Stockholms stad

GDPR Årsrapport

2022

Stockholms stads kommunstyrelse

GDPR årsrapport
Januari 2023

Dnr: KS 2022/1278
Datum: 2023-01-02
Kontaktperson: Kommunstyrelsens dataskyddsombud

1 Bakgrund

Dataskyddslagstiftningen, där dataskyddsförordningen[1] ingår, ska värna och skydda individens integritet och har sin grund i Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna, Europakonventionen. Att implementera dataskyddsregelverket säkerställer således att kommunmedlemmarnas, medarbetarnas samt andra individers mänskliga rättigheter till respekt för sitt privat- och familjeliv, sitt hem och sin korrespondens införlivas i verksamheten.

Dataskyddslagstiftningens regelverk behöver vara fullt ut implementerat utifrån kommunstyrelsens olika ansvarsområden. Det innebär att integritetsskyddet bland annat ska vara implementerat i kommunstyrelsens ansvarsområde att leda och samordna den kommunala förvaltningen. I reglementet för kommunstyrelsen, 2022:18, framgår kommunstyrelsens uppgifter och ansvarsområden, likaså att uppgifter kan tillkomma genom kommunallagen och annan lagstiftning. Dataskyddslagstiftningen är ett exempel på annan tvingande lagstiftning.

Enligt dataskyddsförordningen ska utnämnt dataskyddsombud oberoende rapportera direkt till högsta förvaltningsnivå avseende verksamhetens efterlevnad av dataskyddslagstiftningen och ge råd avseende de skyldigheter som lagstiftningen uppställer. Kommunstyrelsen ska säkerställa att dataskyddsombudet på ett korrekt sätt och i god tid deltar i alla frågor som rör skyddet av personuppgifter, inbegripet strategin för skydd av personuppgifter och ansvarstilldelningen, för att kunna fullgöra sitt lagstadgade uppdrag.

Dataskyddsombudets årsrapport är ett medel för Stockholms stads kommunstyrelse att ta emot de råd som dataskyddsombudet är skyldig att ge till ansvarig enligt dataskyddsförordningen samt för att få insyn i vad dataskyddsombudets granskande arbete av verksamhetens status avseende integritet och dataskydd visar. Årsrapporten syftar vidare till att Stockholms stads kommunstyrelse ska kunna följa upp och styra verksamhetens systematiska strategiska och operativa integritets- och dataskyddsarbete samt

[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)

kunna fatta beslut om prioriteringar, resurser och aktiviteter för 2023.

I egenskap av kommunstyrelsens dataskyddsombud lämnar jag följande årsrapport.

.

Innehåll

2 Sammanfattning

Att värna stockholmarens, medarbetarens och andra individers integritet när dennes personuppgifter behandlas är idag en naturlig del av lagstiftningen för att möjliggöra digitalisering, innovation och användande av AI. Integritetsskyddet behöver även vara en naturlig del inom kommunstyrelsens ansvarsområden och uppgifter genom ett systematiskt strategiskt och operativt implementerat dataskyddsarbete.

Enligt gällande dataskyddsförordning ska kommunstyrelsens dataskyddsombud rapportera direkt till högsta förvaltningsnivå. Genom denna rapport genomför dataskyddsombudet sin lagstadgade uppgift och på så vis värnas den registrerades, vars personuppgifter behandlas, integritet.

I GDPR-årsrapport 2022 kommer dataskyddslagstiftning och praxis beskrivas för att öka förståelsen för vad dataskydd och integritetsskydd innebär och vad som behöver beaktas i det strategiska och operativa dataskyddsarbetet för kommunstyrelsens del.

I rapporten kommer beskrivas hur viktigt det är att dataskyddsrättsligt identifiera utifrån vilken ansvarsroll personuppgifter behandlas, att personuppgiftsbehandling har en laglig grund och att alla grundläggande principer genomsyrar faktisk personuppgiftsbehandling. När detta är säkerställt ska adekvata tekniska och organisatoriska åtgärder implementeras utifrån ett dataskyddsrättsligt och informationssäkerhetsperspektiv. Vid implementering av tekniska och organisatoriska åtgärder bör integritetsvänliga åtgärder väljas med inbyggt dataskydd och dataskydd som standard för att underlätta det operativa dataskyddsarbetet.

GDPR-årsrapport 2022 kommer vidare att behandla de obligatoriska områdena registerförteckning, styrdokument avseende dataskydd, tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar, konsekvensbedömning avseende dataskydd, individens rättigheter och personuppgiftsincident. Löpande i årsrapporten kommer dataskyddsombudet att ge råd och rekommendationer för att höja kunskapsnivån och säkerställa regelefterlevnaden avseende integritetsskydd, dataskydd.

GDPR årsrapport 2022 kommer även att beröra risk och dataskydd. Riskanalysen och konsekvensbedömningen avseende dataskydd ska ha individens fokus och inte verksamhetens fokus. Vid riskanalys av integritetsskyddet är det därför viktigt att ta del av dataskyddsrättslig praxis och vägledningar. GDPR-årsrapport kommer att hänvisa till vägledningar.

Därefter redogörs för genomförda granskningar av dataskyddsombudet samt informeras om obligatoriska e-utbildningar avseende dataskydd och informationssäkerhet. GDPR-årsrapport kommer även kort beröra arbetet med bedömning av tredjelandsöverföring med anledning av EU-domstolens dom, Schrems II.

GDPR-årsrapporten avslutas med avsnitt om inhämtning av GDPR-årsrapport/er och riktade aktiviteter med anledning av årsrapporten. För att värna individ och integritetsskydd är det viktigt att följa upp och genomföra dataskyddsaktiviteter utifrån dataskyddsombudets årsrapport. Dataskyddsombudet bistår gärna med råd vid framtagande av aktiviteter.

2.1 Översikt över resultat av granskning och dataskyddsombudets råd

2.1.1 Registerförteckning

En riktad insats behöver utföras av verksamheten för att säkerställa att alla personuppgiftsbehandlingar inom kommunstyrelsens ansvarsområde och uppgifter är registerförtecknade utifrån ansvarsrollerna personuppgiftsansvarig och personuppgiftsbiträde. Med verksamheten avses i detta fall respektive avdelning inom stadsledningskontoret. Skillnaden mellan registerförteckning och informationsklassning behöver även omhändertas.

Dataskyddsombudet kommer att informera verksamheten om vad stickprovskontrollerna i registerförteckningen visar.

Lokal anvisning för kommunstyrelsen behöver tydligt peka ut vem eller roll som ansvarar för den systematiska inventeringen av personuppgiftsbehandling och registerförteckning inom kommunstyrelsens ansvarsområde. Inventering och registerförteckning bör ske i samverkan med arbetet avseende kommunstyrelsens/SLK:s hanteringsanvisningar samt informationsklassning.

2.1.2 Styrdokument avseende dataskydd

Dataskyddsombudets råd från 2021 kvarstår. Rutiner och instruktioner gällande hur personuppgifter får behandlas inom kommunstyrelsens ansvarsområde och uppgifter behöver prioriteras. Under 2023 behöver det även tydligt pekas ut vem, roll, som ansvarar för genomförandet av denna aktivitet. Befintliga och framtida rutiner och instruktioner kan med fördel samlas och publiceras på intranätet under informationssäkerhet och dataskydd på stadsledningskontoret.

En förstärkning av dataskyddsperspektivet i tillämpningsanvisning till stadens riktlinje för informationssäkerhet planeras för 2023.

2.1.3 Implementera tekniska och organisatoriska skyddsåtgärder och hantera personuppgiftsincidenter

Dataskyddslagstiftningen reglerar numera skyddsnivån för individernas personuppgifter. Detta är särskilt viktigt att känna till när information och personuppgiftsbehandlingar informationsklassas och tekniska och organisatoriska åtgärder implementeras. Lagstiftningen föreskriver vilken säkerhet som ska vara implementerad i verksamheten, vilket kräver ett nära samarbete mellan it, jurist eller annan dataskyddskunnig medarbetare samt dataskyddsombud. Medarbetare kan med fördel utbildas gällande dataskyddsrättsliga krav och normerande informationsklassning innehållande dataskyddsrättsliga krav kan tas fram.

I kommunstyrelsens ansvarsområde ingår att vara objektägare till stadsövergripande system och tillhandahålla stadsgemensam it-infrastruktur. Då är det särskilt viktigt att beakta att kommun-styrelsen har ett eget ansvar enligt dataskyddslagstiftningen gällande de tekniska åtgärderna och organisatoriska åtgärderna och behöver säkerställa en säkerhetsnivå som är lämplig för faktisk personuppgiftsbehandling som sker i dessa system eller tjänster.

I GDPR-årsrapport 2021 har lyfts fram att informationsklassning behöver prioriteras. Denna rekommendation har fått genomslag och det syns i årets kartläggning över genomförd informationsklassning.

Ett viktigt fokusområde för integritetsskyddet är att tekniska och organisatoriska säkerhetsåtgärder är implementerade och att

åtgärderna motsvarar gällande lagkrav. Ett sätt att förenkla uppgiften är att säkerställa att it-säkerhetsregelverket speglar de dataskyddsrättsliga regelverket.

Personuppgiftsincident är definierat i dataskyddsförordningen, även när den ska anmälas till Integritetsskyddsmyndigheten och när berörd individ ska informeras om personuppgiftsincidenten.

Under 2022 har stadsledningskontorets rutin för hantering av informationssäkerhetsincidenter, inklusive personuppgifts-incidenter, uppdaterats av informationssäkerhetssamordnare.

Rådet från GDPR-årsrapport 2021 kvarstår;
Tillhandahållandet av stadsövergripande system och stadsgemensam it-infrastruktur innebär att kommunstyrelsen behöver förbättra sin förmåga att identifiera, dokumentera, hantera och skyndsamt informera övriga nämnder och bolag om personuppgiftsincidenter. Generellt behöver dessa förmågor fortsättas att utvecklas.

Dataskyddsombudet ser även att verksamheten behöver utbildas gällande lagkraven om personuppgiftsincident för att förbättra regelefterlevnaden avseende dataskydd. Dataskyddsombudet kommer även i början av 2023 slutföra en vägledning gällande dataskyddsförordningens regelverk avseende en personuppgiftsincident. Vägledningen kommer att publiceras på intranätet under informationssäkerhet och dataskydd på stadsledningskontoret.

Enligt information ska under 2023 en behovsinsamling ske gällande systemstöd för informationssäkerhetsarbetet, däri ingår systemstöd för personuppgiftsincidentsdokumentation. Dataskyddsombudets rådgivning gällande dataskyddslagkrav bör inhämtas i arbetet under 2023.

Under 2023 är det även viktigt att dataskyddsombudet får ge råd avseende dataskyddsregelverket i förhållande till arbetet med CERT för att främja kommunstyrelsen efterlevnad av att ha förmåga att upptäcka och identifiera personuppgiftsincidenter samt för att efterleva lagkraven utifrån ansvarsrollerna personuppgiftsansvarig och personuppgiftsbiträde.

2.1.4 Konsekvensbedömning avseende dataskydd

Konsekvensbedömning avseende dataskydd är en rättsligt reglerad bedömning och ska utföras när hög risk för individs integritet, rättigheter och friheter enligt gällande lagstiftning föreligger. Syftet med bedömningen är att förebygga risker för individ och personuppgiftsincidenter innan de uppkommer.

Uppdaterat metodstöd och mall för konsekvensbedömning avseende dataskydd har tagits fram under 2022.

För att efterleva Stockholms stads kvalitetsprogram och säkerställa att relevant lagstiftning följs och att stockholmarnas personuppgifter och integritet hanteras aktsamt bör användandet av metodstöd och mall för konsekvensbedömning avseende dataskydd öka inom kommunstyrelsen.

Metodstöd bör även tas fram på strategisk nivå gällande referenskonsekvensbedömning och hur konsekvensbedömning ska utföras inom Stockholms stad som består av flera personuppgifts-ansvariga nämnder/bolag och där nämnder/bolag kan bli interna personuppgiftsbiträden.

2.1.5 Individens rättigheter

KF/KS Kansli samordnar och säkerställer att frågor som rör individens rättigheter kopplade till kommunstyrelsen hanteras enligt dataskyddslagstiftningen. Med anledning av uppdaterad praxis och vägledning behöver kommunstyrelsens metodstöd för hantering av den registrerades rättigheter ses över under 2023.

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

3 Dataskyddslagstiftningen

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

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

I Sverige återfinns skyddet för personlig integritet i regeringsformen 2 kapitlet 6 §, var och en är gentemot det allmänna skyddad mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskilds personliga förhållanden.

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

Kompletterande lagstiftning är dataskyddslagen[2]. Annan dataskyddslagstiftning innefattar även registerförfattningar såsom patientdatalagen, och kamerabevakningslagen.

3.1 Ansvarsroller

För att kunna implementera och efterleva dataskyddslagstiftningen korrekt behöver verksamheten initialt fastställa enligt gällande

[2] Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning

riktlinje från Europeiska dataskyddsstyrelsen[3] eppb_guidelines_202007_controllerprocessor_final_en.pdf (europa.eu) eller gällande lag om verksamheten är personuppgiftsansvarig eller personuppgiftsbiträde.

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.

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

Då Stockholms stad består av flera nämnder och bolag, tillika personuppgiftsansvariga kan interna biträdesförhållanden uppkomma inom stadens verksamhet. Ett exempel på internt biträdesförhållande är när kommunstyrelsens stadsledningskontor förvaltar sociala system åt socialnämnden, stadsdelsnämnder m.fl. I sådant fall är socialnämnden personuppgiftsansvarig och kommunstyrelsen personuppgiftsbiträde.

När ett personuppgiftsbiträdesförhållande identifieras ska ett personuppgiftsbiträdesavtal med ifyllande av instruktion tecknas. När ett personuppgiftsbiträdesförhållande uppstår mellan stadens nämnder ska istället den stadeninterna instruktionen för personuppgiftsbehandling mellan nämnder tecknas.

Juridiska avdelningen har på uppdrag av funktionen för stadenövergripande informationssäkerhet och i samråd med dataskyddsombudet under 2022 uppdaterat mall för personuppgiftsbiträdesavtal med instruktion och stadenintern instruktion för personuppgiftsbehandling mellan nämnder, som ska användas när ett personuppgiftsbiträdesförhållande uppkommer.

[3] Europeiska dataskyddsstyrelsen är ett oberoende europeiskt organ som bidrar till en enhetlig tillämpning av dataskyddsregler i hela Europeiska unionen och främjar samarbete mellan EU:s dataskyddsmyndigheter.
Dataskyddsstyrelsen består av företrädare för nationella dataskyddsmyndigheter och Europeiska datatillsynsmannen (EDPS).

Vilken ansvarsroll kommunstyrelsen har utifrån dataskydds-lagstiftningen påverkar vilket regelverk i dataskyddsförordningen som behöver implementeras i verksamheten. I rapporten kommer de olika ansvarsrollerna beröras, då kommunstyrelsen kan vara både personuppgiftsansvarig, för egen del, och personuppgiftsbiträde när styrelsens uppgifter och ansvarsområden utförs av stadsledningskontoret.

3.2 Personuppgift och personuppgiftsbehandling

Nästa steg för implementering av dataskyddsregelverket är att kartlägga och inventera vilka personuppgifter[4] och personuppgiftsbehandling[5] som verksamheten hanterar inom kommunstyrelsens hela ansvarsområde både som personuppgiftsansvarig och personuppgiftsbiträde till andra nämnder och bolag inom Stockholms stad. Observera att personuppgiftsbegreppet är vidsträckt och omfattar även indirekta uppgifter som kan hänföras till en individ, såsom exempelvis lokaliseringsuppgifter och metadata i digitala tjänster och system. Anledningen till att båda begreppen personuppgift och personuppgiftsbehandling är vidsträckta är för att integritetsskyddet inte ska urholkas.

Tillsynsmyndigheten, Integritetsskyddsmyndigheten, delar in personuppgifter i personuppgifter, integritetskänsliga och känsliga personuppgifter.

Integritetskänsliga personuppgifter är exempelvis personnummer, samordningsnummer, löneuppgifter, uppgifter om lagöverträdelser, värderande uppgifter, till exempel uppgifter från utvecklingssamtal, uppgifter om resultat från personlighetstester eller personlighets-profiler, information som rör någons privata sfär och uppgifter om

[4] varje upplysning som avser en identifierad eller identifierbar fysisk person (nedan kallad en registrerad), varvid en identifierbarfysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.

[5] en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.

sociala förhållanden. Integritetskänsliga personuppgifter och känsliga personuppgifter kräver högre säkerhetsnivå, påverkar riskbedömningar och krav för konsekvensbedömning av dataskydd samt att personuppgiftincident behöver anmälas till Integritetsskyddsmyndigheten.

Känsliga personuppgifter definieras i dataskyddsförordningen och är personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening och behandling av genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning. Dessa personuppgifter får endast behandlas om ett undantag enligt dataskyddsförordningen föreligger.

Under 2022 har EU-domstolen i domen *C-184/20 Vyriausioji tarnybinės etikos komisija* tydliggjort att personuppgifter om relationsstatus är en känslig uppgift, då den avslöjar en fysisk persons sexualliv eller sexuella läggning.

Integritetsskyddsmyndigheten har även den 20 december 2022 publicerat ett rättsligt ställningstagande, *IMYRS 2022:3*, där Integritetsskyddsmyndigheten anger att en uppgift om att en person har förvaltare enligt 11 kap. föräldrabalken (FB) utgör en uppgift om hälsa och är en känslig personuppgift.

Praxis från EU-domstolen och Integritetskyddsmyndighetens rättsliga ställningstaganden påverkar således skyddsnivån som krävs vid personuppgiftsbehandling. Det innebär konkret att stadsledningskontorets avdelningar behöver ta hänsyn till praxis och rättsliga ställningstaganden vid informationsklassning och utföra eventuella nödvändiga justeringar i befintlig informationsklassning och registerförteckning. Detta föranleder att kommunstyrelsen under 2023 behöver säkerställa att uppdateringar i registerförteckning och informationsklassningar utförs.

3.3 Grundläggande principer

Verksamheten behöver även säkerställa att alla personuppgifts-behandlingar inom kommunstyrelsens ansvarsområde, både befintliga och framtida behandlingar iakttar de grundläggande dataskyddsprinciperna i artikel 5 i dataskyddsförordningen. De grundläggande principerna ska genomsyra all personuppgifts-

behandling och sätter ramarna för att en personuppgiftsbehandling ska vara tillåten.

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

Principerna innebär i korthet följande. Den personuppgiftsansvariga måste ha stöd i dataskyddsförordningen för att få behandla personuppgifter. Personuppgifter får bara samlas in för specifika, särskilt angivna och berättigade ändamål och fler personuppgifter får inte behandlas än vad som behövs för ändamålen. Personuppgifterna ska vara riktiga och personuppgifter som inte behövs ska raderas[6]. Personuppgifterna ska skyddas så att inte obehöriga får tillgång till dem eller att de förvanskas, förloras eller förstörs. Den personuppgiftsansvarige ska även visa att den efterlever och hur den efterlever dataskyddsförordningen.

3.4 Laglig grund

Vad innebär då laglig grund eller rättslig grund? Det innebär att verksamheten behöver ta ställning till om personuppgifts-behandlingen är laglig enligt dataskyddsförordningen innan personuppgiftsbehandling påbörjas och för befintlig behandling.

Ställningstagande om rättslig grund är särskilt viktigt vid innovation och användande av IoT. Dataskyddspraxis visar idag att Integritetsmyndigheten särskilt i sina tillsyner bedömer om personuppgiftsbehandlingen har laglig grund

Det finns sex 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

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

använda samtycke i förhållandet myndighet – kommunmedlem och arbetsgivare – medarbetare.

Det är alltid den personuppgiftsansvarige som ska säkerställa om denne har rättslig grund att behandla personuppgifter.

4 Obligatoriska rapporteringsområden

Dataskyddsombudets årsrapport inom Stockholms stad avser att minst behandla sex obligatoriska rapporteringsområden.

De obligatoriska rapporteringsområdena är registerförteckning, styrdokument avseende dataskydd, tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar, konsekvensbedömning avseende dataskydd, individens rättigheter och personuppgifts-incident.

Nedan redogörs för de obligatoriska rapporteringsområdena.

4.1 Registerförteckning

I dataskyddsombudets årsrapport 2021 redogjordes för lagstiftning och utveckling av praxis avseende skyldigheten att föra register över personuppgiftsbehandling, registerförteckning.

Det som bör lyftas fram för 2022 utifrån lagstiftning och praxis är att registerförteckningsskyldigheten föreligger för hela kommunstyrelsens ansvarsområde och både utifrån ansvarsrollerna när kommunstyrelsen är personuppgiftsansvarig och internt personuppgiftsbiträde inom staden till övriga nämnder och bolag. Dataskyddsförordningen anger detaljerat vad ett behandlingsregister ska innehålla utifrån de olika ansvarsrollerna. I Integritetsskydds-myndigheten praxis framkommer att registerförteckningen är en viktig grundförutsättning för det interna integritetsarbetet och att en korrekt, komplett och systematiskt uppdaterad förteckning säkerställer regelefterlevnad av integritetsskyddet.

4.1.1 Status för registerförteckning och dataskyddsombudets råd

Kommunstyrelsens registerförteckning är digitaliserad och utgår ifrån personuppgiftsbehandlingarna när kommunstyrelsen är personuppgiftsansvarig och i personuppgiftsbiträdesrollen utifrån it-system/tjänst som kommunstyrelsen tillhandahåller till övriga nämnder och bolag inom Stockholms stad.

Ram och utgångspunkt för registerförteckningen är hanterings-anvisningarna för kommunstyrelsen/stadsledningskontoret, dokumenthanteringsplan. Det innebär att registerförteckningen håller samma kvalité som arkivredovisningen, även kallad informationsredovisningen. Grunden för informationsredovisningen är klassificeringsstrukturen som visar enligt vilka processer myndigheten arbetar samt styr hur de enskilda informations-mängderna ska hanteras. Detta redovisas i en hanteringsanvisning, vilken således ska åskådliggöra all information inom kommunstyrelsens ansvarsområde, såväl den som ska bevaras som den som ska gallras. Här finns således en synergi och resurs-effektivitet om avdelningarnas arkivredogörare och avdelningarnas registerförtecknare samordnar informationsredovisningen till hanteringsanvisningarna och registerförteckningen av personuppgiftsbehandlingarna. Det finns emellertid även en integritetsrisk om informationsredovisningen, arkivredovisningen inte innehåller fullständig, korrekt eller uppdaterad information om de personuppgiftsbehandlingar som de facto utförs.

Det är således viktigt att det finns ett utpekat operativt ansvar inom varje avdelning på stadsledningskontoret för att säkerställa att hela kommunstyrelsens ansvarsområde är registerförtecknat avseende de faktiska personuppgiftsbehandlingarna.

Idag följs det operativa registerförteckningsarbetet upp till viss del av informationssäkerhetssamordnare i och med ledningens genomgång av informationssäkerhet. När informationssäkerhets-samordnare rapporterar antalet informationsklassningar i jämförelse med registerförteckningar i januari 2023 framkommer att det finns en skillnad mellan informationsklassificerad information i system och registerförtecknade personuppgiftsbehandlingar som utförs i system. Informationsklassificerade system är högre till antal än personuppgiftsbehandlingar i system. Detta bör följas upp av avdelningarna inom stadsledningskontoret under 2023 för att säkerställa korrektheten och kvalitén på registerförteckningen.

Det finns således ett samband mellan arkivredovisning, informationsklassning av information och registerförteckning av personuppgifter, då alla aktiviteter avser att ringa in den information/personuppgifter som hanteras inom kommunstyrelsens ansvarsområde. Om verksamheten samverkar i dessa aktiviteter kommer alla aktiviteter tillsammans bidra till att faktisk information skyddas och till regelefterlevnad.

Kommunstyrelsens dataskyddsombud och dataskyddshandläggare har varit verksamheten behjälplig vid ett fåtal nya register-förteckningar under 2022. Dataskyddshandläggare har även per mejl 2022 påmint avdelningarna om att registerförteckningarna behöver ses över och att alla personuppgiftsbehandlingar behöver registerförtecknas.

Kommunstyrelsens dataskyddsombud har även gjort stickprovskontroller och identifierat att vissa uppdateringar under 2023 är nödvändiga bland annat på grund av att förnyade informationsklassificeringar gjorts samt att dataskyddsrättslig praxis under 2022 behöver införlivas i registerförteckningen. Samtidigt behöver ytterligare kontroller utföras avseende om alla kommunstyrelsens ansvarsområden innehållande personuppgifter är registerförtecknade under 2023.

Under 2022 har informationssäkerhetssamordnare, dataskyddshandläggare och dataskyddsombud tagit fram en intranätssida, informationssäkerhet och dataskydd på stadsledningskontoret, Informationssäkerhet och dataskydd på stadsledningskontoret - Stockholms stads intranät

På intranätssidan informeras om arkivredovisningens, registerförteckningens och informationsklassningens samband för att synergieffekter ska tillvaratas fullt ut. Det är viktigt att denna information når medarbetare som registerförtecknar personuppgifts-behandlingar inom kommunstyrelsens ansvarsområde.

Det kan vidare noteras att ansvarsfördelningen av det operativa ansvaret för att tillse att avdelningarna systematiskt för registerförteckning behöver vara tydlig. Delegationsordningen bör även ses över. Detta möjliggör resurseffektivitet, då information kan kommuniceras till rätt person/er och nödvändig information från dataskyddsombudet om uppdateringar på grund av lagkrav kan kommuniceras löpande skriftligt till berörda och inte först i en årsrapport från dataskyddsombudet till kommunstyrelsen.

Slutligen är dataskyddsombudets råd från 2021 fortfarande aktuella, vilket innefattar fortsatt löpande systematisk inventering av personuppgiftsbehandling inom kommunstyrelsens ansvarsområde, i samverkan med fortsatt systematisk uppdatering av hanteringsanvisningarna och fortsatt granskning av registerförteckningen 2023 tillsammans med verksamheten.

4.2 Styrdokument avseende dataskydd

I dataskyddsombudets årsrapport 2021 redogjordes för lagstiftning och principerna om inbyggt dataskydd och dataskydd som standard.

Det som bör lyftas för 2022 utifrån dataskyddslagstiftning och praxis är att lagstiftning och praxis från Integritets-skyddsmyndigheten och domstol visar idag på vikten och skyldigheten att ta fram rutiner och instruktioner gällande hur personuppgifter får behandlas. Medarbetare ska exempelvis få instruktioner från arbetsgivare gällande hur personuppgifter får behandlas i de it tjänster/system som används.

I årsrapport 2021 redogjordes även för organiseringen stadsövergripande funktion för informationssäkerhet och det operativa informationssäkerhets- och dataskyddsutföransvaret. Den centrala funktionen för stadenövergripande informationssäkerhets uppdrag och ansvar är att styra, utveckla och följa upp informationssäkerhetsarbetet i staden. Funktionen för stadsövergripande informationssäkerhet tar även fram metodstöd, handböcker, mallar, utbildningsmaterial och liknande som ger stöd för olika analyser och aktiviteter som ska utföras i nämnder och bolagsstyrelser i Stockholms stad.

Det operativa informationssäkerhetsansvaret och personuppgifts-ansvaret åligger respektive nämnd och styrelse. Det innebär för kommunstyrelsens del att dataskyddsregelverket och krav om informationssäkerhet utifrån personuppgiftsbehandlingens art, omfattning, sammanhang och ändamål samt riskerna för fysiska personers rättigheter och friheter behöver implementeras i hela kommunstyrelsens ansvarsområde och uppgifter. Till stöd för att utföra detta finns idag en informationssäkerhetssamordnare och dataskyddshandläggare. I dataskyddsombudets lagstadgade roll ingår att ge råd om dataskyddslagstiftning, strategier, riktlinjer, anvisningar och granska faktisk personuppgiftsbehandling. Det innebär att ett dataskyddsombud inte kan vara operativ. Lagstiftningen anger även att när kommunstyrelsen agerar i

ansvarsrollerna personuppgiftsansvarig och personuppgiftsbiträde ska denne säkerställa att dataskyddsombudet på ett korrekt sätt och i god tid deltar i alla frågor som rör skyddet av personuppgifter.

4.2.1 Status för styrdokument avseende dataskydd och dataskyddsombudets råd

Vid genomgång av styrdokument som har relevans för integritetsskyddet bör följande styrdokument omnämnas och granskas för att dataskyddsombudet ska kunna ge råd avseende dataskyddsregelverket och dess implementering;

- Stockholms stads kvalitetsprogram
- Riktlinje för informationssäkerhet i Stockholms stad
- Tillämpningsanvisning till stadens riktlinje för informationssäkerhet
- Mall lokal anvisning för informationssäkerhet

Stockholms stads kvalitetsprogram beslutades den 21 februari 2022 av kommunfullmäktige. Programmet är stadens styrande dokument för kvalitetsarbetet och tydliggör ansvaret inom staden för kvaliteten vid tillhandahållande av service och tjänster till alla stockholmare. För att hålla hög kvalité krävs ständiga förbättringar, innovation och digitalisering. I kvalitetsprogrammet anges att informationssäkerhet och integritetsskydd har en självklar plats i stadens kvalitetsarbete och att staden har ett ansvar och en skyldighet att säkerställa att relevant lagstiftning följs och att stockholmarnas personuppgifter och integritet inte ska äventyras.

Att kvalitetsprogrammet omnämner integritetsskydd är en viktig signal, då det i omvärldsbevakning framkommer att vid innovation och digitalisering krävs idag att legala förutsättningar beaktas redan i inledningsskedet. EU sätter ramen för ”Europe´s Digital Decade Strategy” som innefattar en mängd regelverk för information. Dataskyddsförordningen och kompletterande lagstiftning gäller dock fortfarande vid all personuppgiftsbehandling.

Kompletterande riktlinje och tillämpningsanvisning till kvalitetsprogrammet har också tagits fram genom riktlinje för informationssäkerhet i Stockholms stad och tillämpningsanvisning till stadens riktlinje för informationssäkerhet.

I riktlinje för informationssäkerhet definieras dataskydd som innebärande skydd av personuppgifter enligt kraven i dataskyddsförordningen. I riktlinjen anges även att dataskydd är en

del av informationssäkerhetsarbetet i staden och arbetet med dataskydd är integrerat i det generella informationssäkerhetsarbetet. Här är det som dataskyddsombud viktigt att påminna om att det finns flera dataskyddsregelverk, se gärna Så hänger lagarna ihop | IMY.

Till riktlinje för informationssäkerhet hör även en tillämpnings-anvisning för informationssäkerhet. Tillämpningsanvisningen är mer detaljerad än riktlinjen och i den ingår dataskydd. Tillämpningsanvisningen kan uppdateras årsvis. Under 2022 har uppdateringsbehov identifierats för dataskydd, integritetsskydd, bland annat finns ett behov av att tydliggöra ansvarsrollerna enligt dataskyddsförordningen och vilket ansvar respektive roll medför för verksamheten, samt skrivningar avseende rollen dataskyddsombud. Detta uppdateringsbehov planeras att hanteras 2023.

I tillämpningsanvisningen adresseras även att förvaltnings-chef/bolagschef ska för nämndens/styrelsens räkning fastställa en så kallad lokal anvisning som beskriver hur stadens övergripande ledningssystem för informationssäkerhet omhändertas i den egna verksamheten. Den lokala anvisningen ska gås igenom årligen och revideras vid behov. Den lokala anvisningen ska minst beskriva ansvarsfördelning inom den egna informationssäkerhets-organisationen (roller och mandat), vilken effekt informationssäkerhetsarbetet ska leda till, specifik lagstiftning som gäller för verksamhetens informationshantering samt hur arbetet följs upp. Det har tagits fram en mall för lokal anvisning för informationssäkerhet som ska fungera som ett stöd för uppgiften.

I och med att dataskyddsarbetet är samordnat med informations-säkerhetsarbetet enligt befintliga styrdokument behöver mall för lokal anvisning även väva in dataskydd som Integritets-skyddsmyndigheten definierar som hela det regelverk som syftar till att tillgodose registrerades rätt till privatliv i samband med behandling av personuppgifter. Det handlar om att personuppgiftsbehandling sker i enlighet med de grundläggande dataskyddsprinciperna, att behandlingen är laglig, att registrerades rättigheter tillgodoses och att inblandade aktörer uppfyller alla sina respektive skyldigheter, inklusive upprätthållandet av en lämplig säkerhet, se IMY-bloggen: Informationssäkerhet vs it-säkerhet – vad är vad?

När det gäller instruktioner för hur personuppgifter får behandlas och rutiner som behandlar integritetsskydd behövs idag en

förstärkning och viss insats är under planering för 2023. Vem som är ansvarig för detta arbete behöver emellertid utses.

På intranätssidan för informationssäkerhet och dataskydd på stadsledningskontoret finns rubriken våra rutiner inom dataskydd, där framtida rutiner med fördel kan tillgängliggöras Informationssäkerhet och dataskydd på stadsledningskontoret - Stockholms stads intranät.

Integritetsskyddsmyndighetens tillsynsbeslut och domstolspraxis har även under 2022 visat på vikten av att ha dataskyddsrutiner och instruktioner implementerade i verksamheten.

Slutligen är dataskyddsombudets råd från 2021 fortfarande aktuella. Dataskyddsombudet rekommenderar fortsatt att kommunstyrelsens verksamhet under 2023 prioriterar framtagandet av ytterligare rutiner och instruktioner gällande hur personuppgifter får behandlas. I GDPR-årsrapport lyftes särskilt fram behov av instruktion hur personuppgifter får hanteras i e-post internt och externt. En sådan instruktion är under framtagande och kommer att publiceras under 2023.

4.3 Tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar

Efter att ställningstagande om laglig grund och implementering av de grundläggande dataskyddsprinciperna ska lämpliga tekniska och organisatoriska åtgärder implementeras för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken för fysiska personers rättigheter och friheter.

I artikel 32 i dataskyddsförordningen, säkerhet i samband med behandlingen, anges
1. Med beaktande av den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige och personuppgiftsbiträdet vidta lämpliga *tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken, inbegripet, när det är lämpligt*
a) pseudonymisering och kryptering av personuppgifter,
b) förmågan att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingssystemen och -tjänsterna,

c) förmågan att återställa tillgängligheten och tillgången till personuppgifter i rimlig tid vid en fysisk eller teknisk incident,
d) ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet.
2. Vid bedömningen av lämplig säkerhetsnivå ska särskild hänsyn tas till de risker som behandling medför, i synnerhet från 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.
3. Anslutning till en godkänd uppförandekod som avses i artikel 40 eller en godkänd certifieringsmekanism som avses i artikel 42 får användas för att visa att kraven i punkt 1 i den här artikeln följs.
4. Den personuppgiftsansvarige och personuppgiftsbiträdet ska vidta åtgärder för att säkerställa att varje fysisk person som utför arbete under den personuppgiftsansvariges eller personuppgiftsbiträdets överinseende, och som får tillgång till personuppgifter, endast behandlar dessa på instruktion från den personuppgiftsansvarige, om inte unionsrätten eller medlemsstaternas nationella rätt ålägger honom eller henne att göra det.

I KFS 2022:18 reglemente för kommunstyrelsen 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. Ur ett integritetsperspektiv är det viktigt vid innovation, digitalisering och it att utreda ansvarsrollerna enligt dataskyddslagstiftningen, då även personuppgiftsbiträdet har ett ansvar för bland annat säkerheten enligt ovan. Detta blir även relevant för staden, då kommunstyrelsen, när styrelsen tillhandahåller gemensam it och innovativa tjänster till övriga nämnder och bolag, blir ett internt personuppgiftsbiträde och behöver uppfylla även den ansvarsrollens skyldigheter.

Under avsnitt 3.2 Personuppgift och personuppgiftsbehandling ovan har personuppgiftsbegreppet och vad som är integritetskänsliga och känsliga personuppgifter berörts. Här kan återigen lyftas fram att integritetskänsliga och känsliga personuppgifter kräver en högre säkerhetsnivå som exempelvis krypterad e-post. Även person-uppgifter som vanligtvis inte är integritetskänsliga eller inte är känsliga personuppgifter kan beroende på sin art, omfattning, sammanhang och ändamål ändå kräva en högre säkerhetsnivå. Idag finns dataskyddspraxis i form av tillsynsbeslut och domstolsavgöranden avseende säkerhet för personuppgifts-behandling. Det behöver beaktas vid informationsklassning av

personuppgifter och personuppgiftsbehandling. Lagstiftning föreskriver nu vilken säkerhet som ska vara implementerad i verksamheten, vilket kräver ett nära samarbete mellan it, jurist eller annan dataskyddskunnig medarbetare samt dataskyddsombud.

Behov av organisatoriska åtgärder har redogjorts för ovan under avsnitt 4.2 Styrdokument avseende dataskydd.

4.3.1 Status för tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar och dataskyddsombudets råd

Enligt dataskyddsförordningen är personuppgiftsansvarig nämnd ytterst ansvarig för personuppgiftsbehandlingen och personuppgiftsansvaret kan aldrig överlåtas. Emellertid har personuppgiftsbiträdet fått utökade skyldigheter och ett eget ansvar för personuppgiftsbehandlingen, exempelvis att föra register över personuppgiftsbehandlingar och att säkerställa en lämplig säkerhetsnivå. Ett personuppgiftsbiträde kan även påföras administrativ sanktionsavgift.

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

Stockholms stads informationstillgångar ska informationsklassas enligt gällande riktlinjer och tillämpningsanvisningar för informationssäkerhet. Under 2022 har kartläggningsarbetet av informationssäkerhetssamordnare fortsatt avseende vilka informationstillgångar/tjänster/system som är informationsklassade och vad som kvarstår. Kartläggningsarbetet visar att verksamheten under 2022 har prioriterat informationsklassningsarbetet och dataskyddsombudets råd om prioritering har omhändertagits. Ett viktigt fokusområde för integritetsskyddet är att tekniska och organisatoriska säkerhetsåtgärder är implementerade och att åtgärderna motsvarar gällande lagkrav. Ett sätt att förenkla uppgiften är att säkerställa att it-säkerhetsregelverket speglar de dataskyddsrättsliga regelverket. Här har ett samarbete etablerats mellan funktionen för stadenövergripande informationssäkerhet och

dataskyddsombudet. Ett annat sätt är att operativt arbeta med inbyggt dataskydd och dataskydd som standard.

Inbyggt dataskydd innebär att verksamheten ska ta hänsyn till integritetsskyddsreglerna redan när it-tjänst/system och rutiner utformas. Det är ett effektivt sätt säkerställa att kraven i dataskyddsförordningen uppfylls och att individens personliga integritet skyddas. Dataskydd som standard innebär i korthet att verksamheten som behandlar personuppgifter ska säkerställa att personuppgifter i standardfallet inte behandlas i onödan, exempelvis genom att förvalda inställningar i en tjänst är satta så att inte mer information än nödvändigt samlas in, delas eller visas.

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 åtgärderna. Dataskydd som standard innebär att integritetsvänliga teknologier och designmönster bör väljas.

Slutligen rekommenderar dataskyddsombudet att det säkerställs att de kravställda skyddsåtgärderna i informationsklassningen implementeras och att skyddsnivåerna är i paritet med gällande lagstiftning. För att underlätta arbetet kan normerande klassningsnivåer tas fram.

Observera att begreppet känsliga personuppgifter har utvidgats under 2022, i jämförelse med verksamhetens hantering av personuppgifter, av EU-domstolen och Integritetsskydds-myndighetens rättsliga ställningstagande som tagit upp under avsnitt 3.2 Personuppgift och personuppgiftsbehandling. Detta har en direkt påverkan på informationssäkerhetsarbetet och informationsklassningen.

Medarbetare behöver således utbildas gällande dataskyddsrättslig påverkan på informationsklassning för att integritetsskyddet ska fullt ut integreras med informationssäkerhetsarbetet.

4.4 Konsekvensbedömning avseende dataskydd

I dataskyddslagstiftningen finns det numera en skyldighet att genomföra en konsekvensbedömning avseende dataskydd. Det är en bedömning, utifrån individens perspektiv, med en fastställd rättslig

ram som innefattar en riskbedömning och riskhantering. Syftet med konsekvensbedömning avseende dataskydd är att förebygga risker för individ och personuppgiftsincidenter innan de uppkommer.

En konsekvensbedömning ska alltid utföras när hög risk föreligger för individ. Hög risk utgår ifrån dataskyddsregelverket och Integritetsskyddsmyndighetens förteckning[7]. Det innebär att verksamheten inte kan fatta beslut om konsekvensbedömning ska utföras eller inte innan den minst tagit del av Integritetsskydds-myndighetens förteckning.

4.4.1 Status för konsekvensbedömning avseende dataskydd och dataskyddsombudets råd

Under 2022 har juridiska avdelningen i samråd med dataskydds-ombudet på uppdrag av funktionen för stadenövergripande informationssäkerhet uppdaterat metodstöd och mall för konsekvensbedömning avseende dataskydd.[8] Metodstöd innehåller vägledning om när och varför en konsekvensbedömning ska genomföras, tröskelanalys för att avgöra om konsekvensbedömning behöver genomföras med anledning av hög risk, referenskonsekvensbedömning samt vad en konsekvensbedömning ska innehålla. Metodstödet avser att öka förståelsen för konsekvensbedömning avseende dataskydd och när en konsekvensbedömning behöver utföras av kommunstyrelsen eller kommunstyrelsen behöver delta, då styrelsen innehar ansvarsrollen personuppgiftsbiträde.

Under 2022 har även informationssäkerhetssamordnare i samråd med dataskyddsombudet tagit fram ett flöde som är publicerat på intranätet[9], för att öka förståelsen för att det finns samband mellan aktiviteterna registerförteckning, informationsklassning, tekniska och organisatoriska skyddsåtgärder, riskanalys och konsekvensbedömning avseende dataskydd.

Dataskyddsombudet är en obligatorisk part när en konsekvens-bedömning ska utföras av personuppgiftsansvarig enligt

---

[7] ARTICLE29 - Guidelines on Data Protection Impact Assessment (DPIA) (wp248rev.01) (europa.eu) och Förteckning över när en konsekvensbedömning ska göras | IMY

[8] Finns publicerade på intranätet under avsnittet konsekvensbedömningar Dataskyddsförordningen (GDPR) och personuppgiftsbehandling - Stockholms stads intranät

[9] https://intranat.stockholm.se/PageFiles/97577/%c3%96versiktsbild.pptx

dataskyddsförordningen. I dataskyddsförordningen anges att dataskyddsombudet ska rådfrågas och även övervaka genomförandet av en konsekvensbedömning. Det innebär att dataskyddsombudet har insyn i om en konsekvensbedömning utförts av verksamheten för kommunstyrelsens räkning. Under 2022 har dataskyddsombudets deltagit i en konsekvensbedömning avseende dataskydd för Stockholms stads visselblåsarfunktion, då kommunstyrelsen ansvarar för en stadsgemensam intern rapporteringskanal enligt lagen om skydd för personer som rapporterar om missförhållanden.[10] Det pågår även konsekvensbedömningar där kommunstyrelsen är personuppgifts-biträde gällande digitalisering av vissa sociala personuppgifters flöden, där har kommunstyrelsens dataskyddsombud deltagit till viss del och fått lämna övergripande råd utifrån ett personuppgifts-biträdesperspektiv, då kommunstyrelsen har ett visst ansvar för tekniska och organisatoriska skyddsåtgärder.

Som dataskyddsombud rekommenderar jag att verksamheten tar del av informationen på Integritetsskyddsmyndighetens webbsida Förteckning över när en konsekvensbedömning ska göras | IMY, då digitalisering och innovation, såsom IoT, myndighets digitala plattformar som ger service till stockholmare, idag 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.

För att efterleva kvalitetsprogrammet och säkerställa att relevant lagstiftning följs och att stockholmarnas personuppgifter och integritet värnas bör användandet av metodstöd och mall för konsekvensbedömning avseende dataskydd öka på stadsledningskontoret. Dataskyddsombudet rekommenderar att en kartläggning genomförs under 2023 på respektive avdelning gällande befintliga personuppgiftsbehandlingar som kräver en konsekvensbedömning. Detta får gärna ske i samråd med dataskyddsombud och informationssäkerhetssamordnare.

Metodstöd bör även tas fram på strategisk nivå gällande referens-konsekvensbedömning och hur konsekvensbedömning ska utföras inom Stockholms stad som består av flera personuppgiftsansvariga nämnder/bolag och där nämnder/bolag kan bli interna personuppgiftsbiträden till varandra.

[10] Lag (2021:890) om skydd för personer som rapporterar om missförhållanden

4.5 Individens rättigheter

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

Under 2022 har Integritetsskyddsmyndigheten inlett tillsyn och tillsynsbeslut har publicerats gällande individens rättigheter och informationsplikten. Specifik tillsynspraxis finns även gällande kraven för identifiering när den registrerade önskar tillvarata sina rättigheter i kontakt med personuppgiftsansvarig.

4.5.1 Status för individens rättigheter och dataskyddsombudets råd

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

KF/KS Kansli har även under 2022 samarbetat med dataskyddsombudet vid faktisk hantering av rättigheterna. På grund av utveckling av vägledningar[11] och praxis behöver emellertid metodstöd för hur rättigheterna ska hanteras av kommunstyrelsen ses över under 2023.

Alla frågor och individs begäran om rättighet som har inkommit till kommunstyrelsen 2022 har hanterats inom föreskriven lagstadgad tidsram om trettio dagar. Årligen hanteras ungefär fyra till fem inkomna begäranden avseende den registrerades rättigheter som avser kommunstyrelsen behandling av personuppgifter som personuppgiftsansvarig. Under 2022 var inkomna förfrågningar lägre än föregående år.

[11] Guidelines 01/2022 on data subject rights - Right of access | European Data Protection Board (europa.eu)

Slutligen rekommenderas att verksamheten behöver utöver uppdatering av metodstöd, se över publicerade informationstexter om hur personuppgifter behandlas och den faktiska hanteringen vid kontakt med den registrerade för att säkerställa att ett korrekt integritetsskydd är implementerat. Publicerade informationstexter behöver exempelvis utvecklas i linje med tillsynsmyndighetens praxis och om informationstexter för personuppgiftsbehandling saknas utifrån gällande praxis behöver detta identifieras.

4.6 Personuppgiftsincident

En personuppgiftsincident[12] inträffar när personuppgift som kommunstyrelsen behandlar berörs av en säkerhetsincident som resulterar i ett brott mot konfidentialitet, tillgänglighet eller riktighet avseende individens rättigheter och friheter.

I artikel 33 dataskyddsförordningen, anmälan av en personuppgiftsincident till tillsynsmyndigheten, anges

1. Vid en personuppgiftsincident ska den personuppgiftsansvarige utan onödigt dröjsmål och, om så är möjligt, inte senare än 72 timmar efter att ha fått vetskap om den, anmäla personuppgiftsincidenten till den tillsynsmyndighet som är behörig, såvida det inte är osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter. Om anmälan till tillsynsmyndigheten inte görs inom 72 timmar ska den åtföljas av en motivering till förseningen.
2. Personuppgiftsbiträdet ska underrätta den personuppgiftsansvarige utan onödigt dröjsmål efter att ha fått vetskap om en personuppgifts-incident.
3. Den anmälan som avses i punkt 1 ska åtminstone
a) beskriva personuppgiftsincidentens art, inbegripet, om så är möjligt, de kategorier av och det ungefärliga antalet registrerade som berörs samt de kategorier av och det ungefärliga antalet personuppgiftsposter som berörs,
b) förmedla namnet på och kontaktuppgifterna för dataskyddsombudet eller andra kontaktpunkter där mer information kan erhållas,
c) beskriva de sannolika konsekvenserna av personuppgiftsincidenten, och
d) beskriva de åtgärder som den personuppgiftsansvarige har vidtagit eller föreslagit för att åtgärda personuppgiftsincidenten, inbegripet, när så är lämpligt, åtgärder för att mildra dess potentiella negativa effekter.

[12] 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.

4. Om och i den utsträckning det inte är möjligt att tillhandahålla informationen samtidigt, får informationen tillhandahållas i omgångar utan onödigt ytterligare dröjsmål.
5. 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 denna artikel.

Om personuppgiftsincidenten sannolikt leder till en hög risk för fysiska personers rättigheter och friheter ska den personuppgifts-ansvarige dessutom utan onödigt dröjsmål informera den registrerade om incidenten.

Det är således vid implementering av integritetsskyddet viktigt att klargöra i vilken ansvarsroll kommunstyrelsen agerar när den fullgör uppgifter inom sitt ansvarsområde. När kommunstyrelsen tillhandahåller stadsövergripande system och stadsgemensam it-infrastruktur inträder kommunstyrelsen ofta i ansvarsrollen personuppgiftsbiträde och ska då skyndsamt ge övriga nämnder och bolag den information som föreskrivs i artikel 33 dataskydds-förordningen, se ovan.

Det finns idag en riktlinje och vägledningar[13] som behandlar personuppgiftsincidenter och skyldigheterna som uppkommer i de olika ansvarsrollerna avseende personuppgiftsincidenter. Enligt gällande dataskyddslagstiftning måste alla lämpliga tekniska skyddsåtgärder och organisatoriska åtgärder ha vidtagits för att kunna fastställa om en personuppgiftsincident har ägt rum. I detta ingår att ha förmåga att upptäcka, åtgärda, förebygga och rapportera personuppgiftsincidenter för att förhindra konsekvenser som exempelvis diskriminering, identitetsstöld, bedrägeri, förlorat anseende och ekonomisk förlust för individ. I riktlinje WP250 rev.01 anges även att ”För att hitta oriktigheter i databehandlingen kan den personuppgiftsansvarige eller personuppgiftsbiträdet använda vissa tekniska åtgärder som dataflödes- och logganalysinstrument. Med hjälp av dessa kan man definiera händelser och varningar genom att korrelera loggdata”[14].

[13] 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)
[14] Observera att loggdata kan klassificeras som personuppgifter och ska hanteras enligt gällande dataskyddslagstiftning.

4.6.1 Status för hantering av personuppgiftsincidenter och dataskyddsombudets råd

Under 2022 har stadsledningskontorets rutin för hantering av informationssäkerhetsincidenter uppdaterats av informationssäkerhetssamordnare. Personuppgiftsincidenthantering ingår i denna rutin. Rutinen finns publicerad på intranätet, Informationssäkerhet och dataskydd på stadsledningskontoret - Stockholms stads intranät.

Enligt gällande rutin är alla medarbetare ansvariga för att uppmärksamma, dokumentera och registrera informationssäkerhetsincidenter. När informationssäkerhetsincidenter upptäcks ska de alltid rapporteras i stadens verktyg för incidenthantering.

Det är viktigt att medarbetare på stadsledningskontoret tar del av upprättad rutin och utbildas i vad som utgör en personuppgiftsincident under 2023. När väl en incident sker är tidsramen kort för att avgöra om en personuppgiftsincident ska anmälas till Integritetsskyddsmyndigheten och om den berörde individen ska informeras.

Den korta tidsramen gör att redan innan en personuppgiftsincident uppkommer ska ansvarsrollerna internt mellan nämnder och bolag samt kommunstyrelsen vara klarlagda. Kommunstyrelsen kan både vara personuppgiftsansvarig och personuppgiftsbiträde vid en personuppgiftsincident. Kommunstyrelsen behöver iaktta skyldigheterna som ett personuppgiftsbiträde har att uppfylla. Personuppgiftsbiträdet ska underrätta internt personuppgiftsansvarig nämnd eller bolag, utan onödigt dröjsmål, efter att ha fått vetskap om en personuppgiftsincident och tillhandahålla i lag specificerad information till personuppgiftsansvarig nämnd och bolag för att ansvarig ska kunna uppfylla sina skyldigheter och utreda om anmälan till Integritetsskyddsmyndigheten behöver ges in och om berörd individ ska informeras om personuppgiftsincidenten.

För 2022 är ett mindre antal personuppgiftsincidenter dokumenterade i verktyget. Det är ett lågt antal mot bakgrund av kravet om att alla personuppgiftsincidenter ska dokumenteras. I sammanhanget kan även noteras att de personuppgiftsincidenter som har dokumenterats är incidenter där medarbetare aktivt tagit kontakt med dataskyddsombudet och där även bedömning gjorts om anmälningsskyldighet föreligger och individ behöver kontaktas. Det kan emellertid inte uteslutas att personuppgiftsincidenter kan ha dokumenterats på annat vis.

För att efterleva lagkravet om att alla personuppgiftsincidenter ska dokumenteras och att dokumentationen ska möjliggöra för Integritetsskyddsmyndigheten att kontrollera efterlevnaden har dataskyddshandläggare och informationssäkerhetssamordnare i samråd med dataskyddsombudet upprättat övergripande dokumentation över informationssäkerhetshändelser under 2022 som innefattar personuppgifter. Under 2023 ska även enligt uppgift en behovsinsamling ske gällande systemstöd för informations-säkerhetsarbetet, däri ingår systemstöd för personuppgiftsincidents-dokumentation. Dataskyddsombudets rådgivning gällande dataskyddslagkrav bör inhämtas i arbetet under 2023. Det planeras således för att skapa ett register över kommunstyrelsens personuppgiftsincidenter, som uppfyller gällande lagkrav och som dataskyddsombudet kan ta del av och granska.

För att efterleva dataskyddslagstiftningen krävs idag även att kommunstyrelsen har förmåga att upptäcka och identifiera personuppgiftsincidenter. Detta är särskilt viktigt eftersom kommunstyrelsen är objektägare till stadsövergripande system och tillhandahåller stadsgemensamma it-infrastrukturen Under 2022 har CERT, Computer Emergency Response Team etablerats. CERT avser förmågan att upptäcka, hantera och förebygga it-säkerhets-incidenter. Under 2023 är det viktigt att dataskyddsombudet får ge råd avseende dataskyddsregelverket i förhållande till arbetet med CERT för att främja kommunstyrelsen efterlevnad av att ha förmåga att upptäcka och identifiera personuppgiftsincidenter samt för att efterleva lagkraven utifrån ansvarsrollen personuppgifts-ansvarig och personuppgiftsbiträde.

I detta sammanhang kan det även informeras om att enligt dataskyddsförordningen är dataskyddsombudet Integritetsskydds-myndighetens kontaktpunkt i frågor som rör personuppgifts-behandling, likaså ska personuppgiftsansvarig och personuppgiftsbiträdet enligt dataskyddsförordningen säkerställa att dataskyddsombudet på ett korrekt sätt och i god tid deltar i alla frågor som rör skyddet av personuppgifter.

Någon personuppgiftsincident, där kommunstyrelsen är personuppgiftsansvarig har inte inrapporterats till Integritets-skyddsmyndigheten under 2022. Integritetsskyddsmyndigheten sammanställer varje år en rapport avseende anmälda personuppgiftsincidenter, se IMY Anmälda personuppgiftsincidenter 2021.

Slutligen kvarstår rekommendationerna från GDPR-årsrapport 2021. Framtagen informationssäkerhetsincidentrutin, där personuppgiftsincidenter ingår, måste testas och övas av verksamheten, då lagkrav uppställer kort tidsram för att efterleva regelverket.

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

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

Generellt behöver förmågan att hantera personuppgifter fortsatt utvecklas och det är av vikt att aktiviteter enligt ovan utförs i samråd med dataskyddsombudet.

Dataskyddsombudet kommer i början av 2023 slutföra en vägledning gällande dataskyddsförordningens regelverk avseende en personuppgiftsincident. Vägledningen kommer att publiceras på intranätssidan informationssäkerhet och dataskydd på stadsledningskontoret.

5 Risk och dataskydd

I GDPR-årsrapport 2021 behandlades risker inom dataskydd och att dataskyddsförordningen är uppbyggd utifrån risk och att dokumenterade riskanalyser ska utföras och att konsekvens-bedömning avseende dataskydd ska utföras vid hög risk.

Riskanalys avseende dataskydd ska utföras med individen i fokus, det vill säga den personuppgiftsansvarige ska bedöma om behandlingen kan äventyra den registrerades friheter och rättigheter, särskilt personuppgifter, och om personuppgiftsbehandlingen kan

orsaka den registrerade fysisk, materiell eller immateriell skada utifrån dataskyddsregelverket och gällande vägledningar från Europiska dataskyddsstyrelsen.

Under 2022 har en uppdaterad handbok för riskanalys och riskhantering vid SLK, inom området informationssäkerhet, inklusive dataskydd, tagits fram. Handbok och bilagor är publicerade på intranätet Informationsklassning, riskanalys och konsekvensbedömning - Stockholms stads intranät.

5.1 Dataskyddsombudets råd till kommunstyrelsen

Dataskyddsombudets råd från GDPR-årsrapport 2021 lyfts även i årets rapport. Kommunstyrelsen behöver säkerställa att det faktiska dataskyddsarbetet är definierat, känt bland medarbetare och proaktivt för att därefter säkerställa att processer, rutiner och instruktioner efterlevs, utvecklas och motsvarar gällande dataskyddslagstiftning. Kommunstyrelsens dataskyddsombud och stödfunktionerna såsom informationssäkerhetssamordnare och dataskyddshandläggare bistår utifrån sina roller i detta arbete.

Avsikten med dataskyddsombudets råd i GDPR-årsrapport är att öka mognadsgraden avseende dataskydd och att minska dataskyddsriskerna samt arbeta mot ett utvecklat och proaktivt integritetsskydd.

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

6 Genomförda granskningar

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

Dataskyddsombudet har under 2022 inte, tillsammans med verksamheten, utfört några riktade granskningar av verksamhetens dataskydd, utan i stället gett råd om dataskyddslagstiftning och fått delta rådgivande i pågående dataskyddsarbete, särskilt vid utförande av tredjelandsöverföringsbedömningar och informationsklassning. Medarbetare har även löpande ställt dataskyddsfrågor till dataskyddsombudet.

Att delta i pågående dataskyddsarbete ställer emellertid krav på ett dataskyddsombud, då ett dataskyddsombud enligt gällande lagstiftning inte ska utföra operativt dataskyddsarbete. Det operativa dataskyddsarbetet ska alltid omhändertas av verksamheten. Samtidigt är dataskyddslagstiftningen komplex och dataskyddsombudets råd bör inhämtas i inledningsskedet vid innovation, IoT, AI, automatiskt beslutsfattande och när integritetskänsliga och känsliga personuppgifter behandlas.

I och med upprättande av GDPR-årsrapport 2022 har dataskyddsombudet granskat styrdokumenten Stockholms stads kvalitetsprogram, riktlinje för informationssäkerhet i Stockholms stad, tillämpningsanvisning till stadens riktlinje för informationssäkerhet och mall lokal anvisning för informationssäkerhet. Ett uppdateringsarbete är planerat för 2023 avseende tillämpningsanvisningen.

Dataskyddsombudet har under arbetet med GDPR-årsrapport 2022 även granskat hur dataskyddsombudets råd i föregående rapport har hanterats samt upprättad registerförteckning. Informationssäkerhetssamordnare har bistått med information om informationsklassning.

Dataskyddsombudet välkomnar att verksamheten utifrån båda kommunstyrelsens ansvarsroller personuppgiftsansvarig och personuppgiftsbiträde inhämtar dataskyddsombudets rekommendationer löpande och möjliggör till riktad granskning tillsammans med verksamheten, utöver registerförteckning, styrdokument och informationsklassning under 2023.

7 Övrigt att rapportera

7.1 Tredjelandsöverföring

Stockholms stads stadsledningskontor har även under 2022 bedrivit ett omfattande arbete i samråd med dataskyddsombudet med

anledning av EU-domstolens dom, *Schrems II-domen*, meddelad den 16 juli 2020. Vid personuppgiftsöverföring till exempelvis USA ska förutom standardavtalsklausuler ytterligare tekniska och organisatoriska skyddsåtgärder implementeras, då USA:s lagstiftning inte kan anses tillförsäkra en i allt väsentligt likvärdig skyddsnivå för personuppgifterna som inom EU/EES.[15]

Under 2022 har juridiska avdelningen i samråd med dataskydds-ombudet tagit fram mall för tredjelandsöverföringsbedömning, Transfer Impact Assessment, och PM med vägledning vid användning av standardavtalsklausuler.

Dataskyddsombudet omvärldsbevakar löpande och följer vad som sker avseende ett framtida möjligt beslut om adekvat skyddsnivå från EU-kommission gällande USA under 2023.

7.2 Utbildning avseende dataskydd

I GDPR-årsrapport 2021 rapporterades om att Stockholms stad har som krav att samtliga genomgår en obligatorisk grundkurs i dataskydd och en informationssäkerhetsutbildning[16]. Svars-frekvensen avseende dessa obligatoriska utbildningar följs upp och redovisas.

7.3 Inhämtning av GDPR-årsrapport/er och riktade aktiviteter

För att implementera och anses värna integritetsskyddet är det viktigt att följa upp och genomföra dataskyddsaktiviteter utifrån dataskyddsombudets GDPR-årsrapport. Dataskyddsombudet bistår gärna vid framtagande av aktiviteter för kommunstyrelsens dataskyddsarbete.

---

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

[16] Utbildningarna finns på Stockholms stads utbildningsplattform, https://utbildning.stockholm.se/

Utifrån kommunstyrelsens ansvar för stadenövergripande informationssäkerhet är det dessutom angeläget att det sker en samlad analys av samtliga nämnders och bolags dataskyddsombuds GDPR-årsrapporter. Vid behov bör denna analys föranleda aktiviteter eller åtgärder för att stärka stadenövergripande informationssäkerhet och integritetsskydd.