att integritetsskyddet är proaktivt och känt bland dem som behandlar personuppgifter i sitt dagliga arbete.

Kommunstyrelsens dataskyddsombud och stödfunktionerna såsom informationssäkerhetssamordnare och dataskyddshandläggare bistår utifrån sina roller i detta arbete. En kanal som används i detta arbete är vår intranätssida. På intranätssidan informeras om arkiv-redovisningens, registerförteckningens, informationsklassningens, SLK:s riskanalys och riskhantering samt konsekvensbedömning avseende dataskydds samband för att synergieffekter ska tillvaratas.

Avsikten med dataskyddsombudets råd i GDPR-årsrapport är att rådge stadsledningskontoret för att öka förståelsen för integritets-skyddet och dess utveckling genom domstolspraxis och därigenom minska dataskyddsrisker samt att verka för ett proaktivt införlivat integritetsskydd. Dataskyddsombudet ska även rapportera till kommunstyrelsen för att styrelsen ska få insyn i vad dataskydds-ombudets rådgivande och granskande arbete visar avseende stadsledningskontorets integritetsskyddsarbete. För att kommunstyrelsen ska kunna styra det ändamålsenliga och systematiska dataskyddsarbetet både på strategisk och operativ nivå under 2024.

6 Genomförda granskningar

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

Dataskyddsombudet har även under 2023 prioriterat att ge råd om dataskyddslagstiftning och fått delta rådgivande i pågående dataskyddsarbete, särskilt vid utförande av tredjelandsöverförings-bedömningar och informationsklassning. Medarbetare har även löpande ställt dataskyddsfrågor till dataskyddsombudet. Några riktade granskningar under 2023 har inte utförts, tillsammans med verksamheten, utan istället har granskning ägt rum utifrån pågående frågor och den insyn som dataskyddsombudet getts under året, vilken sammanfattats utförligt ovan i form av riktade rekom-mendationer.

Utifrån rekommendationerna i föregående årsrapport har dataskyddsombudet fått rådge och involverats avseende förstärkning av dataskydd i tillämpningsanvisningar till stadens riktlinje för informationssäkerhet. Sett till spridning och kunskapshöjning värderas denna aktivitet högt av dataskyddsombudet.

Det är vidare viktigt, för att värna stockholmarnas och anställdas rätt till integritet och dataskydd, att dataskyddsombudets råd obligatoriskt inhämtas av stadsledningskontoret i inledningsskedet vid innovation, IoT, AI, automatiskt beslutsfattande och när integritetskänsliga och känsliga personuppgifter behandlas oavsett ansvarsroll i dataskyddslagstiftningen.

Riktad granskning bör framgent vidtas tillsammans med verksamheten utifrån ett framtaget *årshjul för integritetsskydd*, där dataskyddsombudets årshjul samverkar med dataskyddsorganisationens årshjul för det operativa dataskyddsarbetet.

7 Övrigt att rapportera

7.1 Analys av dataskyddsombudens årsrapporter

Stockholms stads nämnder och bolag ses utifrån den registrerades perspektiv, som en organisation, en kommun. Ur stockholmarnas perspektiv är det därför viktiga att samordna och följa upp integritets- och dataskyddet på övergripande nivå.

Dataskyddsombudets årsrapporter är ett medel för kommunstyrelsen att säkerställa samordning och uppföljning av integritetsskyddet inom staden. Dataskyddsombudets kvarstår i sin rekommendation att stadenövergripande informationssäkerhet bör utföra en samlad analys av samtliga nämnders och bolags dataskyddsombuds GDPR-årsrapporter för att se övergripande trender och integritetsrisker. Analysen bör delas med stadens alla dataskyddsombud och vid behov bör denna analys föranleda aktiviteter eller åtgärder för att stärka det stadenövergripande integritetsskyddet.