Stadsrevisionen

Göteborgs Stad

STADSREVISIONENS DATASKYDDSARBETE 2023

Dataskyddsombudets rapport

Innehållsförteckning

Inledning

EU:s dataskyddsförordning (i det följande DSF) trädde i kraft 2018-05-25. Undertecknad utsågs 2018-05-15 av revisorskollegiet att från och med 2018-05-25 vara dataskyddsombud (DSO) för stadsrevisionen i Göteborg. Jag har sedan dess haft detta uppdrag.

Denna skriftliga rapport är den fjärde i ordningen jag avlämnar avseende stadsrevisionens dataskyddsarbete och omfattar 2023. I vissa fall har jag valt att även redovisa vissa iakttagelser från inledningen av 2024 med direkt koppling till 2023 års verksamhet.

2023 års rapport har disponerats enligt följande.

Efter denna inledning följer:

1. En översiktlig genomgång av väsentliga händelser inom dataskyddsområdet under 2023. Genomgången innefattar iakttagelser och rekommendationer från ett urval av Integritetsmyndighetens centrala publikationer runt integritets- och dataskyddsfrågor.

2. Några kommentarer runt integritetsmyndighetens tillsynsarbete under 2023.

3. En beskrivning av stadsrevisionens arbete med informationssäkerhet och dataskydd under 2023.

4. En sammanfattande kommentar och bedömning av stadsrevisionens arbete inklusive rekommendationer för det fortsatta arbetet.

Göteborg den 1 mars 2023

Anders Landkvist

1. Väsentliga händelser inom dataskydd 2023

Utvecklingen inom dataskyddsområdet har fortsatt under 2023. De aktörer som formar den normerande synen på hur regelverket ska tolkas och hanteras är liksom tidigare EU-domstolen, nationella domstolar, nationella tillsynsmyndigheter och organisationen European Data Protection Board (nedan EDPB).[1]

I Sverige är Integritetsskyddsmyndigheten[2] (nedan IMY) tillsynsmyndighet som också har en vägledande roll i sitt uppdrag. Myndighetens uttalanden, rekommendationer och råd får därmed en viss indirekt normerande verkan.

Jag kommer nedan att översiktligt redovisa vilka iakttagelser jag gjort efter att ha gått igenom domar, riktlinjer, rapporter, och rekommendationer med mera som dessa aktörer publicerat under 2023.

Jag kommer slutligen också att kortfattat kommentera pågående och kommande utveckling inom EU runt reglering av datahantering och digitala tjänster.

Domar från EU-domstolen

En genomgång av domar från EU-domstolen som redovisats i nyhetsflödet runt dataskydd visar att uttolkningen av regelverket runt integritetsskydd fortsätter. Några stora och omtalade principiella mål, med generell påverkan på de personuppgiftsansvariga, har dock inte hanterats under året.

När det gäller tillsyn och tillsynsmyndigheterna har emellertid en viktig dom avkunnats i december 2023. Domen konstaterar att där gäller mer långtgående krav på myndigheternas utredningsskyldighet av klagomål på personuppgiftsbehandlingar än vad som tidigare antagits. I sak innebär det att myndigheternas arbete att utreda och sannolikt också att utföra

[1] EDPB är ett samverkansorgan för de nationella tillsynsmyndigheterna för integritetsskydd inom EU, viss normerande verkan har också de ställningstaganden som görs av Dataskyddsombudsmannen (EDPS) som utövar tillsyn över EU:s institutioner.
[2] IMY hette tidigare Datainspektionen.

tillsyn med anledning av utredda klagomål kommer att öka i medlemsstaterna.[3]

Nytt adekvansbeslut beträffande tredjelandsöverföring av personuppgifter till Förenta staterna.

Som redogjorts för i tidigare upprättade DSO-rapporter har EU-kommissionens tidigare adekvansbeslut beträffande överföring av personuppgifter (”Safe Harbour” och ”Privacy Shield”) prövats och underkänts av EU-domstolen. Detta skedde via de så kallade ”Schremsmålen[4].”

Utvecklingen därefter har inneburit att såväl kommissionen som Förenta staterna arbetat för att finna lösningar som kan leda fram till ett nytt adekvansbeslut. Ett sådant har också fattats den 10 juli 2023. Beslutet gäller inte generellt för alla typer av överföringar av personuppgifter till USA utan är begränsat till att gälla överföringar som sker till organisationer etablerade där och som omfattas av det nya ramverket ”EU-US data privacy framework.”[5]

Ramverket är en mekanism för självcertifiering där de organisationer som vill delta får genomgå en särskild process för att godkännas. Certifieringen gäller för ett år i taget och kan därefter förnyas via ytterligare en process.

Det är dock inte självklart att adekvansbeslutet kommer att fortsätta gälla om EU-domstolen prövar det. Det finns tydliga signaler att det kommer att utmanas i framtiden. Organisationen NOYB (NOt Your Business) som

---

[3] EU-domstolens dom den 7 december i förenade målen C-26/22 och C-64/22, UF och AB mot Land Hessen och Schufa Holding AB

[4] I dessa mål (”Schrems I” respektive ”Schrems II”) underkändes EU-kommissionens beslut att godkänna de avtal som upprättats mellan EU och Förenta staterna för överföring av personuppgifter. Följden av detta blev stora praktiska svårigheter för personuppgiftsansvariga inom EU att använda sig av många IT-system och applikationer som ägdes/kontrollerades av amerikanska företag utan att också riskera att bryta mot DSF. Exempel på vanligt förekommande IT-system som träffades av sådan tredjelandsproblematik var applikationer inom Microsoft Office 365 och Facebook.

[5] Microsoft Corporation är certifierade under det nya ramverket vilket innebär att tredjelandsproblematiken för de IT-system man tillhandahåller i dagsläget är godkända att göra enligt gällande villkor för adekvansbeslutet.

driver flera integritetsrättsliga frågor internationellt har aviserat att man avser att få det nya adekvansbeslutet prövat. Samma organisation initierade de tidigare ”Schremsmålen” enligt ovan.[6]

Domar från svenska domstolar

Domar från svenska domstolar som också redovisats i nyhetsflödet runt dataskydd och som uppmärksammats i olika dataskyddssammanhang gäller IMY:s roll och mandat. Här finns det flera mål där personuppgifts-ansvariga begärt att IMY:s beslut om sanktionsavgifter ska prövas av domstol. Utfallen i dessa mål har skiftat.

Där finns också mål där en person som framställt klagomål till IMY som myndigheten beslutat att inte utreda valt att överklaga *detta* beslut. Vidare finns ett mål där IMY:s beslut att avsluta ett tillsynsärende som inletts till följd av klagomål utan åtgärd överklagats av den klagande.

I de båda målen hade underrätterna bedömt att IMY:s beslut inte var överklagbara av de klagande. HFD gjorde dock motsatt bedömning och återförvisade målen för ny prövning av lägre instans.

Detta har en viktig principiell betydelse i att det innebär att den som lämnar in ett klagomål till IMY ska anses få en partsställning i förhållande till myndigheten i det ärende som inleds i och med det inkomna klagomålet.

Partsställningen aktualiserar då förvaltningslagens regelverk beträffande:

- Kommunicering
  - Rätt att ta del av och möjlighet att yttra sig över allt material som är av betydelse i ärendet innan myndigheten att ta beslut i det.
- Partsinsyn.
  - Rätt att ta del av allt material som tillförts ärendet.

Den klagandes ställning stärks därför väsentligt i förhållande till IMY i och med domarna.[7] Det ökar i sin tur kraven på hur IMY:s rutiner och arbetssätt för hantering av klagomål måste utformas.

---

[6] Se: NOYB enforces your right to privacy everyday och European Commission gives EU-US data transfers third round at CJEU (noyb.eu)
[7] Jfr HFD mål nr 6193-22 respektive 3691-22.

Detta, tillsammans med EU-domstolens dom, som beskrivits under punkten avseende EU-domstolen ovan beträffande utökade krav på tillsynsmyndigheternas utredningsskyldighet av klagomål – kommer att påverka IMY:s arbete framåt. Myndigheten konstaterar själv att:

”Besluten påverkar myndighetens arbete med klagomål på ett genomgripande sätt och kräver mer resurser. Det innebär att vi måste prioritera ner bland annat delar av vårt vägledningsarbete, arbetet med riskbaserad tillsyn samt vår möjlighet att delta i utrednings- och lagstiftningsarbete. Det innebär också längre handläggningstider och högre balanser för andra obligatoriska uppgifter, till exempel tillstånds-ansökningar.”[8]

Riktlinjer och rekommendationer med mera från EDPB

Som beskrivits ovan består EDPB av de nationella tillsynsmyndigheterna för dataskydd i EU:s medlemsstater. Organisationen fungerar som ett samverkansorgan för gemensam uttolkning av regelverket för dataskydd inom EU.[9]

EDPB publicerar framför allt riktlinjer och rekommendationer till hjälp för de personuppgiftsansvariga i deras arbete att anpassa sina person-uppgiftsbehandlingar till de krav regelverket ställer.

Riktlinjerna är rådgivande och är därför inte direkt normerande på samma sätt som förordningstext eller EU-domstolens uttolkning av regelverket. De utgör ändå betydelsefulla hjälpmedel för enskilda personuppgifts-ansvariga för att förstå hur tillsynsmyndigheterna ser på olika aspekter på dataskydd. EDPB har publicerat sammanlagt 12 riktlinjer och 1 rekommendation under 2023.

Under 2023 har EDPB även genomfört en samordnad undersökning runt dataskyddsombuden roll och ställning i medlemsstaterna. IMY har deltagit i undersökningen och de nationella iakttagelserna om för-hållandena i Sverige kommenteras separat under avsnittet som beskriver IMY:s publikationer nedan.

EDPB publicerade sin sammanhållna rapport över förhållandena i de 25 medlemsstaterna och konstaterade i detta att:

[8] IMY Årsredovisning 2023 s. 29
[9] https://edpb.europa.eu/edpb_sv

- Majoriteten av de tillfrågade verksamheterna anser att dataskydds-ombuden har nödvändiga färdigheter och kunskaper för att utföra sitt arbete och får regelbunden utbildning i dataskyddsfrågor,
- att de har tydligt definierade uppgifter och
- att de inte får påtryckningar om hur de ska utöva sina uppgifter.
- Dessutom anger verksamheterna

- att ombuden rådfrågas i de flesta fall och förses med tillräcklig information för att fullgöra sina uppgifter,
- att deras åsikter och rekommendationer följs och att ombuden har tillräckliga resurser för att utföra sitt jobb.
- Att det dock fortfarande finns för många dataskyddsskyddsombud som inte är i en sådan position.

EDPB lämnar också flera rekommendationer till de personuppgifts-ansvariga för att säkerställa att dataskyddsombuden har ändamålsenliga och tillräckliga förutsättningar för att fullgöra sina uppdrag.

Rekommendationerna är generella och gäller exempelvis betydelsen av

- att avsätta tillräckliga resurser för dataskyddsombuden arbete,
- att säkerställa att dataskyddsombuden har tillräcklig kunskap för sitt arbete,
- att risk för intressekonflikter i uppdraget hanteras och
- att deras rapportering sker till organisationens högsta ledning.

EDPB driver också ett arbete med att ta fram en riktlinje, som fått viss uppmärksamhet, kring användning av barns personuppgifter och en vägledning riktad mot spelplattformar som behandlar barns person-uppgifter. Vägledningen förväntas bli klar under 2024.

Rapporter med mera från IMY

IMY är en statlig myndighet som inom ramen för sitt uppdrag arbetar för att skydda personuppgifter så att uppgifterna hanteras korrekt. IMY är som nämnts ovan också nationell tillsynsmyndighet i fråga om regel-verket för integritetsskydd i Sverige deras huvuduppgifter är att;

- granska och verkställa tillämpningen av dataskyddsreglerna,
- ge vägledning och stöd till myndigheter, företag och organisationer samt till allmänheten,
- bidra till en enhetlig tillämpning av dataskyddsreglerna inom EU,
- utfärda tillstånd och genomföra tillsyn avseende kamerabevakning och kreditupplysning och att
- följa och rapportera om utvecklingen inom integritetsområdet.

IMY har vuxit storleksmässigt under senare år och fortsätter att växa för att kunna hantera ett uppdrag vars komplexitet också växer i takt med ökad digitalisering i samhället. Ett allmänt ökat riskmedvetande runt dataskydd, informations- och cybersäkerhet innebär också att trycket på myndigheten för vägledning ökar. Detta avspeglas också i den tilldelning av resurser som görs, IMY fick från 2023 en förstärkning av sitt anslag med närmare 40 procent jämfört med tidigare.

Fokuseringsfrågor 2023

Vid sidan av de förtecknade huvuduppgifterna ovan arbetar IMY med fokuseringsfrågor via uppdrag eller särskilda satsningar. Exempel på detta är att IMY som tillsyns- och expertmyndighet i integritetsfrågor under 2023 varit engagerad i det arbete regeringen och samhället drivit och driver mot organiserad brottslighet. Utredning av lämpliga åtgärder för utökad kontroll av olika slag i syfte att beivra brott innebär alltid en avvägning runt risker ur integritetssynpunkt. Här har IMY en viktig uppgift att fylla så att en balanserad avvägning kan göras i exempelvis beredningen av olika lagförslag.

Ett annat viktigt exempel är kopplat till tillämpningen av artificiell intelligens (AI). 2023 har varit det år då AI blivit känt för den breda allmänheten. AI och innovation hänger nära ihop eftersom AI skapar tekniska möjligheter som inte funnits tidigare. Sådana möjligheter kan också innebära integritetsrisker av olika slag. IMY har varit tidigt ute för att arbeta fram verktyg för vägledning inom innovationsområdet. Hittills har två projekt kopplade till sådana verktyg genomförts; ett avseende federerad maskininlärning[10] i vården via AI och ett avseende sensorer som alternativ till kamerabevakning i det offentliga rummet.

Strategisk inriktning framåt

IMY arbetar utifrån en strategisk inriktning med målbilden att personlig integritet och dataskydd år 2025 har ett tydligt fokus på alla nivåer i samhället. Myndighetens målbild innefattar att år 2025 ska:

[10] Federerad maskininlärning är inlärningsalgoritmer som drar nytta av data distribuerad över flera (lokala) klienter. Inlärningen sker huvudsakligen lokalt på klienterna men med hjälp av en central server kan klienterna samarbeta och nå bättre resultat. Det ger både möjlighet att skydda integriteten hos data och att använda distribuerad beräkningskapacitet.

- Enskilda individer ha god kunskap om sina rättigheter.
- Privata och offentliga verksamheter arbeta mer systematiskt med dataskydd och driva en integritetsvänlig digitalisering.
- Innovation och utveckling av teknik och tjänster ske på ett sätt som värnar den personliga integriteten.
- Sverige ha en tydlig integritetsskyddspolitik som bidrar till en hållbar digitalisering.
- IMY fortsatt vara en attraktiv arbetsgivare.

Publikationer 2023

Bland IMY:s publikationer för 2023 märks (liksom tidigare år) ett antal informativa rapporter. Rapporterna innehåller iakttagelser myndigheten gjort i fråga om brister, liksom identifierade utvecklingsområden vid tillämpning av reglerna för dataskydd.

Under 2023 har 3 rapporter publicerats:

- Dataskyddsarbetet i praktiken[11]
- Anmälda personuppgiftsincidenter 2022[12]
- Vägledning vid kamerabevakning[13]

Av dessa kommer de två första i uppställningen att kommenteras vidare nedan.

Dataskyddsarbetet i praktiken

Rapporten är IMY:s nationella redovisning av ”sin del” av EDPB samordnande undersökning av dataskyddsombudens roll och ställning i medlemsstaterna som beskrivits ovan. IMY:s undersökning baseras på en webbenkät som skickats till registrerade dataskyddsombud i landet. Svarsfrekvensen har varit relativt låg, varför IMY konstaterar att slutsatser behöver dras med viss försiktighet.[14]

Från denna utgångspunkt gör myndigheten ändå följande iakttagelser:

[11] IMY rapport 2023:1
[12] IMY rapport 2023:2
[13] IMY rapport 2023:3
[14] Undersökningen baseras på 800 svar, vilket motsvarar svar från drygt 2 av 10 tillfrågade verksamheter.

- Att det praktiska dataskyddsarbetet i stora delar bedrivs av landets alla dataskyddsombud. För att klara av sitt uppdrag behöver de tillräckligt med tid, något som många ändå saknar enligt undersökningen.

- Att det är oroande att bara mindre än hälften av dataskyddsombuden anser att den egna organisationen arbetar kontinuerligt och systematiskt med dataskyddsfrågor.

- Att det är viktigt att dataskyddsombudet får både tillräckliga och rätt resurser för att kunna utföra sina uppgifter inom organisationen. Till exempel måste dataskyddsombudet ha tillräckligt med tid för uppgifterna och få tillgång till den information som behövs.

- Att dataskyddsombudet också måste kunna upprätthålla sin sakkunskap, till exempel genom kompetensutveckling.

- Att det för att få till stånd ett systematiskt och kontinuerligt arbete med integritets- och dataskyddsfrågor är avgörande att det både finns kunskap om dataskyddsförordningen och engagemang för frågor som rör integritet och dataskydd hos organisationens ledning.

- Att det därför är oroande att mindre än hälften av de svarande anser att den egna organisationen arbetar kontinuerligt och systematiskt med dataskyddsfrågor.

IMY menar också att det framstår som att de största utmaningarna för det praktiska dataskyddsarbetet idag är;

1) att få till fungerande rutiner och processer respektive,
2) att få dataskyddsreglerna att inte hindra eller försvåra verksamheten.

Allt fler dataskyddsombud verkar också uppleva att ett av de största problemen kopplat till det praktiska dataskyddsarbetet är bristande engagemang och låg kunskap hos ledningen. Själva uttolkningen av regelverket verkar däremot nu (jämfört med tidigare undersökningar) vara ett mindre problem.

IMY har även beslutat att inleda tillsyn mot ett antal offentliga och privata personuppgiftsansvariga för att fördjupa sin kunskap runt hur förutsättningarna för dataskyddsombuden ser ut i Sverige. Detta beskrivs närmare under avsnitt 2 (Integritetsmyndighetens tillsynsarbete 2023) nedan.

Anmälda personuppgiftsincidenter 2022

Denna rapport beskriver liksom tidigare år vilka mönster som kan urskiljas för personuppgiftsincidenter som anmälts till IMY under närmast föregående år.

Under 2022 togs cirka 5 330 anmälningar om personuppgiftsincidenter emot av IMY, varav 70 procent kom från offentlig sektor. 63 procent av dessa anmälning kunde tillskrivas någon typ av obehörigt röjande: antingen genom felskick, 38 procent, eller genom annan felaktig hantering av personuppgifter, 25 procent.

Den mänskliga faktorn angavs som orsak i 59 procent av samtliga anmälningar om personuppgiftsincidenter 2022.

Oftast handlade det då om personer som begått misstag när de hanterat personuppgifter i sina verksamheter. Över än hälften av de personuppgiftsincidenter som orsakats av den mänskliga faktorn var felskickade brev, mejl eller sms. Andelen anmälningar med den mänskliga faktorn som orsak inom hälso- och sjukvården har också ökat jämfört med föregående år.

IMY konstaterar, med stöd av en jämförelse mellan anmälningsfrekvens i de nordiska länderna relaterat till folkmängd, att det sannolikt finns många personuppgiftsincidenter som inte anmäls i Sverige. Denna kan då handla om i storleksordningen 10 000 oanmälda personuppgiftsincidenter i vårt land.

I rapporten lämnar myndigheten följande rekommendationer för hur en verksamhet ska resonera och agera för att kunna förebygga personuppgiftsincidenter – de återges här i oredigerat skick.[15]

- Ett systematiskt informationssäkerhetsarbete är centralt.

  Att den mänskliga faktorn anges frekvent som orsak till personuppgiftsincidenter och att den kan leda till allvarliga incidenter innebär att det är en viktig faktor att beakta i er verksamhets systematiska informationssäkerhetsarbete. De

[15] Se vidare IMY rapport 2023:2 s.7

organisatoriska och tekniska säkerhetsåtgärderna behöver vara integrerade i verksamhetens arbetssätt och skapa förutsättningar för att det ska vara lätt att göra rätt och svårt att göra fel.

- Verksamhetens säkerhetsnivå i relation till riskerna för enskildas friheter och rättigheter.

  Säkerhetsnivån ska sättas i relation till vilka personuppgifter som behandlas och de specifika risker för enskildas friheter och rättigheter som föreligger i er verksamhet. Verksamheten kan därför inte rakt av kopiera andras säkerhetsåtgärder och säkerhetsarbetet måste pågå kontinuerligt då verksamheten, tekniken och därmed riskerna hela tiden förändras.

- Minska risken för misstag

  Ni kan minska risken att medarbetare begår misstag genom organisatoriska och tekniska åtgärder. Exempel på det är att tekniskt förhindra att medarbetare sparar information på löstagbara medier eller att förhindra dem att installera program och appar som inte godkänts av verksamheten. Lösningar som gör det enkelt för medarbetarna att lösenordskydda och kryptera e-post och bifogade fler är också åtgärder som kan höja säkerheten.

- Aktiv behörighetsstyrning

  En annan viktig och grundläggande säkerhetsåtgärd är att ha en aktiv behörighetsstyrning. Behörigheterna ska vid varje tid vara anpassade så att varje medarbetare bara får tillgång till de personuppgifter som medarbetaren behöver för att kunna utföra sina arbetsuppgifter.

- Processer som stärker det systematiska informations-säkerhetsarbetet

  Alla verksamheter som hanterar personuppgifter behöver ha dokumenterade och implementerade riskhanterings- och personuppgiftsincidenthanteringsprocesser för att kunna förebygga, upptäcka och hantera personuppgiftsincidenter. Processerna ska också leda till ett kontinuerligt lärande.

- Säkerhetskultur

> För att få en god säkerhetskultur krävs att ledningen är engagerad i verksamhetens säkerhetsfrågor, vilket även inkluderar skyddet för personuppgifter. I en god säkerhetskultur kommuniceras även dragna lärdomar av inträffade incidenter, och hur dessa lärdomar sedan ska realiseras för att skapa en ännu bättre säkerhetskultur och därmed bidra till det systematiska säkerhetsarbetet.

För egen del kan jag konstatera att dessa rekommendationer är generellt giltiga och därför definitivt bör beaktas av alla personuppgiftsansvariga för att begränsa riskerna för att personuppgiftsincidenter inträffar.

Utblick om integritetsskydd och utveckling inom EU

IMY konstaterar att personlig integritet och dataskydd påverkas i hög grad av långsiktiga och omvälvande förändringar i vår omvärld. Exempel på detta är den genomgripande digitaliseringen av samhället och den mycket snabba teknikutvecklingen. I detta ser myndigheten flera trender framåt som har direkt inverkan på frågor runt integritetsskydd. Dessa trender är:

- Att utvecklingen av AI går i mycket hög fart. Under senare tid har de stora språkmodellernas[16] genombrott gjort det mer tydligt för den breda allmänheten vilken potential AI har, och hur den kan förändra till exempel hur vi arbetar och söker information. Användningen av AI kommer utgöra en större del av digitaliseringen de kommande åren, inom alla samhällets sektorer.

- Att data fortsatt är en viktig resurs, både för företag och offentlig sektor. Data behövs som ”råvara” i AI-baserade processer och är därmed nödvändig för den effektivisering som sådana processer kan leda till. Förmågan att hantera och omvandla data till nytta blir viktigare. Arbete med att lösa frågan om mer hantering av data med hög kvalitet pågår både inom forskning och näringsliv.

[16] En språkmodell är en sannolikhetsfördelning för sekvenser av ord. Språkmodeller används i samband med AI för att datorers kommunikation ska efterlikna hur mänskligt språk, exempelvis mänskliga samtal, är uppbyggda.

- Att många menar att behovet av systemsäkerhet kan tillgodoses genom identifiering med hjälp av olika biometriska[17] identifieringslösningar. Ett överanvändande av biometriska uppgifter är dock riskfyllt. Ett lösenord som kommit i orätta händer går att byta ut, men om någon obehörig får tillgång till ett fingeravtryck eller ansiktsbiometri går inte detta att ersätta med ett annat.

- Att virtuella världar[18] betraktas som framtidens internet. Genom virtuella världar kommer vår upplevelse av internet att förändras. Vissa gör bedömningen att inverkan är lika stor som när internet slog igenom. Genom virtuella världar möjliggörs en massiv insamling av data om individer, framför allt av olika biometriska data eller andra uppgifter om hälsa.

- Att den nya generationens mobilnät 5G byggs ut. Med 5G ökar möjligheten till snabbare och säkrare fjärrstyrning av enheter. 5G anses vara en förutsättning för fullt uppkopplade städer och hem.

- Att användningen av blockkedjeteknik[19] har ökat i fler sektorer än den finansiella och flera regeringsuppdrag pågår på området. Kryptovalutors sammankoppling med det traditionella finansiella systemet ökar.

Myndigheten konstaterar också att omvärldsläget 2023 i övrigt har karaktäriserats av flera säkerhetsutmaningar;

- det säkerhetspolitiska läget med hybridkrigsföring,

- den höga terrorhotsnivån mot svenska mål samt

- omläggningen av den svenska kriminalpolitiken för att möta den inhemska organiserade brottsligheten och stävja skjutvapenvåldet.

---

[17] Termen biometri används för de tekniker som finns tillgängliga för att mäta delar av kroppen elektroniskt och därigenom kunna identifiera personer.
[18] Virtuella världar kan beskrivas som datorburna funktioner där människor agerar och interagerar.
[19] Blockkedjeteknik är den tekniska grunden för användning av kryptovalutor såsom BitCoin och liknande.

IMY fastslår slutligen (än en gång) också att det finns en nära koppling mellan dataskydd och informationssäkerhet. Krav på tekniska och organisatoriska säkerhetsåtgärder kan tillsammans verka för att stärka robusthet och motståndskraft i samhället.[20]

Beträffande utvecklingen inom EU konstaterades redan i föregående års DSO-rapport att EU driver ett mycket omfattande och ambitiöst utvecklingsarbete inom det digitala området. Man talar om att 2020-talet är EU:s digitala årtionde. Ett led i det digitala årtiondet är att ta fram nya rättsakter som ger förutsättningar för den digitala omställningen samtidigt som de säkerställer mänskliga rättigheter, demokrati och rättsstatens principer. En följd av detta är att ett nytt rättsligt landskap kommer att växa fram. Dataskyddsförordningen är ett av grundfundamenten för detta. Två andra EU-förordningar som - då de införs - bedöms få stor påverkan på integritetsskyddet i samhället är AI-förordningen respektive förordningen om det europeiska hälsodataområdet (EHDS).

AI förordningen planeras beslutas under våren 2024 och då börja gälla två år senare. EHDS bedöms kunna beslutas under 2024. Implementeringstiden för denna kan dock komma att bli längre än för AI-förordningen.[21]

Det finns ytterligare pågående och beslutade initiativ, EU-förordningar och EU-direktiv om digitalisering med påverkan på dataskyddsområdet. Exempel på sådana är:

- Cyberresiliensakten
- CSAM-förordningen
- Akter om interoperabilitet
- NIS 2
- Cybersäkerhetsakten
- Förordning om digitala tjänster (DSA)
- Dataförvaltningsförordningen (DGA)
- eIDAS 2,
- Data Act, dataakten

Sammantaget påverkar både trender, utmaningar, omvärldshot och pågående och kommande regulatoriska förändringar svenska myndigheter och dess verksamheter. Det är därför viktigt för alla

[20] Jfr IMY Årsredovisning 2023 s. 8 f.
[21] A.a. s. 9 f.

myndigheter att ha ett strategiskt perspektiv på informations-, cyber-säkerhet och dataskydd. Det är därför också lika viktigt att säkerställa att det finns tillräckliga avsatta resurser till att arbeta med denna typ av frågor.

Sammanfattning av avsnittet:

- EU-domstolen har inte avgjort några större principiellt och generellt viktiga dataskyddsmål under 2023. En dom avseende kraven på tillsynsmyndigheternas utredningsskyldighet med stor praktisk betydelse har dock avkunnats under året. Domen påverkar hur tillsynsmyndigheterna behöver arbeta med klagomål.

- EU-kommissionen nya adekvansbeslut avseende Förenta staterna som tagits 2023 kan antas bli föremål för prövning i EU-domstolen i framtiden.

- Dataskyddsmål av visst intresse i svenska nationella domstolar har handlat om överklaganden av IMY:s beslut och klargörande av klagandes partsställning i förhållande till myndigheten. Detta kommer att påverka IMY:s arbete framåt.

- EDPB har publicerat 12 riktlinjer och 1 rekommendation under 2023. Man har en även genomfört en samordnad undersökning i medlemsstaterna runt dataskyddsombudens roll och ställning.

- IMY har publicerat flera rapporter under 2023. Av särskilt intresse är IMY:s iakttagelser i rapporten om de svenska dataskyddsombudens arbete och rapporten om anmälda personuppgiftsincidenter 2022. De rekommendationer som lämnas i den senare, om hur personuppgiftsansvariga ska tänka och agera för att begränsa risk för personuppgiftsincidenter, bedöms kunna fungera väl som vägledning för alla personuppgiftsansvariga.

- Den tekniska utvecklingen runt digitalisering innebär ett fortgående högt förändringstryck för både organisationer och enskilda där det är viktigt att skyddet för den personliga integriteten upprätthålls. Ett förändrat säkerhetsläge innebär också utmaningar kopplat till olika hotbilder mot det digitaliserade samhället.

- EU driver ett omfattande och ambitiöst arbete för ”det digitala årtiondet 2020”. Detta, tillsammans med det höga förändringstrycket och de olika omvärldshoten som finns, innebär att kraven ökar på svenska myndigheter att ha ett strategiskt förhållningssätt och att avsätta tillräckliga resurser för arbete med informations- , cybersäkerhet och dataskydd.

2. Integritetsskyddsmyndighetens tillsynsarbete

IMY:s tillsynsuppdrag gäller alla som omfattas av regelverket för integritetsskydd. Detta innebär att såväl privata som offentliga personuppgiftsansvariga kan granskas inom ramen för tillsynen. Från och med 2021 är tillsynen i huvudsak klagomålsbaserad. Tidigare var den främst riskbaserad.

Antal inkomna klagomål 2023 var 3 200, vilket är en ökning med närmare 50 procent jämfört med tidigare.[22] Myndigheten redovisar för 2023 en handläggningstid inom 3 månader för 60 procent av klagomålsärendena ,att jämföra med 83 procent och 79 procent för 2022 respektive 2021.

Handläggningstiderna har därmed alltså ökat för 2023, vilket rimligen hänger samman med den volymökning av klagomål som också kan konstateras. Det framstår inte som osannolikt att handläggningstiderna för klagomål kan komma att öka ytterligare under kommande år mot bakgrund av det förändrade/förtydligade rättsläget i fråga om tillsynsmyndigheters utredningsskyldighet (inom EU) och specifikt för IMY p g a de svenska domarna rörande klagandes ställning som part i förhållande till myndigheten.[23]

Klagomål kan leda till att tillsyn inleds och trenden är att antal tillsynsärenden har ökat kraftigt 2023.

År	Antal inledda tillsynsärenden
2020	47
2021	101
2022	120
2023	207

[22] Fakta- och volymuppgifter runt IMY:s tillsynsverksamhet har huvudsakligen hämtats från IMY Årsredovisning 2023.
[23] Se s. 9 ovan.

Tillsynen är nationell och även gränsöverskridande. Den gränsöverskridande tillsynen aktualiseras när ärenden berör verksamheter eller individer i flera EU/EES-länder. Gränsöverskridande tillsyn innebär en mer omständlig process än den nationella tillsynen då den bland annat innefattar kommunikation och samråd med andra berörda nationella tillsynsmyndigheter i och runt ärendet.

Vid allvarliga brister kan administrativa sanktionsavgifter påföras den personuppgiftsansvarige. Dessa kan uppgå till 20 miljoner euro eller 4 procent av ett företags/företagskoncerns årsomsättning, beroende på vilket värde som är högst. För offentliga verksamheter är den maximala sanktionsavgiften 10 miljoner kronor. Storleken på sanktionsavgiften är kopplad till hur allvarliga de brister som konstaterats bedöms vara. Nivån på sanktionsavgifter har varierat inom EU, vilket föranlett EDPB att ta fram riktlinjer för hur sanktionsavgifter bör beräknas. IMY har sedan införandet av DSF legat på förhållandevis återhållsamma nivåer i fråga om sanktionsavgifter.

Under 2023 har 11 tillsynsärenden lett till sanktionsavgifter om totalt 120 000 000 kronor, att jämföra med 5 tillsynsärenden och sanktionsavgifter om 9 720 000 kronor för 2022.

Ett urval av 2023 års tillsynsärenden beskrivs kortfattat nedan:

Personuppgifts-ansvarig	Brister	Sanktionsavgift
Spotify	IMY fann att den information som bolaget lämnat till enskilda om hur deras personuppgifter behandlas inte varit tillräckligt tydlig.	58 000 000 kronor.
Trygg-Hansa	IMY konstaterade att Trygg-Hansa har haft säkerhetsbrister som medfört att ett stort antal kunduppgifter var åtkomliga på internet.	35 000 000 kronor.
Bonnier	IMY fann att företaget hade profilerat sina kunder och webbesökare utan deras samtycke.	13 000 000 kronor

Tele 2 och CDON	IMY beslutade om sanktionsavgifter på 12 000 000 kronor respektive 300 000 kronor för att företagen hade fört över personuppgifter till USA via analysverktyget Google Analytics.	12 000 000 kronor respektive 300 000 kronor
Utbildningsnämnden i Stockholms Stad	IMY beslutade om en sanktionsavgift eftersom kamerabevakningen på Aspuddens skola varit för omfattande.	800 000 kronor
Barn- och utbildningsnämnden i Östersund*	IMY beslutade om en sanktionsavgift för att nämnden infört den digitala skolplattformen Google Workspace utan konsekvensbedömning	300 000 kronor
Region Skåne*	IMY beslutade om en sanktionsavgift för bristande säkerhet efter att regionen har lagrat känsliga personuppgifter på ett okrypterat USB−minne som sedan tappats bort	200 000 kronor

*) Kommenteras vidare nedan.

Merparten av de beslut IMY fattar som innefattar sanktionsavgifter överklagas, men även andra ärenden överklagas i viss utsträckning. Exempel på sådana andra ärenden är då IMY fattar beslut att inte inleda tillsyn.

Särskilt om tillsyn i kommun- och regionsektorn 2023

Liksom tidigare år bedömer jag att det finns ett värde i att följa och även kommentera delar av den tillsyn som sker i kommunsektorn, då det ger viss ledning i hur IMY ser på tillämpningen av regelverket i kommun-/regionsektorn och kanske även hur strängt man bedömer konstaterade

brister i enskilda ärenden. Jag kommer därför att återge ett antal sådana ärenden nedan.

Barn- och utbildningsnämnden, Östersunds kommun[24] (Beslut)

I ärendet konstaterades att IT-systemet (skolplattformen) Google Workspace for Education sedan hösten 2020 hade använts i 24 kommunala skolor i Östersund. Närmare 6 000 elevers och 1 300 anställdas personuppgifter hade behandlats i skolplattformen.

IMY konstaterade att en personuppgiftsansvarig, innan en sådan omfattande behandling av barns personuppgifter i skolverksamhet införts, behövt göra en konsekvensbedömning för att identifiera risker och behov av skyddsåtgärder. Detta har inte skett. På grund av det utfärdade IMY en administrativ sanktionsavgift på 300 000 kronor för överträdelse av dataskyddsförordningen.

Dataskyddsombudens roll och ställning[25] (Pågår)

Som beskrivits i föregående avsnitt har EDPB genomfört en samordnad åtgärd som gällde dataskyddsombudens roll och ställning. IMY genomför inom ramen för denna åtgärd också tillsyn för sammanlagt 44 verksamheter inom både privat och offentlig sektor. Flera kommunala verksamheter omfattas av tillsynen, i Göteborgs Stad; Göteborg Energi AB och Socialnämnderna i Staden. Tillsynen avser att granska bland annat om;

- om organisationens ledning tydligt definierat och gett en skriftlig beskrivning av dataskyddsombudets uppgifter,
- vilka arbetsuppgifter dataskyddsombudet har och
- om dataskyddsombudet har tillräckliga resurser för att utföra dessa arbetsuppgifter.
- Om dataskyddsombudets synpunkter i allmänhet följs av organisationen och om det dokumenteras i de fall organisationen inte följer dessa råd.
- Om ledningen ser till att dataskyddsombudet på ett korrekt sätt och i god tid deltar i alla frågor som rör skyddet av person-

[24] Dnr IMY-2023-1647
[25] Flera ärenden; För tillsynskrivelsen, se: Tillsyn enligt dataskyddsförordningen (imy.se)

uppgifter och har de resurser som behövs för att fullgöra sina uppgifter.

Tillsynen pågår och kan, utöver eventuella sanktioner för de granskade, komma att leda till nya råd för tillämpningen av DSF:s regelverk för alla personuppgiftsansvariga som är skyldiga att utse dataskyddsombud.

Regionstyrelsen i Region Skåne[26] *(Beslut)*

IMY inledde - efter att ha tagit emot klagomål från registrerade och en anmälan om personuppgiftsincident - ett tillsynsärende och granskning av Region Skåne. Bakgrunden var att en medarbetare tappat bort ett okrypterat USB-minne som innehöll personnummer och känsliga personuppgifter för närmare 2 000 personer. Under granskningen framkom att USB-minnet inte heller återfunnits.

IMY slutsats efter granskningen var att de tekniska och organisatoriska åtgärder som regionen vidtagit inte var tillräckliga för att tillgodose en lämplig säkerhetsnivå i förhållande till risken med behandlingen. Detta eftersom regionen hade lagrat känsliga personuppgifter på ett okrypterat USB−minne som sedan hade tappats bort.

Innehållet på USB-minnet kopplade ihop uppgifter om hälsa med ett stort antal patienter genom deras personnummer, vilket då innebar en hög risk för de registrerades fri- och rättigheter. IMY konstaterade att regionen därmed inte uppfyllt säkerhetskraven enligt dataskyddsförordningen och att det i det aktuella fallet var allvarligt eftersom det var frågan om en sådan typ av personuppgifter som enligt regelverket kräver ett starkt skydd.

Det var vidare regionen, som i egenskap av personuppgiftsansvarig hade det yttersta ansvaret för hur personuppgifter hanterades i verksamheten. I det ansvaret ingick bland annat att vidta både tekniska och organisatoriska säkerhetsåtgärder för att skydda personuppgifterna, till exempel genom att tillhandahålla krypterade USB-minnen.

IMY konstaterade slutligen i sitt beslut att överträdelsen rörde ett stort antal registrerade vars personuppgifter var skyddade av sekretess. Det var dessutom en försvårande omständighet att USB-minnet inte återfunnits

[26] Dnr IMY-2022-1290

och att det var oklart vilken spridning personuppgifterna som skett. Myndigheten bestämde därför utifrån en samlad bedömning att påföra regionen en administrativ sanktionsavgift på 200 000 kronor.

Region Uppsala, gällande hantering av e-post[27] *(Pågår)*

IMY har inlett en tillsyn och granskning för att ta reda ta reda på om man inom Region Uppsala i tillräcklig utsträckning har tagit hänsyn till patienternas rätt till integritetsskydd vid användningen av e-post.

Bakgrunden är att IMY tagit emot en anmälan om en personuppgifts-incident från regionen som indikerar att personuppgifter om hälsa under lång tid har skickats och lagrats i e-postprogrammet Outlook.

IMY konstaterar att personuppgifter om patienter är särskilt skyddsvärda och att det därför krävs att de hanteras i tekniska system som har hög säkerhet. IMY:s granskning av regionen sker i form av en inspektion för att ta reda på vilka tekniska och organisatoriska säkerhetsåtgärder som vidtagits för att skydda personuppgifter om patienter när e-post används.

Hälso- och sjukvårdsnämnden i Region Dalarna[28] *(Överklagat beslut)*

IMY har genomfört tillsyn av Region Dalarna efter att ha tagit emot klagomål gällande att regionen skrivit ut kallelser till patientbesök där den vårdinrättning som besöket avsett har varit fullt synlig i fönster-kuvertet. IMY:s inledande bedömning var att behandlingen av person-uppgifter i det aktuella fallet delvis var automatiserad och att dataskydds-förordningen därför var tillämplig.

Efter granskningen konstaterades att användningen av fönsterkuvert vid utskick av kallelser från de mottagningar som granskningen omfattade innebar att känsliga personuppgifter obehörigen röjts för ett okänt antal personer som kommit i kontakt med brevet. Det handlade om cirka 2 500 kallelser per år, bland annat till en barn- och ungdomsmedicinsk mottagning och till en samtalsmottagning för barn och unga.

Hälso- och sjukvårdsnämnden i Region Dalarna uppgav att den upphandlat en tjänst för utskick av kallelser där det inte skulle framgå av

[27] Dnr – ej angivet av IMY
[28] Dnr IMY-2022-695

kuvertet vilken mottagning som en kallelse till vårdbesök avsåg. Efter att IMY inlett tillsyn genomförde nämnden dock en utredning som visade att den aktuella tjänsten inte omfattat alla kallelser och att kallelser från vissa vårdinrättningar därför skickats i kuvert som visat vilken klinik besöket avsåg.

IMY konstaterade i sitt beslut att regionen inte har vidtagit tillräckliga säkerhetsåtgärder för att skydda känsliga personuppgifter mot obehörigt röjande i samband med utskicken. Myndigheten utfärdade därför en administrativ sanktionsavgift på 200 000 kronor mot regionen för överträdelse av dataskyddsförordningen.

Regionen överklagade beslutet till förvaltningsrätten som avslog överklagandet. Domen har därefter överklagats av regionen till kammarrätten som meddelat prövningstillstånd.

Region Uppsala, personuppgiftsincidenter[29] *(Beslut)*

IMY har med anledning av två anmälningar om personuppgiftsincidenter granskat Region Uppsala, regionstyrelsen och sjukhusstyrelsen. Myndigheten konstaterade efter granskningen att regionen inte har vidtagit tillräckliga tekniska och organisatoriska åtgärder för att säkerställa en lämplig säkerhetsnivå i förhållande till risken för de personuppgifter som behandlades.

Den ena granskningen rörde känsliga personuppgifter och personnummer som skickats via e-post. Själva överföringen av e-posten var krypterad men inte informationen i e-postmeddelandena. Det rör dels mejl med patientuppgifter som skickats automatiserat till berörda vårdförvaltningar inom regionen, dels mejl med patientuppgifter som skickats manuellt till forskare och läkare inom regionen. För de konstaterade bristerna i denna granskning utfärdade IMY en administrativ sanktionsavgift på 300 000 kronor mot regionstyrelsen i Region Uppsala.

Den andra granskningen rörde hur Akademiska sjukhuset i Uppsala skickat e-post med patientuppgifter till patienter och remittenter i tredjeland, alltså länder utanför EU. IMY:s granskning omfattade även lagringen av patientuppgifter i sjukhusets e-postserver. Myndigheten har granskat säkerheten för de personuppgifter som behandlats men inte

[29] Dnr DI-2019-9457 respektive DI-2021-5595

lagligheten i själva tredjelandsöverföringen. För de konstaterade bristerna som granskningen påvisat utfärdade IMY en sanktionsavgift på 1 600 000 kronor mot sjukhusstyrelsen i Region Uppsala.

Sveriges Kommuner och Regioner, väntetidsdatabas[30] (Pågår)

SKR använder sig av ett IT-system i form av en nationell väntetids-databas för att ta fram väntetidsstatistik i vården. Informationen i databasen består av uppgifter som samlats in från patientjournaler i regionerna och som sedan överförts från regionerna till SKR.

IMY har beslutat att granska hur SKR hanterar personuppgifter i IT-systemet.

Uppföljning av överklagade beslut (från 2022 och tidigare)

Föregående års DSO-rapport redovisade ett antal överklagade beslut avseende kommun- och regionsektorn som då ännu inte var slutligt avgjorda. En uppföljning av dessa för 2023 ser ut som följer.

Utvecklingen efter 2022 års rapport är markerad med mörkblå fet text i tabellen.

Personuppgifts-ansvarig	Brister	Överklagandestatus
AB Storstockholms lokaltrafik, SL	IMY konstaterade att SL brutit mot DSF när biljettkontrollanter utrustats med kropps-kameror som spelar in bild och ljud. IMY riktade även kritik mot att SL i sitt sätt att informera om kamera-bevakningen inte gjort vad som krävs, bland annat genom att inte tydligt ange att kamerorna inte bara	Ärendet överklagades till förvaltningsrätten som nedsatte sanktionsavgiften till 12 000 000 kronor. IMY överklagade förvaltningsrättens dom till kammarrätten som nedsatte sanktionsavgiften till 8 000 0000 kronor IMY har överklagat kammarrättens dom till

[30] Dnr DI-2021-9333

	spelat in bilder utan även ljud. Administrativ sanktions-avgift mot SL. 16 000 000 kronor.	högsta förvaltnings-domstolen. **HFD har meddelat prövningstillstånd 2023-11-01, mål 870-23.**
Regionstyrelsen Region Värmland, (Rådgivningsnummer 1177)	Inspelade samtal till 1177 har legat tillgängliga utan lösenordsskydd eller annan säkerhet på en webbserver och därmed funnits tillgängliga via internet. Administrativ sanktionsavgift mot Region Värmland. 250 000 kronor.	Ärendet överklagades till förvaltningsrätten som fastställde IMY:s beslut. **Ärendet har inte överklagats vidare.** ***Beslut om sanktion-avgifter kvarstår.***
Region Östergötland, Region Västerbotten, Sahlgrenska Universitetssjukhuset, Karolinska Universitetssjukhuset (Åtta offentliga och privata vårdgivare samgranskades).	Vårdgivares hantering av personalens åtkomst (behörigheter) till verksamheternas huvud-journalsystem. Administrativ sanktionsavgift mot: Region Östergötland 2 500 000 kronor. Region Västerbotten 2 500 000 kronor. Sahlgrenska Universitetssjukhuset 3 500 000 kronor. Karolinska Universitetssjukhuset 4 000 000 kronor.	Vårdgivarna överklagade IMY:s beslut till förvaltningsrätten som avslog överklagandena. Vårdgivarna överklagade då ärendena vidare till kammarrätten som upphävde IMY:s beslut. IMY har överklagat kammarrättens dom till högsta förvaltnings-domstolen och inväntar prövningstillstånd. **HFD meddelar inte prövningstillstånd. Kammarrättens avgörande står därmed fast.** ***Beslut om sanktion-avgifter undanröjs.***
Utbildningsnämnden i Stockholms Stad - Skolplattformen	Allvarliga och omfattande brister i fråga om behörigheter och åtkomst till personuppgifter kopplade till elever, lärare och vårdnadshavare.	Överklagad av Stockholms Stad till förvaltningsrätten som nedsatte sanktionsavgiften till 3 000 000 kronor.

	Bristerna omfattade delvis även integritetskänsliga (särskilda/känsliga) personuppgifter. Administrativ sanktionsavgift mot Stockholms Stad 4 000 000 kronor.	Domen överklagades (av IMY) till kammarrätten som upphävde förvaltningsrättens dom och fastställde sanktionsavgiften till 4 000 000 kronor. Kammarrättens dom är överklagad till högsta förvaltningsdomstolen. **HFD meddelar inte prövningstillstånd. Kammarrättens avgörande står därmed fast.** ***Beslut om sanktionsavgift kvarstår.***

Sammanfattande kommentar – tillsyn i kommun- och regionsektorn

Av de redovisade ärendena kan följande slutsatser dras.

- Personuppgiftsansvaret knyts vid tillsyn alltid tydligt till verksamheternas översta ledning – det vill säga till styrelser och nämnder. Det saknar betydelse om bristerna handlar om detaljfrågor såsom brister i datasystem, handhavandefel, brister i praktisk hantering eller rent slarv från medarbetare. Ansvaret för att detta inte ska förekomma vilar enligt regelverket på ledningen och därför krävs också ansvaret ut där, oavsett var en brist i en verksamhet uppstår. Det är därför viktigt att styrelser och nämnder betraktar integritets-frågorna som strategiska frågor som kräver kunskap, engagemang och resurser.

- Det är viktigt att verksamheterna har en bra och ändamålsenlig kontroll över hur känsliga personuppgifter behandlas. Brister i fråga om detta ses regelmässigt som allvarliga vid tillsyn, vilket också är konsekvent mot hur reglerna är utformade.

- Ärendena bekräftar att tillsynsärenden både kan initieras när en anmälningspliktig PU-incident inträffar och då klagomål inkommer mot en personuppgiftsansvarigs verksamhet.

- Ärendena visar också att IMY:s bedömningar tenderar att stå sig baserat på utfallen de överklagandeprocesser man kunnat följa så här långt.

Sammanfattning av avsnittet:

- IMY:s verksamhet och kapacitet fortsätter att växa. Fokus för tillsynen är de klagomål som inkommer till myndigheten, dessa har ökat kraftigt från 2023. Kraven på hur klagomål ska utredas och handläggas av IMY har skärpts via rättspraxis 2023.

- Beslutade sanktionsavgifter under 2023 har ökat kraftigt från ca 9,7 miljoner kronor (2022) till 120,0 miljoner kronor.

- IMY:s beslut där sanktionsavgifter påförs blir som regel föremål för prövning i domstol. Tendensen är att IMY:s bedömningar står sig vid prövningarna.

- Personuppgiftsansvaret knyts vid tillsyn alltid tydligt till verksamheternas översta ledning, vilket i kommun- och regionsektorn är styrelser och nämnder. Det saknar betydelse om bristerna handlar om detaljfrågor såsom brister i datasystem, handhavandefel, brister i praktisk hantering eller rent slarv från medarbetare. Det är därför viktigt att även styrelser och nämnder är medvetna om detta och betraktar integritetsfrågorna som strategiska frågor.

3. Stadsrevisionens informationssäkerhets- och dataskyddsarbete 2023

Informationssäkerhetsarbete och dataskydd hänger mycket tätt ihop. Det ena är en förutsättning för det andra och olika informationssäkerhets-frågor har ofta direkta dataskyddsaspekter kopplade till sig.

I detta avsnitt kommer jag att redogöra för mina iakttagelser över hur stadsrevisionens arbete med informationssäkerhet och dataskydd fortskridit under 2023. I viss mån har även iakttagelser avseende Göteborgs Stads arbete beskrivits. Då jag bedömt att gjorda iakttagelser behövt kommenteras så har jag lagt till kommentarer i kursiv stil under varje aktuellt delavsnitt.

Stadsrevisionens strävan att utveckla sitt informationssäkerhetsarbete inleddes 2019 och har bedrivits sedan dess. Det har också fortsatt under 2023. Styrande för utvecklingen har den handlingsplan som togs fram till sommaren 2020 fortsatt att vara. Planen identifierade ett antal fokus-områden för stadsrevisionen att arbeta med framåt.

Status 2023 för hantering av fokusområdena framgår av nedanstående tabell:

	Fokusområde	Status 2023
A	Kompetensutveckling För all personal - höj kunskapen om hantering av personuppgifter och sekretesskyddad information	Genomfört och pågående [31]

[31] Kompetensutveckling inom informationssäkerhet måste bedrivas kontinuerligt Stadsrevisionen har under 2023 arbetat med ut- och fortbildning rörande informationssäkerhet/dataskydd och allmänna handlingar/offentlighet och sekretess. En viktig källa till kompetensutveckling utgörs också av granskning av informationssäkerhet och närliggande frågor. Under 2023 har sådan granskning genomförts avseende Göteborgs Hamn AB, Göteborgs Stadshus AB, inköp- och upphandlingsnämnden, Renova AB

B	Klassning av information	Genomfört. Det noteras att en ny klassningsmodell för information införts i Göteborgs Stad våren 2023. En översyn av stadsrevisionens informationsklassning behöver därför göras.
C	Systemförteckning (Baserad på tjänste- och applikationslistan från intraservice)	Väsentligen genomfört. Kvarstående åtgärder kopplar i kontinuitets-planering, lokala systemansvarsfrågor och synkronisering av ansvarsfrågor för IT-miljön som tillhandahålls av intraservice.
E	Utveckla rutiner och arbetssätt (Såväl DSF-relaterade rutiner och arbetssätt som övriga rutiner och arbetssätt för kontorets förvaltnings- och granskningsverksamhet) Exempel: • Rutin för behörighets-hantering. • Rutin för lagring av digital information (innefattande e-post, server- och moln-lagring m m). • Rutin för hantering av PU-incidenter. • Rutin för hantering av registerutdrag.	Arbete pågår, rutiner för Rutiner för hantering av PU-incidenter och hantering av registerutdrag har framtagits under 2023 Kvarstående frågor handlar om att fortsätta utveckla behörighetshantering generellt och även utveckla arbetssätt kopplade till informations-hantering/lagring av digital information generellt och specifikt vid användning av IT-systemet Visma Ciceron.
F	Synkronisera informationssäkerhetsarbetet med övrigt säkerhetsarbete	Synkronisering med övrigt arbete för intern kontroll har skett. Kontinuerlig översyn/ utvärdering behöver göras över tid.

Stadsrevisionen har arbetat aktivt med fokusområdena och har successivt löst in de flesta uppgifterna som identifierades som nödvändiga att hantera enligt handlingsplanen från 2020. Då informationssäkerhets-arbetet för en organisation alltid behöver bedrivas kontinuerligt och systematiskt, blir det dock aldrig helt ”klart”. I Stadsrevisionens fall bedömer jag dock att arbetet nu börjar övergå i en ny fas som kommer att handla mer om att förvalta och utveckla det arbete som gjorts 2020-2023. Denna fas kommer också att behöva hantera uppdatering av tidigare upprättade dokument avseende exempelvis informations-klassning och förteckning över personuppgiftsbehandlingar.

Ett arbete av viss omfattning kommer också att behöva göras för att se över och utveckla befintliga arbetssätt runt handlings- och informationshantering i verksamheten kopplat till att IT-systemet Visma Ciceron DoÄ införs 2024. Förutsättningarna för detta arbete kommenteras under separat rubrik nedan.

Informationssäkerhet och dataskydd i Göteborgs Stad 2023

I föregående års DSO-rapport noterades att det gick att se tydliga målsättningar från Staden att strama upp det samlade informationssäkerhetsarbetet och att eftersträva en bättre samordning av detta än vad som funnits tidigare. Under 2023 har detta arbete fortsatt genom att förtydliganden av krav för ett ändamålsenligt informationssäkerhetsarbete på nämnder och styrelser. De stadsgemensamma dataskyddsombudens arbete förefaller också funnit sin form och olika organisatoriska åtgärder verkar också börja komma på plats. Jag ska kommentera något runt detta under egna delrubriker nedan.

Ny riktlinje för informationssäkerhet

En ny riktlinje för informationssäkerhet antogs av fullmäktige under våren 2023. Riktlinjen ersätter tidigare styrdokument och förtydligar respektive utvecklar Stadens krav på sina verksamheter. I korthet ser kravbilden ut enligt följande:

Samtliga nämnder och styrelser ska:

- Genomföra informationsklassning
- Säkerställa /tillfredställande/ informationssäkerhet vid införande av nya system
- Säkerställa /tillfredställande/ informationssäkerhet vid upphandling av nya system
- Hantera incidenter så att skador minimeras i verksamheten och att eventuell anmälningsskyldighet fullgörs.
- Säkerställa att det finns en åtgärdsplan (kontinuitetsplan) så kritisk verksamhet kan fortgå
- Säkerställa att där finns personrelaterade säkerhetsåtgärder i verksamheten man ansvarar för.

- Säkerställa att där finns organisatoriska säkerhetsåtgärder i verksamheten man ansvarar för.
- Säkerställa att där finns fysiska säkerhetsåtgärder i verksamheten man ansvarar för.
- Säkerställa att där finns tekniska säkerhetsåtgärder i verksamheten man ansvarar för.
- Säkerställa att där finns systemdokumentation (system- och driftsdokumentation) för varje system.
- Säkerställa att där finns säkerhetsåtgärder för nätverk och nätverkstjänster i verksamheten man ansvarar för.
- Säkerställa att i riktlinjen föreskrivna krav för anskaffning, utveckling, underhåll och avveckling av IT-system finns.
- Följa upp sitt eget informationssäkerhetsarbete.

Stadsrevisionen omfattas inte med automatik av riktlinjen då stadens revisorer– bortsett i fråga om krav på följsamhet mot fullmäktiges arkivreglemente – själva inom ramen för gällande lagstiftning fattar beslut kopplade till sin egen förvaltning. Detta inkluderar rätten att välja vilka av Stadens riktlinjer och i vilken utsträckning dessa ska tillämpas i den egna förvaltningen. Samtidigt följer revisorerna av tradition de centrala stadsinterna regelverken runt exempelvis personal/HR, ekonomi/redovisning och upphandling/ inköp. Som användare av kommungemensamma IT-system och tjänster i den kommungemensamma IT-miljön som tillhandahålls av nämnden för intraservice torde det då också vara svårt, att med trovärdighet hävda, att revisorerna inte ska följa och iaktta vad fullmäktige föreskrivit för övriga verksamheter i staden runt hur det samlade informationssäkerhetsarbetet i staden ska se ut.

CISO tillsatt för Göteborgs Stad

Göteborgs Stad har utsett en tjänsteperson i rollen som CISO[32] (informationssäkerhetsansvarig) för Staden med placering vid stadsledningskontoret. Rollen innefattar att leda och samordna informationssäkerhetsarbetet i förvaltningar och bolag i Staden.

CISO har även besökt revisionskontoret under hösten 2023 och informerat om sitt uppdrag och om Stadens nya riktlinje för informationssäkerhet. Detta bedöms vara en positiv åtgärd för att stärka medvetenheten hos organisationen om Stadens pågående utveckling av sitt samlade informationssäkerhetsarbete.

Intraservice roll och ansvar för stadsgemensam IT-miljö

I arbetet att förtydliga olika verksamheters ansvar i den stadsgemensamma IT-miljön utifrån sina respektive roller och funktioner driver intraservice ett arbete att upprätta avtal i form av SLA (Service Level Agreements) respektive PUB-avtal (personuppgiftsbiträdesavtal) med Stadens verksamheter. Arbetet har dock inte lett fram till att några avtal kunnat tecknas med stadsrevisionen under 2023.

Stadsrevisionen har i detta sammanhang haft dialog med intraservice runt utformningen av i första hand PUB-avtal, som i framtagna utkast till handlingar inte motsvarat DSF:s krav. Detta behöver hanteras framåt. Jag har i samband med stadsrevisionens arbete att ta fram konsekvensbedömningar för nya IT-system påtalat vikten av att korrekta PUB-avtal upprättas.

Beslutad omorganisation – avdelning för dataskydd/stadsledningskontoret

Stadsledningskontoret har utrett behovet av en omorganisation av avdelningen för dataskydd vid intraservice där de stadsgemensamma DSO är placerade. Utredningen landade i förslaget att den nuvarande organisationen vid intraservice ska kompletteras med en central funktion

[32] CISO utläses som Chief Information Security Officer och är en vedertagen benämning på rollen som informationssäkerhetsansvarig person i en organisation i informationssäkerhetssammanhang.

för samordning och styrning av dataskyddsfrågor placerad vid stadsledningskontoret. Omorganisationen bedömdes inte medföra några ökade kostnader för staden som helhet då den bygger på en omfördelning av befintliga avsatta resurser till intraservice. Förslaget tillstyrktes av kommunstyrelsen och behandlades av fullmäktige vid sammanträde 2023-12-07. I samband med fullmäktiges beslut intogs även ett tilläggsyrkande med innebörden att berörda nämnder (kommunstyrelsen/ intraservice) i nära samverkan med berörda fackliga parter ska genomföra en riskbedömning utifrån säkerhet och arbetsmiljö och vid behov återkomma med förslag på åtgärder.[33]

Det är för tidigt att ha några särskilda synpunkter på beslutet i fråga. Att utredningen kommit fram till att strategiska perspektiv på stadens dataskyddsarbete behövs synes klokt. Att ett sådant perspektiv avses att finansieras via en minskad granskande och stödjande verksamhet från dataskyddsombudens sida synes kanske mindre klokt om det också skulle medföra inskränkningar av det arbete som utförs där.

Stadsövergripande iakttagelser från stadens DSO

Som berörts ovan bedöms de stadsgemensamma dataskyddsombudens arbete ha börjat finna sin form. Det är också ofta intressant att ta del av de synpunkter och råd som formuleras av avdelningen för dataskydd för Stadens verksamheter.

Avdelningen har också tagit fram bra och användbara stöddokument för praktiskt dataskyddsarbete. Stadsrevisionen har utgått från de stöddokument som finns framtagna för riskanalys- och konsekvensbedömningar vid sitt arbete med sådana under 2023-2024.

Jag vill här citera ett stycke ur en av dataskyddsenhetens årsrapporter för 2023 runt perspektiv på Stadens dataskyddsarbete som jag finner både intressant och tänkvärt för envar med intresse för frågorna som sådana.[34] Jag har också valt att markera ett stycke i den citerade texten med fetstil.

”Fokus på ny teknik och AI har en enorm potential för att göra våra liv bättre, men den digitala utvecklingen blir inte hållbar utan begränsningar. Utan tydlig styrning i arbetet med digital innovation är risken att det går fort och att man i sin iver att röra

[33] Se vidare KF protokoll 2023-12-07 samt handling 2023 nr 223.
[34] Dataskyddsenheten vid intraservice, Årsrapport för dataskyddsarbetet, Grundskolenämnden, s.4

sig framåt glömmer att hänsyn behöver tas till den personliga integriteten och att personuppgifter behandlas på ett korrekt sätt.

Verksamheter i Göteborgs stad behöver tydligt ha med sig integritetsaspekten vid framtagandet av innovativa och nya lösningar inom till exempel AI. Arbetet med att säkerställa att personuppgifter behandlas enligt reglerna i dataskyddslagstiftningen behöver genomsyra arbetet inom de kommunala verksamheterna på alla olika plan.

Det gäller allt från rutiner och processer för det dagliga arbetet, till arbetet med innovations- och digitaliseringslösningar för framtidens arbetssätt inom Göteborgs Stad. Som en stor offentlig aktör har Göteborg som stad att förvalta alla invånare och besökares förtroende. Oavsett om det handlar om elever, vårdnadshavare, brukare inom socialtjänst, eller någon annan kategori av kommuninvånare, så ska man kunna känna sig trygg med att användandet av innovativ teknik sker med respekt för den personliga integriteten och de regelverk som finns för att skydda enskildas personuppgifter. I takt med att tekniken tar en allt större plats i våra liv ökar också riskerna för att spåra och övervaka människor. På det rättsliga området har detta fört med sig att regleringarna på EU-nivå blir fler och alltmer komplexa. För att utvecklingen ska kunna ske på ett långsiktigt hållbart sätt är det nödvändigt att varje verksamhet förstår de regelverk som finns, och varför de finns. Man kan naturligtvis se det som en balansakt, men som dataskyddsombud vill vi vara extra tydliga med att balansen alltid behöver vara lagd till de enskilda registrerades fördel och aldrig får innebära att verksamheter tummar på det regelverk som finns till för att skydda personuppgifter.

Verksamheterna behöver följa dataskyddslagstiftningen på samma sätt som man behöver följa all annan lagstiftning. Dataskyddsombudet bedömer att det inom Staden finns en felaktig uppfattning om att det är omöjligt att följa GDPR och samtidigt driva den digitala utvecklingen framåt. Det finns också en felaktig uppfattning om att GDPR är en lagstiftning som inte är obligatorisk att följa. Dataskyddsombudet vill därför särskilt lyfta att dessa uppfattningar är problematiska och medför risker i form av att dataskyddsperspektivet förbises i digitaliseringsarbetet.

Fokus behöver därför skiftas från att betrakta reglerna i dataskydds-lagstiftningen som hinder, till att i stället fokusera på syftet med lagstiftningen och använda den som en grund att utgå från i utvecklingen av innovations- och digitaliseringslösningar. Ett sådant fokus kommer gynna enskilda individer och samtidigt medföra en mer hållbar och rättssäker digitalisering i samhället på lång sikt”

Dataskyddsenheten har, i fråga om dataskyddsfrågorna i Staden, ett översiktsperspektiv som i viss mån kan jämföras med stadsrevisionens översiktsperspektiv för verksamhetsrisker i samma Stad. De iakttagelser man gör och skriver om beträffande stadens uppfattning runt följsamhet mot gällande regelverk bör därför noteras och även övervägas vidare som en betydelsefull verksamhetsrisk av Stadens revisorer.

Stadsrevisionens löpande hantering av vissa särskilda frågor inom informationssäkerhet och dataskydd 2023

Stadsrevisionens arbete med att utveckla sitt informationssäkerhetsarbete har som angetts ovan fortsatt under 2023. Jag kommer här att kommentera vissa särskilda frågor med bäring på dataskydd som hanterats under året. Jag kommer också att lämna uppföljande kommentarer för sådana frågor som uppmärksammades i föregående års DSO rapport (2022).

Utarbetade rutiner och anvisningar 2023 med mera

Jag har tidigare lyft behovet av att stadsrevisionen utarbetar lokala rutiner och anvisningar för hantering av DSF-relaterade frågor i verksamheten. Syftet med detta är att det både skapar en stödjande struktur vid faktisk handläggning och dessutom dokumenterar att organisationen aktivt eftersträvar en följsamhet mot regelverket (vilket man behöver kunna visa vid en eventuell tillsyn.)

Under 2023 har rutiner och anvisningar utarbetats beträffande hantering av personuppgiftsincidenter och begäran om registerutdrag enligt DSF. Stadsrevisionen har också tagit fram en informationstext till hemsidan där det beskrivs hur personuppgifter hanteras, Hänvisning med länk till informationstexten finns numera i alla e-postsignaturer för medarbetarna.

Stadsrevisionen har också berörts av några personuppgiftsincenter under året. De har uppstått i den kommungemensamma IT-miljön och rapporterats av nämnden för intraservice. DSA[35] för stadsrevisionen har utrett och hanterat dessa samt i ett fall också anmält incidenten till IMY. Anmälan ledde inte till vidare åtgärd. Personuppgiftsincidenterna har dokumenterats lokalt av stadsrevisionen. Jag har bistått DSA vid hanteringen i en rådgivande roll.

Användning av MS Office 365 i verksamheten

Tidigare problematik kopplat till tredjelandsöverföringar till Förenta staterna för användare av Microsoft Office 365 och avsaknaden av giltigt adekvansbeslut har upphört under 2023 i och med EU-kommissionens

[35] DSA (Dataskyddsansvarig) är administrativ chef hos stadsrevisionen.

nya beslut. Problematiken kan dock aktualiseras på nytt om det nya adekvansbeslutet upphävs efter prövning av EU-domstolen.[36]

Konsekvensbedömningar

Innan ett nytt IT-system som behandlar personuppgifter på något sätt ska tas i bruk, så ska en personuppgiftsansvarig pröva om användningen av det kommer att innebära behandling av personuppgifter som sannolikt leder till en hög risk för fysiska personers rättigheter enligt DSF. Detta kallas ibland för att göra en tröskelanalys. Om prövningen (tröskel-analysen) visar att sådan risk finns, ska den personuppgiftsansvarige göra en utförlig riskanalys och en konsekvensbedömning. Det ska tilläggas att det i praktiken inte ställs särskilt höga krav för att skyldigheten att göra en konsekvensbedömning ska utlösas. En personuppgiftsansvarig kan också frivilligt välja att göra en konsekvensbedömning även om det inte skulle visa sig vara obligatoriskt enligt tröskelanalysen.

Stadsrevisionen har under ledning av DSA genomfört två konsekvens-bedömningar under 2023/2024 avseende de två kommungemensamma IT-systemen Digitala navet och Visma Ciceron DoÄ.

Utbildningsinsats inom informationssäkerhet och dataskydd

All reell informations- och datasäkerhet i en organisation behöver bygga på en förståelse för syften och förutsättningar för att hantera och skydda information av olika slag inom och utom IT-system. I en offentlig verksamhet behövs också kunskap om de regelverk som styr offentlighet och sekretess i förhållande till detta. Stadsrevisionen har därför under 2023 – som ett led i att förbereda införandet av IT-systemet Visma Ciceron DoÄ, genomfört en riktad utbildningsinsats angående detta för samtliga medarbetare under två halvdagar. Jag har ansvarat för att ta fram och genomföra utbildningsinsatsen i fråga.

Särskilt om införande av Visma Ciceron DoÄ[37]

Stadsrevisionen inför det nya stadsgemensamma systemet för dokument- och ärendehantering 2024, Visma Ciceron DoÄ (i det följande Ciceron).

---

[36] Se vidare s. 7 ovan.
[37] Denna punkt är baserad på text som återfinns i dokumentet Bilaga 3 - Kommentarer och rekommendationer från dataskyddsombudet till Konsekvens-bedömning avseende Visma Ciceron DoÄ Diarienummer 0229/22

Införandet av systemet vilar på en strävan från Staden att samtliga fackförvaltningar och bolag, genom förändrade arbetssätt ska uppnå ökad rättssäkerhet, kostnadseffektivitet och transparens, därtill kommer en målsättning att uppnå ökad styrförmåga ur ett hela-staden perspektiv.[38]

I enlighet med stadens riktlinje för styrning, samordning och finansiering av digital utveckling och förvaltning ansvarar vidare varje nämnd och styrelse för att implementera verksamhetsförändringar, såsom exempelvis nya arbetssätt kopplade till användningen av systemet/tjänsten.[39] Stadsrevisionen omfattas inte med automatik av ovannämnda riktlinje, i enlighet med vad som diskuterats ovan. Av tradition följer dock revisorerna, som en del av stadens organisation, vanligtvis vad fullmäktige föreskrivit i förvaltningsfrågor.

För stadsrevisionens del innebär införandet av systemet – på samma sätt som för andra användare/verksamheter i Göteborgs Stad – att arbetssätt behöver ses över och anpassas i viss mån. Detta gäller då särskilt arbetssätt för dokumentation av granskning, som tidigare skett i en äldre systemmiljö som inte är anpassad till nu gällande krav för personuppgiftshantering. För vidare utveckling av behovet av och motiven för förändrade arbetssätt hänvisas till det yttrande jag avlämnat som bilaga till den konsekvensbedömning stadsrevisionen gjort avseende Ciceron.[40]

Den utveckling/förändring av arbetssätt som kommer att krävas har icke dess mindre väckt viss oro i organisationen. Detta har också kanaliserats via de lokala fackliga organisationerna. Jag kan i fråga om det konstatera att revisionsledningen adresserat frågorna löpande och också avsatt tid framåt för att hantera de svårigheter och den eventuella fortsatta oro som kan finnas inför de nödvändiga förändringar som förestår.

Att på ett konstruktivt sätt lösa de eventuella problem som kan uppstå kommer dock att vara en utmaning för hela organisationen. Det är då av central betydelse att revisionsledningen bibehåller ett engagemang och fokus för den förändringsledning som krävs. En viktig komponent för att kunna uppnå detta är en ökad kunskap om sakfrågorna som ligger till

---

[38] Jfr Generell Nyttorealiseringsplan Mallversion 4.0 Införa stöd för dokument- och ärendehantering med vidare hänvisning till Göteborgs Stads riktlinje för styrning, samordning och finansiering av digital utveckling och förvaltning D nr 0437/20 som trädde i kraft 2023-01-01.
[39] Jfr a.a.
[40] Diarienummer 0229/22, beslut av revisorskollegiet 2024-02-20.

grund för de behov de förändrade arbetssätten behöver lösa in. Det handlar då både om systemkunskap och om kunskap om de krav-ställningar som gäller för informations- och handlingshantering i stads-revisionens verksamhet. Jag vill här återkoppla till IMY:s uttalanden som återgivits ovan.[41]

IMY menar också att det framstår som att de största utmaningarna för det praktiska dataskyddsarbetet idag är;

1) att få till fungerande rutiner och processer respektive,
2) att få dataskyddsreglerna att inte hindra eller försvåra verksamheten.

Allt fler dataskyddsombud verkar också uppleva att ett av de största problemen kopplat till det praktiska dataskyddsarbetet är bristande engagemang och låg kunskap hos ledningen.

Stadsrevisionen har enligt min bedömning kommit långt i sin utveckling av sitt informationssäkerhets- och dataskyddsarbete kopplat till styrande och stödjande processer – i vart fall om det ställs i relation till hur utgångsläget var 2019/2020.

Den stora utmaningen framåt är att också skapa och implementera fungerande rutiner, processer och arbetssätt för stadsrevisionens kärnverksamhet som består av yrkesrevisionell granskning. I detta kan Ciceron vara ett mycket användbart hjälpmedel förutsatt att organisationen förmår göra det till sitt och även använda det som det verksamhetsverktyg det har alla förutsättningar för att bli i framtiden. Jag har tidigare redovisat min inställning till detta i ovannämnda yttrande till konsekvensbedömningen för Ciceron och där lämnat följande rekommendation i frågan.

Stadsrevisionen rekommenderas att säkerställa att tillräckliga resurser avsätts för att driva en aktiv förändringsledning i fråga om verksamhetens arbetssätt så att användningen av Ciceron såväl uppnår en stärkt följsamhet mot regelverken för dataskydd och offentlighet/

[41] Se s. 13 ovan.

sekretess som Stadens mål om ökad rättssäkerhet, kostnadseffektivitet och transparens eftersträvar.

Det är viktigt att denna rekommendation omhändertas under 2024 och framåt.

Planerade översyner – framåtriktat arbete

Stadsrevisionens övriga framåtriktade arbete handlar väsentligen om tre saker:

1. Ett fortsatt sammanhållet arbete för att säkerställa en ändamålsenlig behörighetshantering i för hela verksamheten. Detta arbete är påbörjat sedan tidigare och var en del av handlingsplanen för utveckling av informationssäkerhetsarbetet 2020. Införande av Ciceron kommer att underlätta detta arbete via systemets inbyggda behörighetsstruktur via definierade systemroller.

2. En harmonisering mot stadens nya riktlinje för informations-säkerhet i tillämpliga delar. Som beskrivits ovan har riktlinjen införts 2023. Väsentliga delar av den har direkt bäring på alla verksamheter som är användare av den kommungemensamma IT-miljön. Stadsrevisionen behöver beakta detta och exempelvis uppdatera sin befintliga informationsklassning till stadens nya modell.

3. En översyn och löpande uppdatering av övriga framtagna DSF-relaterade dokument. Exempelvis befintlig förteckning över personuppgiftsbehandlingar (enligt artikel 30).

Det pågår en dialog mellan revisionsdirektör, DSA och undertecknad i en rådgivande roll beträffande hur detta framåtriktade arbete ska organiseras.

Systematisk uppföljning av kvarstående identifierade risker 2020

2020 års DSO rapport identifierade en rad risker inom dataskydds-området som stadsrevisionen bedömdes behöva omhänderta. En systematisk uppföljning har gjorts av dessa enligt nedan. Åtgärder som genomförts 2023 är markerade med mörkblå text.

Nr.	Identifierad risk 2020	Åtgärder 2021-2023	Anmärkning
1)	**Det finns risker** kopplade till bristande kunskap om hantering av PU och särskilda (känsliga) PU som behandlas i verksamheten. Sådana risker behöver omhändertas genom ytterligare utbildnings-insatser och generell översyn av styrande och stödjande dokument med fokus på att ”DSF-säkra” dessa.	Flera åtgärder har genomförts för att öka kunskapen under 2021-2023. Kontorsgemensam (åter-kommande) gallringsdag avseende arbetsmaterial i revisionsakter genomförd med fokus på samspelet mellan regelverk inom kommunalrätt, offentlighet/ sekretess samt integritetsrätt/dataskydd. Kontorsgemensam utbildning i säkerhetsskydd inklusive dataskyddsaspekter. Granskning av DSF:s tillämpning hos ett antal av Göteborgs Stads verksamheter inom ramen för den årliga granskningen. Omfattande utbildningsinsatser för samtliga medarbetare under 2023 som täcker områdena informationssäkerhet, dataskydd och allmänna handlingar/ offentlighet och sekretess. Praktiskt arbete kopplat till hantering av PU-incidenter, konsekvensbedömningar och olika typer av frågor kopplat till informationshantering.	*Stadsrevisionens organisatoriska mognad i fråga om förståelse för integritets- och dataskydd bedöms successivt öka, om än från olika nivå hos enskilda medarbetare.* *Det är viktigt att långsiktigt fortsätta att förankra integritets- och dataskydds-frågorna i organisationen.* **För att få ett brett genomslag i utveckling av arbetssätt i kärnverksamheten som ger god följsamhet mot DSF är det mycket viktigt framåt att revisionsledningen tillägnar sig en större kunskap om och insikt i regelverken – dess syften och funktion.** **Detta bedöms vara en grund-förutsättning för att säkerställa en effektiv och ändamålsenlig förändringsledning i fråga om dokumentation av kärnverksamheten i Ciceron och i övrigt.**
4)	**Det finns risker** kopplade till att frågan om PUB-avtal i förhållande till revisionsbyråerna ännu inte är klar.	Stadsrevisionen har agerat för att SKR ska adressera frågan och därigenom ge förut-sättningar för en enhetlig och korrekt tolkning på nationell nivå.	*Risken är inte omhändertagen förrän rättsläget är klart så det går att agera på ett korrekt sätt efter gällande reglering.* **Kvarstående osäkerhet finns i denna fråga. Den kan dock komma att bortfalla från 2025 och framåt vid förändrade avtalsförhållanden kopplade till redovisningsrevision.**
5)	**Det finns risker** kopplade till överföringar av PU till tredjeland inom stadsrevisionens verksamhet som behöver identifieras och värderas vidare.	Stadsrevisionen har identifierat risker kopplade till användning av MS Office 365. Kompletterande åtgärder i form av lokala anvisningar för hur systemet får användas ska tas fram så snart som möjligt.	*Det är viktigt att lokala anvisningar tas fram på planerat sätt.* *Det finns även risker kopplat till tredjelandsöverföringar som sker via användning av molnbaserad teknik i mobiltelefoner och läsplattor.* *Stadsrevisionen bör kartlägga var sådana risker finns och hur de kan begränsas.*

			Riskerna kopplade till MS Office 365 har bortfallit till följd av EU-kommissionens nya adekvansbeslut från 2023 och gällande certifiering för företaget Microsoft. **Risker kan kvarstå beträffande system och applikationer som tillhandahålls av företag som inte omfattas av adekvans-beslut/certifiering.**
8)	**Säkerställande att de registrerades rättigheter alltid kan tillgodoses** De registrerades rättigheter står i centrum för regelverket om integritet och dataskydd. Detta måste alla som arbetar i en organisation som omfattas av DSF vara medvetna om. De måste också förstå innebörden av rättigheterna och ha tillgång till styrande och stödjande dokument som är anpassade efter rättigheterna. För att detta ska kunna uppnås kommer det att krävas utbildning, fort-bildning och framtagande av nya, respektive översyn av befintliga, styrande och stödjande dokument i verksamheten.	Inga riktade åtgärder med specifikt fokus på de registrerades rättigheter under 2021 eller 2022. Se dock risk 1) ovan och åtgärder 2021/2022 där. Stadsrevisionen har under 2023 tydliggjort hur personuppgifter behandlas i verksamheten via information på hemsidan och hänvisar dit med hjälp av e-post signaturer för medarbetarna. Rutin för framtagande av registerutdrag för registrerade har utarbetats och antagits under 2023.	*Frågan måste genomsyra all utbildning och fortbildning. Det är viktigt för organisationen att se till att de registrerades rättigheter är grunden för varför regelverket ser ut som det gör.*
9)	**Det finns risker** kopplade till att stadsrevisionen som organisation ännu inte genomsyras fullt ut av de integritetsrättsliga principer som avser att skydda de registrerades rättigheter.	Inga riktade åtgärder med specifikt fokus på integritets-rättsliga principer under 2021/2022. Utbildningsinsatser under 2023 har berört området.	*Se anmärkning ovan.* *Grundförståelse för de integritetsrättsliga principerna måste läras ut via utbildning och fortbildning liksom komma till uttryck i styrande och stödjande dokument.* **Det finns ett behov av en större organisatorisk förståelse för de integritetsrättsliga principerna och dess vikt vid utveckling av befintliga arbetssätt vid granskning och dokumentation av granskning behöver uppnås**. **Denna iakttagelse kopplar också väl i de problemområden som såväl IMY**

			som Stadens DSO sett och påtalat från sina respektive perspektiv.
10)	Det finns risker kopplade till om arbetet att uppnå tillfredsställande följsamhet med DSF:s regelverk drar ut på tiden. Ju länge tid eventuella brister kvarstår desto större risk att dessa kan bli föremål för tillsynsmyndighetens granskning	Inga riktade åtgärder under 2021/2022. Ett större fokus på DSF-relaterade frågor har införts från 2023 i och med ett formellt etablerande av roll som DSA.	*Riskerna kvarstår och kan i antas öka om klagomål riktas mot stadsrevisionen då IMY ändrat inriktning för tillsynen från riskbaserad till fokuserat klagomålsbaserad.* Riskerna hanteras successivt.

Generellt sett kan det, liksom för 2021 och 2022, konstateras att stadsrevisionen i sitt arbete med att genomföra den beslutade färdplanen också successivt begränsat de identifierade riskerna. Det finns dock fortfarande utmaningar att övervinna innan stadsrevisionen kan sägas befinna sig väl i fas med alla detaljer i DSF:s regler.

Revisionsledningen behandlar informationssäkerhets- och dataskyddsfrågor som väsentliga och avsätter resurser för att organisationen ska kunna arbeta med frågorna. Man behöver dock ha klart för sig att det krävs mycket resurser för att nå fram – både till en godtagbar skyddsnivå och till en bred förståelse om frågornas betydelse i organisationen.

4. Sammanfattande kommentar och bedömning

För att sammanfatta iakttagelserna i denna rapport kan det inledningsvis konstateras att domstolarnas, myndigheternas och organisationernas arbete med att uttolka hur DSF ska tillämpas fortsätter inom EU och medlemsstaterna. Betydelsefullt är att tredjelandsöverföring till Förenta staterna nu blivit möjlig med hjälp av ett nytt adekvansbeslut. Rättspraxis har också ökat kraven på hur klagomål till IMY måste hanteras.

I takt med att EU fortsätter att driva utvecklingen runt ”det digitala årtiondet 2020” på europarättslig nivå tillkommer nya regelverk som de personuppgiftsansvariga måste förhålla sig till.

Ett förändrat säkerhetsläge i Europa och världen ställer nya krav på säkerhet och då även på informationssäkerhet. Den tekniska utvecklingen och användningen av AI medför närmast obegränsade möjligheter, men också stora risker.

Allt detta innebär att samhället aktivt måste följa med utvecklingen och också aktivt försöka identifiera och begränsa uppkommande eller befarade risker.

Myndigheter – på nationell, regional och lokal nivå måste i denna kontext agera på ett genomtänkt och systematiskt sätt. Det kan vara en utmaning att göra detta, särskilt om de frågor som måste hanteras framstår som komplexa och/eller tungarbetade.

Min bild av stadsrevisionen arbete är att det finns en tydlig framdrift i det arbete för att utveckla informationssäkerhet och dataskydd som initierades efter införandet av DSF. Ledningens engagemang har också ökat gradvis i takt med att arbetet löpt på. Detta är positivt men också nödvändigt för en långsiktig och uthållig utveckling. Arbetet som sådant blir ju heller aldrig klart – eftersom allt informationssäkerhetsarbete alltid måste bedrivas kontinuerligt över tid.

Jag har som dataskyddsombud haft en aktivt rådgivande roll i många av de informationssäkerhets- och dataskyddsrelaterade frågor som organisationen hanterat under 2023. Mina iakttagelser i samband med detta är att medarbetare och chefer som regel har ett stort intresse för frågeställningarna som sådana. Vad som dock ibland leder till onödig friktion är en stundtals i grunden felaktig syn på vikten och vidden av de integritetsrättsliga principerna i förhållande till andra målsättningar eller önskemål kopplade till hur verksamheten bör fungera. Denna iakttagelse är inte unik för stadsrevisionen, vilket också framgår med all önskvärd tydlighet av de uttalanden från Stadens DSO som citerats ovan.

Jag konstaterar i detta samma sak som Stadens DSO och i fråga om stadsrevisionen nämligen att:

*DSF:s regler och principer ska innefattas som en obligatorisk del i de arbetssätt en personuppgiftsansvarig utvecklar och tillämpar. Detta är inte valfritt utan gäller undantagslöst***.**

Att komma till rätta med ovannämnda problematik kommer att ställa krav på organisationen och dess ledning under 2024 och framåt. Jag ser det som mycket väsentligt och angeläget att det sker och att ledningen aktivt skapar goda förutsättningar för utveckling i denna del. Jag bedömer vidare att en kritisk framgångsfaktor i detta är att ansvariga chefers kunskap om DSF och de integritetsrättsliga kraven som ställs på en myndighet utökas. Kunskap ger förutsättningar att både leda förändring och bemöta oro och eventuella invändningar mot nödvändig utveckling.

För att formellt summera denna rapport kan jag konstatera att:

Jag är utsedd till dataskyddsombud för stadsrevisionen.

Jag har i denna egenskap övervakat;

- organisationens interna efterlevnad av DSF och övrig tillämplig lagstiftning.
- organisationens efterlevnad av sin strategi för skydd av personuppgifter.

Jag har deltagit i en informerande och rådgivande roll i stadsrevisionens pågående arbete att se över och utveckla sitt arbete inom informations-säkerhets- och dataskyddsområdet.

Jag har vid avlämnandet av denna rapport och under 2023-2024 lämnat råd i fråga om konsekvensbedömning av dataskydd inför införande av de kommungemensamma IT-systemen Digitala navet respektive Visma Ciceron DoÄ.

Jag har under 2023 inte haft något aktivt samarbete eller samråd med IMY.

I 2022 års DSO -rapport lämnade jag följande rekommendation:

Stadsrevisionen rekommenderas att prioritera arbetet att utveckla dokumenterade arbetssätt och rutiner för såväl granskning- som förvaltningsverksamheten, för att stärka informationssäkerhetsarbetet och att säkerställa en god följsamhet mot DSF:s regelverk.

Jag bedömer att stadsrevisionen arbetat i linje med rekommendationen under 2023 avseende i första hand förvaltningsverksamheten. Rekommendationen omformuleras därför enligt följande:

Stadsrevisionen rekommenderas att prioritera arbetet att utveckla dokumenterade arbetssätt och rutiner för granskningsverksamheten, för att stärka informationssäkerhetsarbetet och att säkerställa en god följsamhet mot DSF:s regelverk.

Mot bakgrund av vad som anförts ovan runt utveckling av arbetssätt för granskning och utmaningar i detta lämnar jag också följande rekommendation:

Stadsrevisionen rekommenderas att prioritera att kunskapsnivån rörande DSF:s regelverk och tillämpning av detta höjs för ansvariga chefer, för att skapa nödvändiga förutsättningar för att utveckla dokumenterade arbetssätt och rutiner anpassade efter regelverken för granskningsverksamheten.

Bilaga 1 – Uppdragsbeskrivning för dataskyddsombud

Göteborgs Stad

1

Uppdragsbeskrivning för dataskyddsombud (DSO) för Stadsrevisionen i Göteborgs Stad

Stadsrevisionen i Göteborg är en kommunal förvaltningsmyndighet i Göteborgs Stad.

Stadsrevisionen är personuppgiftsansvarig för all behandling av personuppgifter som sker inom ramen för dess verksamhet. Stadsrevisionen ska från den 25 maj 2018 tillämpa dataskyddsförordningens regelverk. I enlighet med detta regelverk ska dataskyddsombud (DSO) utses.

Dataskyddsombudet ska ha följande uppgifter inom ramen för sitt uppdrag:

- Att i**nformera och ge råd** till stadsrevisionen vid behandling av personuppgifter ifråga om gällande skyldigheter enligt dataskyddsförordningen och annan tillämplig dataskyddslagstiftning.
- Att ö**vervaka stadsrevisionens interna efterlevnad** av dataskyddsförordningen och annan tillämplig dataskyddslagstiftning.
- Att **övervaka stadsrevisionens efterlevnad av myndighetens strategi för skydd av personuppgifter** vilket inbegriper ansvarstilldelning, information och utbildning av personal som deltar i behandling och tillhörande granskning.
- Att **på stadsrevisionens begäran ge råd i konsekvensbedömning av dataskydd** och övervaka genomförandet av den.[1]
- Att s**amarbeta med Datainspektionen**.
- Att f**ungera som kontaktpunkt för Datainspektionen** i frågor som rör behandling, inklusive förhandssamråd[2] och vid behov samråda i alla andra frågor.

Dataskyddsombudets uppdrag omfattas av sekretess kopplad till offentlighet- och sekretesslagens regelverk. DSO ska utföra sitt uppdrag utifrån ett riskbaserat perspektiv. Det innebär att ombudets arbetsinsatser i första hand ska fokusera på personuppgiftsbehandlingar som innebär en hög risk för de registrerades integritet.

Dataskyddsombudet ska rapportera till revisionsdirektören.

[1] Se art. 35 dataskyddsförordningen om konsekvensbedömning avseende dataskydd.
[2] Se art. 36 dataskyddsförordningen om förhandssamråd vid konsekvensbedömning avseende dataskydd.

STADSREVISIONEN | 2018-05-15

Bilaga 2 – Principer för integritets- och dataskydd i stadsrevisionens verksamhet

Göteborgs Stad

1

Principer för integritets- och dataskydd i Stadsrevisionen i Göteborgs verksamhet

Stadsrevisionen i Göteborg är en kommunal förvaltningsmyndighet i Göteborgs Stad.

Stadsrevisionen utgörs av 22 förtroendevalda revisorer utsedda av kommunfullmäktige och revisionskontoret som består av tjänstemän sysselsatta i funktioner som sakkunniga biträden och i funktioner för verksamhetsstöd. Revisionskontoret leds av en revisionsdirektör.

Enligt kommunallagen svarar de förtroendevalda för organisationen av sin egen förvaltning. Beslutande organ för stadsrevisionens förvaltning är revisorskollegiet som består av 11 av de förtroendevalda revisorerna.

Revisorskollegiet har antagit detta övergripande styrdokument, innefattande principer för integritetsskydd och hantering av personuppgifter i stadsrevisionens verksamhet i syfte att tydliggöra gällande krav på området i och med införandet av dataskyddsförordningen den 25 maj 2018.

Personuppgiftsansvar
Stadsrevisionen är personuppgiftsansvarig för all behandling av personuppgifter som sker inom ramen för dess verksamhet

Principer för integritetsskydd, hantering av personuppgifter och dataskydd
Dataskyddsförordningen innefattar såväl övergripande principer som detaljerade regler för integritetsskydd vid hantering av personuppgifter.

Stadsrevisionens hantering av personuppgifter ska alltid ske i enlighet med såväl dessa övergripande principer som de detaljregler som är relevanta för stadsrevisionen i egenskap av personuppgiftsansvarig.

Stadsrevisionen ska alltid lägga särskild vikt vid att säkerställa att det arbete med dataskydd som genomförs i organisationen genomsyras av att de registrerade individernas rättigheter är i fokus.

Offentlighetsprincipen
Stadsrevisionen omfattas av offentlighetsprincipen. Detta innebär att allmänna handlingar som upprättas hos eller inkommer till myndigheten som huvudregel är offentliga om de inte omfattas av sekretess.

Personuppgifter i sådana handlingar omfattas av särskilda regler i dataskyddsförordningen som innebär att personuppgifter som ingår i handlingarna kan bli offentliga.

STADSREVISIONEN | 2018-05-15

Stadsrevisionen
Postadress: Box 2141, 403 13 Göteborg
Besöksadress: Stora Badhusgatan 6, Göteborg
Kontaktcenter: 031-365 00 00, kansli: 031-368 07 00
stadsrevisionen@stadsrevisionen.goteborg.se

Göteborgs Stad