Stadsrevisionen

Göteborgs Stad

STADSREVISIONENS DATASKYDDSARBETE 2024

Dataskyddsombudets rapport

Innehållsförteckning

Inledning

Jag är utsedd av revisorskollegiet till dataskyddsombud (DSO) för stadsrevisionen i Göteborg. Jag har i denna roll övervakat och granskat stadsrevisionens dataskyddsarbete under 2024 och även understött verksamheten med information och råd.

Denna skriftliga rapport avseende min granskning är den femte i ordningen jag avlämnar och omfattar främst 2024. I vissa fall har jag valt att även redovisa iakttagelser från inledningen av 2025 med direkt koppling till 2024 års verksamhet.

Rapporten är något mindre omfattande än tidigare år. Det beror på att jag 2024 valt att begränsa de delar som baseras på omvärldsbevakning av dataskyddsområdet till frågor med tydligare anknytning till stads-revisionen och Göteborgs Stad framför den bredare omvärldsbevakning med generella faktagenomgångar som ingått i tidigare års rapporter.

2024 års rapport har disponerats enligt följande.

Efter denna inledning följer:

1. En översiktlig genomgång av händelser inom dataskyddsområdet under 2024. Genomgången görs som en redovisning av ett axplock av nyheter som dels fått viss uppmärksamhet under året, dels också främst har bäring på den offentliga förvaltningens förhållanden.

2. En beskrivning av stadsrevisionens arbete med informationssäkerhet och dataskydd under 2024.

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

Göteborg den 27 februari 2025

Anders Landkvist

1. Ett axplock av nyheter inom dataskydds-området 2024

Som berörts i inledningen av denna rapport har jag från 2024 valt att redogöra för ett antal mer framträdande nyheter under året med anknytning till stadsrevisionen och Göteborgs Stad. Nyheterna kommenteras i förhållande till stadsrevisionens verksamhet och förhållanden och då sist under varje delrubrik.

Förtydliganden om de registrerades rättigheter

Integritetslagstiftningen är ett regelverk till skydd för enskilda individers rättigheter till privatliv och integritet. Dessa rättigheter stärktes väsentligt i och med införandet av EU:s dataskyddsförordning 2018 (DSF).

Det är viktigt att läsa och tillämpa DSF med perspektivet att det är en skydds- och rättighetslagstiftning ***där skyddsintresset gäller och rättighetsinnehavarna är de registrerade***. Registrerad är den vars personuppgifter hanteras på något sätt i ett IT-system eller register.

Detta är tyvärr inte alltid självklart för den som driver en verksamhet av något slag med hjälp av IT-stöd i någon form. Det gäller dessutom i en tid då det torde vara svårt att finna någon offentlig eller kommersiell verksamhet som inte har någon form av IT-stöd kopplade till vad de gör.

I dataskyddssammanhang noteras gång på gång att verksamheter tenderar att prioritera DSF:s skydds- och rättighetsregler lägre än andra intressen för verksamheten. Det kan exempelvis handla om lönsamhets-, effektivitets- eller rentav arbetsmiljöintressen. Då detta görs utsätter sig verksamheten alltid för en risk för att få problem kopplat till regelverket för integritetsskydd.

En iakttagelse avseende 2024 är att det börjar komma fler och fler domar och beslut kopplade till just de registrerades rättigheter. Exempel på detta gäller förbud mot formkrav vid begäran om registerutdrag[1], bibehållen rätt för registrerad att få information raderad i rätt tid trots att begäran inkommit till fel e-postadress[2], rätt till skyndsamhet vid registrerads

[1] KR Sthlm mål: 2639–23 (Spotify). Artikel 12.
[2] Nederländska dataskyddsmyndigheten z2019-28 837 (APG). Artikel 17.1

begäran om tillgång,[3] rätt till insyn/villkor, radering och invändning[4] samt behandling utan laglig grund vid utskick av nyhetsbrev.[5]

Vilka är de registrerades rättigheter?

Vilka är då de rättigheter som den som hanterar personuppgifter (PU) i egenskap av personuppgiftsansvarig (PUA) har att tillgodose?

Den mest grundläggande rättigheten handlar om att en registrerad ska få lov att veta vilka PU någon behandlar avseende en själv. (Rätt till tillgång).

Europeiska dataskyddsstyrelsen (EDPB) beskriver syftet för och innehållet i de registrerades rätt till tillgång till sina personuppgifter på följande sätt:[6]

”Det övergripande syftet med rätten till tillgång är att tillhandahålla enskilda personer tillräcklig, öppen och lättillgänglig information om behandlingen av deras personuppgifter, så att de är medvetna om behandlingen, kan kontrollera att den är laglig samt kan kontrollera att de behandlade uppgifterna är korrekta. Detta kommer att göra det enklare – utan att vara ett villkor – för den enskilde att utöva andra rättigheter, t.ex. rätten till radering eller rättelse.

Rätten till tillgång enligt dataskyddslagstiftningen ska skiljas från liknande rättigheter i andra syften, till exempel rätten till tillgång till offentliga handlingar som syftar till att garantera insyn i offentliga myndigheters beslutsfattande och god förvaltningssed.

Den registrerade behöver däremot inte ange skäl för sin begäran om tillgång och det är inte den personuppgiftsansvariges sak att utreda huruvida denna begäran faktiskt kommer att hjälpa den registrerade att kontrollera att den relevanta behandlingen eller utövandet av andra rättigheter är lagliga.

---

[3] IMY-2023-15892 (SAS). Artikel 15 och IMY-2023-16127 (Ellos). Artikel 12.3 och 15.
[4] IMY 2023–13495 (Google). Artikel 12.2,17c och 21.1.
[5] IMY 2023–17151 (SAS). Artikel 6.1.
[6] EDPB Riktlinjer 01/2022 om registrerades rättigheter – rätt till tillgång Version 2.1 Antaget den 28 mars 2023 s.3 (citerad text har kursiverats).

Den personuppgiftsansvarige måste behandla begäran om det inte är uppenbart att begäran görs enligt andra regler än dataskyddsregler. Rätten till tillgång omfattar följande tre olika komponenter:

- *Bekräftelse av huruvida uppgifter om personen har behandlats eller inte.*
- *Tillgång till dessa personuppgifter.*
- *Tillgång till information om behandlingen, t.ex. ändamål, kategorier av uppgifter och mottagare, behandlingens varaktighet, de registrerades rättigheter och lämpliga skyddsåtgärder vid överföringar till tredjeland."*

Som också berörs i texten från EDPB följer ytterligare rättigheter med rätten till tillgång och insyn i de behandlingar som sker. Dessa är:

Rätt till radering av PU
Rätten att få sina PU raderade kallas ibland för rätten att bli bortglömd. Det innebär att en registrerad har rätt att vända sig till ett företag eller en myndighet eller den som behandlar dennes/as PU och begära att de raderas.

Rätten gäller inte då PUA exempelvis där en myndighet som enligt lag är skyldig att spara PU.

Rätt till rättelse av PU
PU som behandlas av företag, myndigheter och andra verksamheter ska vara korrekta och aktuella. En registrerad har rätt att få felaktiga uppgifter rättade. Man har också rätt att komplettera med relevanta personuppgifter som saknas hos PUA.

Den som är PUA har också själv ett ansvar för att regelbundet se till att uppgifterna är riktiga och uppdaterade.

Rätt till begränsning

Rätt till begränsning av behandling av PU handlar om att en registrerad i vissa särskilda situationer har rätt att kräva att behandlingen begränsas. Ett exempel på en sådan situation är om den registrerade anser att PU är felaktiga och att man begärt att de ska rättas. I den situationen har den registrerade också rätt att kräva att behandlingen (av de felaktiga PU) begränsas under utredningstiden/rättelsetiden.

Rätt att göra invändningar
Rätt att invända mot en PUA:s behandling av en registrerads PU får lov att göras när PU behandlas;

- för att utföra en uppgift av allmänt intresse, eller
- som ett led i myndighetsutövning, eller
- efter en intresseavvägning.[7]

PUA är skyldig att informera den registrerade om dennes rätt att invända. Informationen ska lämnas klart, tydligt och åtskilt från annan information. Den ska också lämnas senast vid det första kontakttillfället mellan registrerad och PUA.

Rättigheter när beslut fattas automatiskt

Vissa typer av PUA använder algoritmer för att fatta så kallade automatiserade beslut. Det innebär att en registrerads PU används i en automatiserad process för att fatta beslut som gäller personen i fråga.

När sådana beslut fattas måste PUA;

- informera om att beslutet är automatiserat och
- ge rätt för den det gäller att få beslutet granskat av en fysisk person och
- ge den det gäller möjlighet att bestrida beslutet.

Rätt att flytta PU (dataportabilitet)

Rätten att få flytta PU mellan olika PUA kallas i DSF för rätt till dataportabilitet. I situationer där PU behandlas med stöd av samtycke eller avtal kan en registrerad dels begära att få ut sina PU (för att kunna överföra dem till en annan PUA). Dels också begära att den PUA som har dem överför dem till en annan PUA om det är tekniskt genomförbart.

Ansvar för rättigheterna och ansvarsfördelning hos PUA

PUA ansvarar för att DSF följs i alla tillämpliga delar. PUA måste också kunna visa detta i samband med tillsyn av verksamheten.

[7] Rätten till invändning är enbart kopplad till de angivna laga grunderna. PU behandling på exempelvis de laga grunderna att fullgöra ett avtal eller samtycke omfattas därmed inte av rätten att invända.

De registrerades rättigheter är en grundläggande del av regelverket och därför måste alla PUA också organisera sina PU-behandlingar på ett sådant sätt så att rättigheterna kan upprätthållas. Enkelt uttryckt betyder det att en PUA alltid måste veta:

- Vilka IT-system och register som hanterar PU.
- Vilka PU som behandlas där.
- Att de PU som behandlas görs det i enlighet med regelverket.
- Att en registrerad som vill utöva sina rättigheter alltid kan få dem tillgodosedda.

För att klara av detta måste en PUA ha ett fungerande och kontinuerligt informationssäkerhetsarbete kombinerat med ett genomtänkt dataskyddsarbete. Inom ramen för dataskyddsarbetet behöver det vidare finnas både tekniska och organisatoriska lösningar för att säkerställa att de PU som behandlas också hanteras på ett korrekt sätt. I praktiken handlar detta både om att ha ändamålsenliga IT-system och kunniga medarbetare och arbetssätt som understödjer dataskyddsåtgärderna. Det handlar i slutänden alltid om att säkerställa att integritetsfrågorna i en verksamhet ges den vikt och betydelse DSF förutsätter att de ska ha.

Ansvaret för att detta uppnås vilar på den högsta ledningen. I en kommunal eller regional kontext betyder det att ansvaret vilar på den nämnd som är PUA. Hos stadsrevisionen innebär det revisorskollegiet. Ansvaret kan inte delegeras bort.

Ansvaret är också mycket långtgående. Enligt ett nytt rättsfall från EU-domstolen rörande skadeståndsansvar kan PUA inte ens undgå ansvar för brister med hänvisning till att anställda inte följt lämnade instruktioner på ett korrekt sätt. Detta visar på vikten av att alltid ta fram, tillämpa och följa upp instruktioner och arbetssätt för PUA.[8] Det är också av grundläggande betydelse att alltid utbilda medarbetare och chefer i en sådan utsträckning att de har rimliga förutsättningar att arbeta på ”integritetssäkert” sätt i verksamheten.

[8] EU domstolens dom av den 11 april 2024, mål C741/21 (immateriellt skadestånd).

Hur skyddas de registrerades rättigheter?

Reglerna för integritetsskydd gäller inom hela den Europeiska unionen. Varje medlemsstat har också en oberoende tillsynsmyndighet vars uppgift det bland annat är att bevaka att reglerna följs.

I Sverige är det Integritetsskyddsmyndigheten (IMY) som är tillsyns-myndighet. Vid konstaterade brister i följsamhet kan en PUA träffas av olika typer av korrigerande åtgärder och/eller sanktioner. Vid allvarligare brister kan kännbara sanktionsavgifter påföras.

En registrerad har alltid rätt att klaga på en PUA hos IMY och att få sitt klagomål utrett och prövat av myndigheten. Utredningsskyldigheten har klargjorts gälla via ett par nationella prejudicerande rättsfall i närtid.[9] Före dessa rättsfall utredde IMY inte alla klagomål, då man bedömde att det inte fanns en legal skyldighet att göra det. Numera utreds alla klagomål, vilket medfört en ökad arbetsbörda för myndigheten, men också ökade anslag.

Det faktum att alla klagomål nu måste hanteras av IMY kan sägas höja ”risknivån” för verksamheter som avviker från DSF:s regelverk vid kontakt med de registrerade och vid hantering av de registrerades rättigheter. Annorlunda uttryckt har risken att träffas av klagomål som kan leda vidare till tillsyn ökat, vilket varje PUA bör vara medveten om. PUA bör därför också se över de rutiner och arbetssätt som avser att säkerställa att de registrerades rättigheter tillgodoses.

Något som inte heller ska glömmas bort då det gäller överträdelser av DSF är att skadeståndsreglerna i artikel 82 ger registrerade rätt till skadestånd av den eller de PUA som behandlat deras PU om skada skulle uppstå. Även personuppgiftsbiträde (PUB) kan i vissa fall bli skadeståndsskyldiga. I svensk rättspraxis har den vanliga nivån på skadestånd legat upp till 5 000 kronor (främst kopplat till lagstiftningen före DSF), vilket kan tyckas blygsamt, men ska ses i kontexten att;

1) Det finns rättsfall från Europa som uttrycker att nivån på skadestånd enligt artikel 82 bör ha en avskräckande effekt och därför bör höjas i praxis. Detta kan påverka skadeståndsnivåerna framåt.

---

[9] Jfr HFD mål nr 6193–22 respektive 3691–22. Den 17 november 2023. Det finns även rättsfall från EU-domstolen.

2) Skadeståndsanspråk mot PUA kan framställas vid domstol av en registrerad, men också av större grupper av registrerade via grupptalan. En mer omfattande grupptalan som bifalls kan då innebära att betydande skadeståndsbelopp måste betalas av PUA.

Sammantaget måste därför PUA vara medveten om att överträdelser av DSF:s regelverk – då det gäller de registrerades rättigheter – både kan träffas av tillsynsmyndighetens olika korrigerande åtgärder/sanktioner samt skadeståndsanspråk från den eller de som lidit skada.

Kommentar runt stadsrevisionens förutsättningar att tillgodose de registrerades rättigheter.

Stadsrevisionen generella ”DSF-mognad” bedöms öka år från år. Detta följer av både utbildningssatsningar och granskningsinsatser av informationssäkerhets- och dataskyddsrelaterade risker hos Stadens verksamheter. Det följer också av det utvecklingsarbete av stadsrevisionens informationssäkerhetsarbete som pågått sedan 2020.

2024 har särskilda insatser också gjorts för att informera brett om hur stadsrevisionen behandlar personuppgifter via text på hemsida och informationslänkar i e-postsignaturer. Framåt behövs dock ett fortsatt och strukturerat arbete för att synlig- och medvetandegöra DSF:s funktion som skydds- och rättighetslagstiftning inom organisationen.

Stadsrevisionen arbetar också vidare med att utveckla och dokumentera rutiner och arbetssätt för att både understödja att verksamheten arbetar i linje med de grundläggande principerna för dataskydd och säkerställandet av de registrerades rättigheter. Det är viktigt att detta arbete fortgår och att även resultaten i form av rutiner och anvisningar systematiseras på ett överskådligt sätt i verksamheten.

Vikten av att veta vad ett IT-system gör med de PU som behandlas i det.

Det kan tyckas självklart att någon som använder IT-system för sin verksamhet som behandlar information, särskilt sådan som utgör PU, från första början säkerställer att man har kontroll över vad som hanteras i systemet. Det finns ett lagkrav enligt DSF att en PUA normalt sett i praktiken alltid ska göra en konsekvensbedömning för att identifiera

eventuella integritetsrisker för dem vars PU hanteras i ett IT-system eller register.[10]

Trots detta upptäcktes via incidentrapportering till IMY under 2021–2022 flera fall där PUA konstaterades ha haft bristande insikt runt och kontroll av funktioner hos den så kallade ”Metapixeln” på sina hemsidor. Detta fick till följd att information som bedömts utgöra känsliga PU överfördes till annan utan att PUA hade kontroll över det.

Företaget Meta som tillhandahåller ”Metapixeln” och bland annat äger och driver plattformarna Facebook och Instagram beskriver vad den är på följande sätt:[11]

”Meta-pixeln är ett kodstycke som placeras på din webbplats. Med hjälp av den kan du mäta hur effektiv din annonsering är genom att få en bättre förståelse för de åtgärder som utförs på din webbplats.
Detta kan du använda Meta-pixeln till:

- *Se till att dina annonser visas för rätt personer. Hitta nya kunder eller personer som har besökt en viss sida eller utfört en viss åtgärd på din webbplats.*
- *Öka försäljningen. Konfigurera automatiska bud för att rikta dig till personer som mer sannolikt utför en åtgärd som är viktig för dig, till exempel köper något.*
- *Mäta annonsernas resultat. Förstå effekten av dina annonser bättre genom att mäta vad som händer när personer ser dem.*

När du har konfigurerat Meta-pixeln registrerar den när någon utför en åtgärd på din webbplats. Exempel på åtgärder är att lägga till en vara i kundvagnen eller köpa något. Pixeln tar emot de här åtgärderna eller händelserna, och du kan se dem på sidan för din Meta-pixel i Händelsehanteraren. Därifrån kan du se vilka åtgärder som dina

[10] Jfr reglerna i DSF artikel 35–36 om konsekvensbedömning (DPIA) och förhandssamråd.
[11] Se vidare: Om Meta-pixeln | Meta Hjälpcenter för företag Citerad text har kursiverats.

kunder utför. Du har också möjlighet att nå dessa kunder igen med hjälp av framtida Meta-annonser.”

Bakgrunden var att två företag som drev apoteksverksamhet via internet haft ”Metapixeln” på sina hemsidor. Som framgår ovan är den ett analysverktyg med funktioner som registrerar vad besökare på hemsidan gör. Den kan därmed understödja företagets uppföljning av besökarnas aktivitet på hemsidan. Den innehöll dock också funktioner som överförde såväl kunders kontaktuppgifter som uppgifter om produkter som kunderna köpt i form av bland annat receptfria läkemedel för behandling av specifika hälsobesvär, självtester och behandling av könssjukdomar samt sexleksaker. Mottagaren av den överförda informationen var företaget Meta.

Syftet med ”Metapixeln” i denna del var att ge förutsättningar för det som kallas ”Automatic Advanced Matching” (AAM). AAM innebär att riktade annonser som matchar en viss användares köpbeteenden och intressen läggs ut till personen som enskild användare av Facebook/ Instagram då den använder dessa plattformar.

Funktionerna för AAM i ”Metapixeln” följde de parametrar som utformats av Meta så länge användarföretaget använde automatiskt konfigurering. Om användarföretaget å andra sidan valt manuell konfigurering kunde överföringarna av information styrts så att skyddsvärda data inte överfördes på samma sätt.

IMY inledde tillsyn då det blev känt att överföringar av PU skett från företagen på det sätt som beskrivits.

Myndighetens granskning visade att företagen inte vidtagit tillräckliga skyddsåtgärder för att skydda sina kunders PU. Bristerna bestod av att företagen inte vidtagit några tekniska åtgärder för att begränsa vilka uppgifter som fördes över till Meta. Företagen hade inte heller de rutiner som krävdes för att själva upptäcka bristerna. Överföringen av PU pågick därför under en längre tid och stoppades först efter att företagen fått kännedom om händelsen av utomstående. Antal registrerade var också omfattande. I det ena fallet omfattades en miljon registrerade, i det andra fallet omfattades 15 000 registrerade.

IMY beslutade i det första fallet att påföra sanktionsavgift om 37 miljoner kronor och i det andra fallet att påföra sanktionsavgift om 8 miljoner kronor.[12]

Kommentar runt stadsrevisionens ansvar för de PU-behandlingar som sker i system som används av verksamheten

De misstag som begicks vid uppsättningen av webbsidor då man inte hade full kontroll av vad ett programelement (”Metapixeln”) gjorde fullt ut visar på betydelsen av att ha ett riskbaserat synsätt så snart PU behandlas i IT-system. Om ett sådant riskbaserat synsätt funnits på plats borde ”Metapixeln” inte införts med mindre än att PUA säkerställt att konfigureringen av den inte medgav några överföringar av PU som man inte hade kontroll över.

Stadsrevisionens IT-miljö består till övervägande del av stads-gemensamma IT-system och IT-tjänster. Ansvaret för uppsättning av dessa ligger regelmässigt utanför stadsrevisionens kontroll.

Samtidigt är det viktigt att även stadsrevisionen alltid har en risk-medvetenhet om att IT-system, IT-tjänster liksom appar i telefoner och läsplattor kan dela information på ett olämpligt eller olagligt sätt. Det är därför av betydelse att framhålla att förtroendevalda och anställda enbart ska använda programvara i datorer, telefoner och läsplattor som installerats via Staden eller godkänts för installation av Staden.

Generellt gäller att en användare av IT-baserad teknik alltid ska vara försiktig med PU som läggs in i olika system. Detta gäller särskilt

---

[12] Se vidare IMY-2022-3270, beslut 2024-08-29 (Apoteket AB) respektive IMY-2022-3272, beslut 2024-08-29 (Apohem AB). Ytterligare tillsyner har också skett mot flera andra företag (Kry International AB, Länsförsäkringar AB och ytterligare 27 bolag inom Länsförsäkringsgruppen) där ”Metapixeln” överfört PU via företagens webbplatser. I dessa tillsyner har IMY konstaterat att DSF inte följts, men att det i dessa fall är fråga mindre överträdelser. Det beror bland annat på att bristerna inte har lett till överföring av några känsliga PU, uppgifter som omfattas av sekretess eller som annars är av mer skyddsvärd karaktär. Sammantaget innebar det att IMY stannat vid att utfärda en reprimand mot de företagen.

känsliga PU som också kräver särskilda skyddslösningar för att överhuvudtaget få lov att behandlas enligt DSF.

För användare i offentlig sektor tillkommer också den så kallade röjandeproblematiken, som även kan gälla annan information (som inte är PU) som omfattas av sekretess enligt offentlighets- och sekretesslagen (OSL). Den som förfogar över sådan information är också skyldig att skydda den från obehörig åtkomst via reglerna om tystnadsplikt i OSL. Tystnadsplikten är ytterst straffsanktionerad på individnivå.

Det är därför mycket viktigt att en offentlig verksamhet har god kontroll över de IT-system och de tekniska hjälpmedel som används i verksamheten. Det är också mycket viktigt att användarna av IT-systemen och de tekniska hjälpmedlen understöds av genomtänkta arbetssätt och goda egna insikter i vilka risker som finns och hur de ska begränsas.

Användning av AI i offentlig sektor

Artificiell intelligens eller AI som den vedertagna förkortningen lyder och dess inneboende möjligheter har varit mycket omtalade under 2024.

Uppmärksamheten runt AI fortsätter också från ingången av 2025 i takt med att både nya innovationer presenteras och olika risker med den ingående tekniken diskuteras.

Ett antal iakttagelser under 2024–2025 gäller att:

- AI-kommissionen har avlämnat sin rapport ”Färdplan för Sverige.”
- Allt fler oroas över att AI gör intrång i den personliga integriteten.
- Specifik lagreglering för AI börjar komma.
- Regeringen har beslutat om flera uppdrag rörande AI.
- EDPB har tagit fram yttrande om träning av och användning av AI modeller.
- IMY har genomfört flera vägledande aktiviteter runt AI.
- Göteborgs Stad har infört den AI-stödda tjänsten Copilot.

Utöver detta noteras att ett antal offentliga och privata aktörer är aktiva i och runt olika aspekter på införande och användning av AI.[13]

AI-kommissionen har avlämnat sin rapport ”Färdplan för Sverige”

AI-kommissionen, som tillsattes enligt ett regeringsuppdrag från 2023, har utarbetat vad de benämner ”Färdplan för Sverige” beträffande önskvärd eller av olika skäl nödvändig utveckling av Sveriges förhållande till AI och innovationer kopplade till AI.[14]

Kommissionen konstaterar i sin rapport att Sverige har goda förutsättningar för att utveckla och använda AI, både i kommersiella sammanhang och i fråga om effektivisering av den offentliga förvaltningen. Samtidigt uttrycks en stark oro över att Sverige inte gör tillräckligt för att placera sig i framkant av utvecklingen och att detta i sin tur innebär många risker att hamna ”efter” i utvecklingen, med konsekvenser för både näringsliv och välfärd som följd.

Kommissionen presenterar också en rad åtgärdsförslag med omfattande satsningar av olika slag för att säkerställa att utvecklingen ”går åt rätt håll” för Sverige. Man är i detta även väldigt tydlig med att det också är bråttom att satsningarna beslutas och genomförs.

Allt fler oroas över att AI gör intrång i den personliga integriteten

AI-kommissionens starka fokus på vikten av snabba och omfattande satsningar för att säkerställa att Sverige som nation inte hamnar ”efter” i utvecklingen av AI innebär dock inte att alla känner tillförsikt inför den nya tekniken.

---

[13] Exempel är Sveriges Kommuner och Landsting (SKR), Organisationen AI Sweden, ESam, med flera.
[14] Regeringen beslutade den 7 december 2023 att tillsätta en kommitté med uppdrag att identifiera behov av och lämna förslag på åtgärder som kan bidra till att stärka utvecklingen och användningen av artificiell intelligens (AI) i Sverige på ett hållbart och säkert sätt. Se vidare Kommittédirektiv 2023:164 Förstärkt AI-förmåga i Sverige. Kommittén tog senare namnet ”AI Kommissionen.”

I den riksomfattande och återkommande undersökningen ”Svenska Folket och AI”[15] konstateras att andelen svenskar som är positiva till AI är på en rekordlåg nivå. Undersökningen, som genomförts för sjunde året i rad, visar att andelen som är positiva till AI nu är på en lägstanivå jämfört med nivån i den första undersökningen (år 1 av 7).

Oron har ökat för att AI ska ta felaktiga beslut om en eller ge en felaktiga rekommendationer. Allt fler oroas också över att AI gör intrång i den personliga integriteten, nästan fyra av tio rankar det som sin främsta oro i undersökningen.

Specifik lagreglering för AI börjar komma

Under 2024 har viss lagreglering för utveckling och användning av AI börjat gälla eller beslutats Det handlar då om rättsakter på EU nivå i form av AI-förordningen[16] och EHDS förordningen[17].

AI-förordningen har börjat gälla[18] och är uppbyggd för att skapa en uppdelning av AI-system utifrån deras användningsområden och risker med dessa. Vissa användningsområden anses så riskabla att de är förbjudna.[19] Andra användningsområden är tillåtna men med vissa anpassningar och krav utifrån om AI-systemen anses medföra hög[20], liten eller ingen risk.[21] Utöver risknivån ställer förordningen olika krav

[15] Undersökningen är framtagen av företaget Insight Intelligence tillsammans med IMY, Myndigheten för digital förvaltning (DIGG), organisationerna eSam och Bonus Copyright Access.
[16] EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2024/1689 av den 13 juni 2024 om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (förordning om artificiell intelligens).
[17] European Parliament legislative resolution of 24 April 2024 on the proposal for a regulation of the European Parliament and of the Council on the European Health Data Space (COM(2022) 0197 – C9-0167/2022 – 2022/0140 (COD).
[18] Reglerna ska börja tillämpas vid olika tidpunkter från den 1 augusti 2024 – med det första ikraftträdandet av förbjudna områden inom 6 månader och efterföljande delar av regleringen inom 12, 24 respektive 36 månader.
[19] Exempel är manipulation för att medvetet skada någon psykiskt eller fysiskt.
[20] Exempel på hög risk innefattar AI-användning inför livsavgörande beslut så som för studier och anställning. Sådan användning kräver kontroll av regelefterlevnad och registrering hos ansvarig myndighet.
[21] AI-system som anses innebära liten eller ingen risk får med vissa undantag användas utan restriktioner.

beroende på vilken roll och vilket ansvar en aktör har i AI-systemets värdekedja (utvecklare - användare). Vidare ska system för styrning och kontroll av efterlevnad införas på både nationell och EU-nivå. Slutligen ställs krav på etablering av s.k. regulatoriska sandlådor i syfte att främja innovation och effektivisera regelefterlevnad.

AI-förordningen gäller som svensk lag men förutsätter kompletterande nationella bestämmelser. Dessa kommer att tas fram enligt regeringens beslut att tillsätta en utredning för detta den 19 september 2024.[22] Av kommittédirektiven framgår att utredningen ska föreslå nödvändiga lagändringar samt åtgärder för insyn och kontroll. Vidare ska de föreslagna nationella reglerna sträva efter att främja innovation och tillväxt genom AI-användning, särskilt för mindre aktörer inom privat och offentlig sektor. Slutredovisning av uppdraget ska ske senast den 30 september 2025.

EHDS-förordningen har antagits av EU-parlamentet under inledningen av 2025 och handlar om hantering av patienters hälsodata inom EU.[23] Under förordningens reglering ska olika vårdgivare inom unionen kunna koppla samman sina organisationer och system för att underlätta ett säkert och tillförlitligt utbyte av hälsodata vid gränsöverskridande hälso- och sjukvård inom EU.

Reglerna talar dels om primäranvändning, dels om sekundäranvändning av hälsodata. Primäranvändning innebär den datadelning som sker hos hälso- och sjukvården inom och mellan vårdgivare och där patienten själv också ska ges tillgång till och kontroll över sin elektroniska hälsodata. Sekundäranvändning innebär när pseudonymiserade eller avidentifierade hälsodata återanvänds i annat, sekundärt syfte, till exempel för forskning, innovation, folkhälsa eller för beslutsfattande.

I det senare fallet, då hälsodata används i sekundärt syfte kan viss problematik runt användning av AI – typiskt sett inom forskning eller innovation - att aktualiseras. Även i fråga om EHDS kommer det att behöva tas fram nationella regler.

Det är viktigt att notera att DSF gäller parallellt med den nya lagregleringen. Behandling av PU inom ramen för AI – som i sig är reglerat av de två förordningarna som diskuteras ovan – måste som

[22] Kommittédirektiv: 2024:83 ”Trygg och tillförlitlig användning av AI.”
[23] Förordningen kommer att börja gälla från våren 2026.

huvudregel alltid ske harmoniserat mot DSF:s integritetsskyddande regler. Exempelvis måste AI-system (som styrs av AI-förordningen) och behandlar PU, fortfarande göra detta med iakttagande av DSF:s krav på laglig grund, korrekthet och ändamålsbegränsning.

Detsamma torde gälla vid sekundäranvändning av hälsodata (som då styrs av EHDS) där DSF:s integritetsrättsliga krav (eller motsvarande integritetsrättsliga krav i speciallag för hälsoområdet) och definitioner av pseudonymisering eller avidentifiering behöver iakttas vid PU-behandling.

Regeringen har beslutat om flera uppdrag rörande AI

Som berörts ovan har regeringen under 2024 beslutat om uppdrag att ta fram nationella bestämmelser för tillämpningen av AI-förordningen. Utöver detta har ett särskilt uppdrag lämnats till IMY och DIGG att ta fram riktlinjer för användningen av generativ artificiell intelligens (AI) inom den offentliga förvaltningen.[24] Uppdraget innefattade att;

”ta fram riktlinjer i syfte att främja att generativ AI används inom den offentliga förvaltningen på ett effektivt, säkert och etiskt sätt. Riktlinjerna ska fungera som en vägledning och ett stöd vid användning av generativ AI för anställda på statliga myndigheter, kommuner och regioner utifrån juridiska, säkerhetsmässiga och etiska perspektiv.

För att öka AI-tillämpningen inom den offentliga förvaltningen är det även viktigt att personer i ledningsfunktion har tillgång till det stöd som behövs för att nyttja tekniken. Riktlinjerna ska därför även fungera som ett metodstöd och utifrån juridiska, säkerhetsmässiga och etiska aspekter ge vägledning för verksamheternas bedömningar av om, och i så fall hur, generativ AI ska användas.”

[24] Regeringsbeslut: Fi2024/01535 ”Uppdrag till Myndigheten för digital förvaltning och Integritetsskyddsmyndigheten att ta fram riktlinjer för användningen av generativ artificiell intelligens inom den offentliga förvaltningen.”

De framtagna riktlinjerna presenterades den 21 januari 2025 varvid DIGG och IMY konstaterade att:

”– Riktlinjerna ska fungera som vägledning och metodstöd. Vi vill bidra till tryggare AI-användare för att skapa enklare, bättre och mer effektiv offentlig förvaltning.”

Respektive:

”– Integritetsfrågorna behöver identifieras och hanteras tidigt i processen när AI ska införas. Vi hoppas att riktlinjerna ger värdefull vägledning för att kunna ta vara på möjligheterna med generativ AI på ett sätt som värnar integritet.”

Myndigheterna konstaterar vidare att riktlinjerna, mot bakgrund av den snabba teknikutvecklingen, kommer att vara föremål för utveckling framöver. I dagsläget finns 18 riktlinjer publicerade som täcker områdena: Ledning och ansvar, Informationssäkerhet, Upphovsrätt, Dataskydd, Etik, Arbetsrätt och Anskaffning. Riktlinjerna finns tillgängliga på DIGG:s webbplats.[25]

En bärande idé i riktlinjerna är att en verksamhet som vill använda sig av generativ AI i förväg behöver fastställas hur det ska användas och till vad. Detta behöver också beslutas av verksamhetens ledning, då den är ytterst ansvarig för att verksamheten bedrivs inom lagens ram. Fastställandet/beslutandet kan med fördel ske genom framtagande och antagande av styrdokument – exempelvis en AI-policy, eventuellt kompletterad av en AI-strategi.

Regeringen har även tidigare lämnat uppdrag till IMY att följa, analysera och beskriva utvecklingen på IT-området när det gäller frågor som gäller integritet och ny teknik. Redovisning ska ske vart

[25] Se vidare: https://www.digg.se/ai-for-offentlig-forvaltning/riktlinjer-for-generativ-ai

fjärde år och redovisning för perioden 2020–2024 har nyligen publicerats i form av en rapport i inledningen av 2025.[26]

Rapporten konstaterar att den personliga integriteten påverkats mycket av samhällets digitalisering och den snabba teknikutvecklingen. Den ökande insamlingen av data om människors beteenden och rörelsemönster, både på via internet och i den fysiska världen, skapar risker ur ett integritetsskyddsperspektiv. I rapporten konstateras också att utvecklingen de senaste åren gått mot att de brottsbekämpande myndigheterna ges möjlighet att använda teknik i större omfattning. Det handlar då till exempel om utökad kamerabevakning, ökad användning av biometri och stöd av AI i det brottsbekämpande arbetet. Övervakningen i arbetslivet har också förändrats i takt med nya tekniska möjligheter.

Även om teknikutvecklingen kan vara svaret på många stora utmaningar som samhället står inför så menar IMY att det finns integritetsrisker i utvecklingen den utveckling vi ser. Myndigheten anser också att det finns många sätt att förbättra integritetsskyddet i samhället utan att det hämmar innovation och ekonomisk utveckling eller lägger hinder mot ökad effektivitet. Det behövs dock mer vägledning och forskning om integritetshöjande teknik, för att minska osäkerhet runt regelverken och öka konkurrenskraften.

IMY konstaterar slutligen också att det nu snart gått sju år sedan DSF började tillämpas och att vi sedan dess sett en rekordsnabb teknisk utveckling. En slutsats i rapporten är därför att tiden är mogen för en översyn av DSF.

EDPB har lämnat yttrande om träning av och användning av AI-modeller

AI-modeller tränas genom att de läser och analyserar stora datamängder. Om dessa innefattar PU omfattas träningen av det integritetsrättsliga regelverket eftersom träningen i sig utgör en PU behandling. Detsamma kan gälla vid användning av en AI-modell där

[26] IMY Dnr IMY-2024-2570 Integritet och ny teknik. Redovisning av integritetsmyndighetens uppdrag att följa, analysera och beskriva utvecklingen 2025-01-25.

en användare låter AI-systemet läsa in och behandla data av olika slag om där också ingår PU.

Detta behöver inte vara otillåtet enligt regelverket, men som med all annan PU behandling krävs det att den utför den (och då är PUA) har kontroll på vad som sker, att det är i enlighet med regelverket och exempelvis då de registrerades rättigheter kan tillgodoses.

Företagen Meta och X har använt PU syfte att träna AI-modeller och den irländska dataskyddsmyndigheten har mottagit klagomål om detta. Myndigheten har därefter vänt sig till EDPB och begärt att organisationen ska yttra sig över hur man ser på träning och användning av AI-modeller.

EDPB har därefter tagit fram ett yttrande i saken[27] som antogs i december 2024 där det konstaterades;

1) I fråga om anonymisering i en AI-modell respektive

2) vilka följderna blir av att kraven på rättslig grund och de grundläggande principerna inte följts då AI-modellen tagits fram, att:

- Det krävs att PU för att anses vara anonymiserade det är osannolikt att någon ska kunna identifiera enskilda personer vars uppgifter användes för att skapa AI-modellen och att någon ska kunna få fram PU vid sökningar som sker med hjälp av AI-modellen. EDPB erinrade i samband med detta också om att en bedömning alltid måste ske i varje enskilt fall. EDPB presenterade även en lista med förslag på kriterier som kan användas för att visa att uppgifterna är anonymiserade. Samt;

- att en AI-modell som tagits fram med PU som behandlats olagligt kan få effekt för den fortsatta användningen av

[27] Se vidare EDPB: Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models Adopted on 17 December 2024.

modellen. (Det vill säga att en olagligt framtagen modell kan vara olaglig att använda vidare.)

Följden blir att den som utvecklar eller använder en AI-modell som omfattar PU och som inte har ”full kontroll” över att den då inte bryter mot DSF – vare sig vid utvecklingen eller vi användningen –riskerar att bryta mot det integritetsrättsliga regelverket.

Det ska tilläggas att både Meta och X enligt uppgift nu har upphört att träna AI-modeller med data från EU-området där DSF gäller.

IMY har genomfört flera vägledande aktiviteter runt AI

IMY har tagit fram både vägledningar och en rapport om användning av AI som stöd vid utlämning av allmänna handlingar.

Vägledningarna finns att nå via IMY:s hemsida och består av två delar. En del (1) som beskriver hur AI tekniskt fungerar och tränas och en del (2) som beskriver de rättsliga aspekterna på användning av AI.[28]

Rapporten om användning av AI som stöd vid utlämning av allmänna handlingar är en del av ett projekt i IMY:s s k regulatoriska sandlåda som undersökt möjligheterna att stödja upprätthållandet av offentlighets-principen med hjälp av koncept för AI-baserade hjälpmedel. Centrala frågor som undersöktes var dels möjligheten att utveckla en automatiserad funktion för utlämningsprövning av allmänna handlingar (helhetstjänsten) och en dels en mer begränsad funktion som i stället enbart skulle ge maskeringsstöd för handläggare (maskeringstjänsten). Den senare bestod i förslagsstöd för hur ”maskning” av sekretesskyddade uppgifter i utlämnade allmänna handlingar ska göras.[29]

Projektets slutsats var att mycket talade *emot* att den undersökta helhets-tjänsten inte var genomförbar inom ramen för gällande integritetsrättsliga regelverk, särskilt då träningen av AI-modellen skulle komma att omfatta

[28] Vägledningarna nås via följande länk: https://www.imy.se/verksamhet/dataskydd/innovationsportalen/vagledning-om-gdpr-och-ai/

[29] IMY Dnr IMY-2024-5156 Utlämnande av allmänna handlingar med hjälp av AI, Slutrapport från integritetsmyndighetens regulatoriska sandlåda om dataskydd.

känsliga och i övrigt skyddsvärda PU i stor omfattning. I fråga om maskeringstjänsten – som i användarledet även omfattade en mänsklig handläggare och beslutsfattare – så bedömdes den däremot vara genomförbar.

En annan slutsats var att det är mycket viktigt att AI-tjänster eller system generellt utvärderas noga innan de tränas eller används med avseende på risk och säkerhet för sådana PU som kan komma att behandlas i dem.

Göteborgs Stads införande av den AI-stödda tjänsten Copilot

Aktuella händelser i Göteborgs Stad utgör ett fall ur verkligheten om hur lansering av AI-baserad teknik kan gå fel.[30] Fallet har en tydlig koppling till stadsrevisionen då man omfattas av den kommungemensamma IT-miljön som tillhandahålls av nämnden för intraservice (intraservice). Risker kopplade till intraservice uppdrag är också ett återkommande riskområde i revisorernas riskanalys.

- Göteborgs Stad använder webbläsaren Edge från företaget Microsoft. Under början av 2024 aktiverades funktionen Microsoft Copilot (Copilot) i webbläsaren.

- Copilot är vad som kallas ett AI-baserat effektivitetsverktyg som avser att underlätta och effektivisera en användares arbete. I samband med att funktionen gjordes tillgänglig i stadens IT-miljö tog Stadens DSO[31] kontakt med förvaltningen för intraservice med frågor om avtal och vilka bedömningar som gjorts inför att funktionen aktiverades.

[30] Redogörelsen är baserad på Dataskyddsombudets rekommendation gällande Microsoft Copilot i Edge av den 23 januari 2025 till förvaltningar och bolag i Göteborgs Stad samt anknytande e-post kommunikation från Nämnden för intraservice som inkommit till Stadsrevisionen.
[31] Stadens DSO finns vid en särskild avdelning, avdelningen för dataskydd, hos nämnden för intraservice. Stadens DSO övervakar följsamhet mot DSF och ger råd och stöd i fråga om dataskydd till Stadens verksamheter med undantag för Stadsrevisionen. Kommunstyrelsen och stadsledningskontoret har också funktioner för dataskydd som hämtats från intraservice avdelning för dataskydd. Stadsrevisionen har eget DSO främst med hänvisning till revisorernas oberoende i förhållande till Stadens organisation.

- DSO ska enligt DSF:s artikel 38.1 på ett korrekt sätt och i god tid delta i alla frågor som rör skyddet av personuppgifter. DSO ska informera, ge råd och utfärda rekommendationer till PUA eller PUB.

- Det konstaterades då att intraservice inte genomfört någon riskanalys utifrån ett informationssäkerhets- och dataskyddsperspektiv samt inte heller kunde besvara dataskyddsombudets frågor gällande avtal runt funktionen. Mot bakgrund av detta rekommenderades förvaltningen den 12 april att omgående vidta åtgärder för att inaktivera funktionen Copilot i Edge. Förvaltningen rekommenderades samtidigt även genomföra en risk- och sårbarhetsanalys för Copilot och som en del i det ta fram ett tekniskt underlag beskrivande hur tjänsten fungerar.

- Efter detta följde ett drygt halvår av dialoger mellan DSO och intraservice. Delar av dialogen innefattade även leverantören Microsoft. Syftet med dialogerna var att främst få svar på frågor som gällde PU-hanteringen i funktionen.

- I november bedömde DSO att det fortfarande fanns risker kopplade till användning av funktionen Copilot. För verksamheter i Staden var de största riskerna att Copilot kunde användas i Outlook via webbläsaren samt att det saknades kunskap om vilka webbdelar/ applikationer som Copilot kunde få tillgång till.

- När det gällde relationen gentemot Microsoft bedömdes oklara ansvarsförhållandena för PU-behandlingarna och obesvarade frågor om delning av data vara de främsta riskerna.

- Den 27 november rekommenderade DSO därför Intraservice återigen att omgående vidta åtgärder för att inaktivera funktionen Copilot samt göra en fullständig risk- och sårbarhetsanalys för Copilot där tjänsten kartlades och ansvarsförhållanden tydliggjordes.

- Den 20 december fick DSO kännedom om att information i webbdelarna av socialförvaltningarnas verksamhetssystem kunde nås av Copilot. Detta kunde konstateras efter att tester genomförts i testmiljöer utan riktiga PU.

- Då det i dessa system finns känsliga och särskilt skyddsvärda personuppgifter kontaktade DSO intraservice den 23 december för att informera om problemet och utifrån de risker som det innebar, att återigen rekommendera förvaltningen att inaktivera Copilot i Edge samt genomföra en ordentlig riskanalys.

- I inledningen av januari 2025 hålls möten mellan DSO och intraservice för att ha samtal kring Copilot och rekommendationen som lämnades den 23 december. Mötena ledde till att DSO den 23 januari 2025 slutligen utfärdade en stadsövergripande rekommendation riktad till förvaltningar och bolag i Göteborgs Stad. Rekommendationen konstaterade:

    - Att Copilot kunde användas i webbapplikationer som hanterade extra skyddsvärda och känsliga personuppgifter samt uppgifter som omfattades av sekretess.

    - Att DSO med anledning av detta menade att information riskerade att röjas till Microsoft i de fall en användare av ett sådant system skulle använda Copilot och/eller ställa frågor gentemot informationen i systemet med hjälp av Copilot.

    - Att lättillgängligheten till Copilot innebar stora risker för felaktig hantering av personuppgifter och ett röjande till Microsoft. Dessa risker bedömdes också ha ökat efter uppdateringen av M365-apparna (januari 2025) som medfört att Copilot nu både fanns tillgänglig som en app samt visades som ett alternativ när användare högerklickade på en webbsida och/eller i en webbaserad PDF.

    - Att DSO därför uppmanade intraservice att stänga Copilot och att genomföra kartläggande åtgärder respektive informera Stadens verksamheter. Stadens verksamheter uppmanades även att omgående vidta åtgärder för att inaktivera funktionen Copilot i Edge.

- Den 29 januari meddelade intraservice att man beslutat att tillfälligt stänga funktionen Copilot för hela Staden och starta en utredning om hur säkerheten kan förbättras. Under utredningen kommer funktionen att vara stängd.

Ovanstående visar hur det kan gå om integritetsrättsliga perspektivet inte finns med ordentligt då nya tekniska funktioner eller tjänster introduceras.

Det är utan tvivel så att Copilot kan vara ett nyttigt verktyg i många verksamheter. Samtidigt är det för en PUA helt grundläggande att man innan man börjar använda ett sådant verktyg säkerställer att användningen är laglig. I det aktuella fallet så visste varken intraservice eller Stadens verksamheter vilka risker som användningen av funktionen kunde medföra, eftersom man inte gjort någon riskanalys före driftsättning. Detta innebär i sig en bristande följsamhet mot DSF eftersom Copilot i det utförande som driftsattes definitivt torde ha utlöst

skyldighet att genomföra tröskelanalys och konsekvensbedömning enligt artikel 35. Intraservice har inte heller involverat Stadens DSO före driftsättningen vilket man också skulle ha gjort enligt regelverket.[32] Hade man gjort det hade utvecklingen i ärendet kanske sett annorlunda ut.

Användningen av Copilot kan slutligen innebära att inte bara PU och känsliga PU hanteras på ett bristfälligt sätt i förhållande till DSF:s regler. Det kan också innebära att uppgifter som inte är PU men som omfattas av sekretess enligt offentlighets- och sekretesslagen (OSL) röjs för utomstående i strid med denna lag. Enligt OSL ska sekretesskyddade handlingar och uppgifter som huvudregel skyddas från obehörig åtkomst.[33] Bearbetning i molnet – som av allt att döma används av Microsoft för att tillhandahålla funktionen Copilot – kan innebära att bearbetad sekretesskyddad information röjs i strid med OSL:s regelverk.

Sammantaget framstår därmed intraservice bristande riskanalysarbete vid lanseringen av Copilot som anmärkningsvärt. Detsamma gäller den kvarstående osäkerhet som uppenbarligen finns runt risk för spridning av PU och röjande av sekretesskyddad information om tjänsten används.

Kommentar runt stadsrevisionens förutsättningar att använda AI i verksamheten

Stadsrevisionens verksamhetsplan 2025 konstaterar att en omvärldsanalys, beträffande AI och i vilken mån det används i revisionsarbete vid andra kommunala revisionskontor och riksrevisionen genomförts under 2024. Under 2025 planeras ett fortsatt arbete för att undersöka vilka AI-verktyg revisionskontoret skulle kunna använda i sin revisionsverksamhet.

Detta framstår som en klok åtgärd. Den bör dock följas av ytterligare åtgärder för att begränsa risker kopplat till en för snabb och okontrollerad användning av AI i verksamheten.

Som beskrivits ovan rekommenderar DIGG och IMY att det finns en tydlig ledning och styrning kopplad till IT-baserad teknik som använder AI. En fri och experimentell användning av AI-verktyg av enskilda

---

[32] Jfr. DSF artikel 38.1.
[33] Jfr. OSL Kap. 8 1 §.

medarbetare bör därför inte förekomma med hänvisning till de integritets- och sekretessrelaterade risker som kan följa med det.

En lämplig väg framåt synes därför vara att stadsrevisionen – innan AI-baserad teknik används i verksamheten – gör en generell riskanalys över vilka PU-behandlingar, respektive vilka behandlingar av sekretesskyddad information som sker. Denna riskanalys kan därefter läggas till grund för lämpliga styrdokument för användning av AI i verksamheten. Dessa bör då reglera hur träning av AI-baserade verktyg får ske och hur de i tränat/utvecklat skick får och ska användas. Stöd och vägledning för arbetet kan exempelvis inhämtas från material som framtagits och publicerats av IMY och DIGG.

Höjda krav på informations- och cybersäkerhet framåt för vissa verksamheter

NIS[34] direktivet (NIS1) är ett EU-direktiv som antogs 2016. Det införlivades i svensk rätt 2018.[35] Regleringen gäller krav på informationssäkerhet i nätverk och IT-system för samhällsviktiga tjänster inom sektorer för;

- energi
- transport
- bankverksamhet
- finansmarknadsinfrastruktur
- hälso- och sjukvård
- leverans och distribution av dricksvatten
- digital infrastruktur, och
- digitala tjänster.

NIS2-direktivet beslutades av EU i december 2022 och ersätter NIS-direktivet från 2016. Samtidigt fattades även beslut om direktivet om kritiska entiteters motståndskraft, CER. I direktivet ställs krav på all annan verksamhet som måste kunna upprätthållas vid olika typer av

[34] NIS utläses “Network and Information Systems.”
[35] Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS-lagen) och genom Förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster.

störningar. Det kan handla om skydd av fysisk säkerhet som exempelvis lokaler och anläggningar och att rätt personer har åtkomst till dessa.

De nya direktiven ska införas i svensk lagstiftning via den s k cybersäkerhetslagen som är under beredning. Det antas komma en proposition under våren 2025. Så här långt finns det en statlig utredning (SOU 2024:18) som tagit fram lagförslag.

Den som omfattas av NIS2 kallas verksamhetsutövare. Verksamhetsutövarna finns i 18 olika sektorer. Det innebär då betydlig fler sektorer än de som omfattas av NIS-lagen idag. De exakta kriterierna för vilka som ska omfattas i Sverige är inte klara ännu.

För varje sektor ansvarar en eller flera tillsynsmyndigheter för vägledning och tillsyn. Tillsynsmyndigheterna har också rätt att utfärda föreskrifter som reglerar kraven i respektive sektor. Eftersom NIS2 täcker fler sektorer än NIS1 krävs en större tillsynsorganisation än tidigare. Av den anledningen tillkommer fler tillsynsmyndigheter. Sanktionsavgifterna blir också högre än dagens nivåer om kraven inte efterlevs.

NIS2 kräver tydligare krav på bland annat riskanalyser och olika säkerhetsåtgärder. Det krävs ett dokumenterat riskbaserat och systematiskt informationssäkerhetsarbete. Direktivet ställer även ökade krav på ledningens deltagande i organisationens cybersäkerhetsarbete jämfört med tidigare. Exempelvis krävs det att ledningen ska godkänna och övervaka verksamhetens riskhanteringsåtgärder för cybersäkerhet.

Det underliggande syftet med de nya direktiven är att uppnå en hög gemensam nivå av cybersäkerhet i hela EU.

Kommentar runt stadsrevisionen och höjda krav med anledning av införlivandet av NIS2 och CER-direktiven i svensk rätt

Införlivandet av de nya EU-direktiven kommer att ställa högre krav på flera samhällsviktiga verksamheter än NIS-lagens nuvarande regler. Det kommer att bli fler verksamheter som träffas av reglerna eftersom antalet sektorer som omfattas ökar.

Intressant är att en av de nya sektorerna är ”offentlig förvaltning.” (och då utöver de offentliga verksamheter som träffas av särskilda sektorer för energi, dricksvatten, avloppsvatten, avfallshantering osv.) Vilka ytterligare delar av den ”offentliga förvaltningen” som då kommer att träffas av reglerna är inte helt klart. Utredningen resonerar runt att

statliga myndigheter kanske kommer att träffas i första hand, men landar inte i något entydigt svar. Här får man avvakta och se vad propositionen föreslår då den kommer. Klart är emellertid att de verksamheter som kommer att omfattas – vilket i vart fall torde vara de verksamheter som idag omfattas av NIS-lagen -också kommer att behöva se över sitt informationssäkerhetsarbete. De kommer också att behöva säkerställa att respektive ledning blir djupare involverade i cybersäkerhetsarbetet i enlighet med det nya regelverkets krav. Det bör beaktas i revisorernas riskanalysarbete framåt för verksamheter i Göteborgs Stad som omfattas.[36]

Dataskyddsombudens ställning

EDPB genomförde 2023 en samordnad undersökning runt dataskydds-ombudens roll och ställning i medlemsstaterna. IMY deltog i under-sökningen och har följt upp de nationella iakttagelserna om för-hållandena i Sverige via en riktad tillsyn under 2024.

Vid tillsynen granskades fem organisationer för att se om det förelåg intressekonflikt genom att dataskyddsombuden hade andra uppdrag i den granskade verksamheten.[37] Vidare kontrollerades ytterligare en organisation för att se om DSO hade den roll och de resurser som krävs för att utföra uppdraget. Tillsynen utgick därmed från DSF:s artikel 38 och kraven på DSO:s oberoende respektive resurstilldelning.

I ett av fallen bedömde IMY att det förelåg en intressekonflikt genom att DSO hade i uppdrag att som regionjurist ge råd i dataskyddsfrågor till verksamheten utöver vad som kunde anses ingå i DSO-uppdraget. IMY ansåg att DSO därmed tvingades granska det dataskyddsarbete som utförts som rådgivare, vilket då gjorde att oberoendet kunde ifrågasättas.[38]

I granskningen av DSO:s roll och resurser konstaterades att verksamheten bland annat inte säkerställt att dataskyddsombudet i god tid deltog i alla

[36] Exempel är Göteborg Energi AB, Göteborgs Hamn AB och Nämnden för kretslopp och vatten.
[37] De organisationer som granskades var: Hemköpskedjan AB, PostNord Sverige AB, Regionstyrelsen i region Västerbotten, Socialnämnden i Stockholms Stad, Socialnämnden i Örebro kommun och Swedavia AB.
[38] Dnr IMY-2023-7987 - Regionstyrelsen i Region Västerbotten, korrigerande påföljd: Reprimand och föreläggande.

frågor som rör skyddet av PU eller att ombudet rapporterade direkt till den högsta förvaltningsnivån.[39]

Tillsynen mot övriga verksamheter föranledde ingen kritik eller synpunkter.

Kommentar angående DSO:s ställning vid stadsrevisionen

Stadsrevisionen har sedan 2023 en etablerad funktion med en tjänsteperson utsedd till dataskyddsansvarig (DSA) som leder och ansvarar för dataskyddsarbetet. DSO lämnar råd och stöd till DSA eller organisationen i övrigt utifrån uppdraget så som det är definierat i DSF. Det är viktigt att rollfördelningen upprätthålls och alltid synliggörs i det löpande arbetet. Det bedöms inte föreligga någon påtaglig risk för intressekonflikter i dagsläget.

DSO bedöms också i dagsläget ha tillräckliga resurser och vara tillräckligt involverad i stadsrevisionens frågor kopplade till PU-behandlingar och dataskydd i förhållande till DSF:s regler.

[39] Dnr IMY-2023-7963 - Socialnämnden i Örebro kommun, korrigerande påföljd: Reprimand.

2. Stadsrevisionens arbete med informationssäkerhet och dataskydd 2024

I uppdraget som DSO ingår att övervaka stadsrevisionens följsamhet mot DSF:s regelverk.

Detta görs löpande under varje verksamhetsår i det att råd och stöd lämnas i informationssäkerhets- och dataskyddsfrågor till i första hand stadsrevisionens dataskyddsansvariga tjänsteperson (DSA), men vid behov även till organisationen i övrigt. Det görs också via en samlad granskningsinsats vid verksamhetsårets slut. Granskningsinsatsen har som mål att sammanfatta hur utvecklingen av informationssäkerhets- och dataskyddsarbetet sett ut under året och även att uppmärksamma risk- eller förbättringsområden.

Övervakningen av verksamhetsåret 2024 har liksom tidigare år följt detta arbetssätt. Jag kommer nedan och efter en kort summering av stadsrevisionens tidigare arbete 2019–2023 med att utveckla informationssäkerhetsarbetet att redogöra för iakttagelserna från 2024 års övervakning.

Kort summering av stadsrevisionens arbete under 2019-2023 att utveckla sitt informationssäkerhetsarbete

Som har beskrivits i tidigare DSO-rapporter inledde stadsrevisionen 2019 ett arbete med att utveckla sitt informationssäkerhetsarbete och därmed också att stärka förutsättningarna för ett effektivt dataskyddsarbete. Styrande för arbetet har varit den handlings- och färdplan som utarbetades 2020 som identifierade prioriterade fokusområden som behövde hanteras. Dessa var i tur och ordning:

- Kompetensutveckling
- klassning av information
- framtagande av systemförteckning
- utveckling av rutiner och arbetssätt och
- synkronisering av informationssäkerhetsarbete mot övrigt säkerhetsarbete.

Min bedömning är att dessa fokusområden nu hanterats så väl det går i det övergripande utvecklingsarbete som utgick från handlings- och färdplanen från 2020. Planen får därmed anses vara genomförd.

Stadsrevisionens organisatoriska informationssäkerhets- och dataskyddsmognad får också anses ha ökat väsentligt under åren 2020–2023 till följd

av såväl utbildningsinsatser, genomförd granskning inom informationssäkerhetsområdet och utveckling av arbetssätt. Detta är positivt och skapar och förutsättningar för en fortsatt och nödvändig utveckling.

Ny teknik, ett osäkert omvärldsläge och tydliga styrsignaler från såväl nationell som lokal nivå om behovet av en effektivare och säkrare informationshantering hos myndigheter och andra verksamheter innebär dock fortsatta stora utmaningar. Det innebär också krav på resurser i form av kompetens och arbetstid hos varje verksamhet för att hantera dessa utmaningar framåt.

Stadsrevisionens informationssäkerhets- och dataskyddsår 2024

Verksamhetsåret 2024 har innefattat en rad åtgärder kopplat till utveckling av *informationshantering* i verksamheten till följd av införande och pågående avveckling av IT-system 2023–2024[40].

Stadsrevisionen hanterar mycket information av olika slag kopplat till sin huvudprocess (granskning). Detsamma gäller för de olika processerna som finns kopplade till revisorernas förvaltning, såsom HR-administration, offentlig upphandling och övriga förvaltningsfrågor.

All sådan information utgör potentiellt allmänna handlingar och träffas därför av de hanteringsregler som gäller för sådana.[41] Utan att gå för djupt in i hur dessa regler är utformade ska det ändå konstateras att en verksamhet som omfattas av reglerna – för att de ska vara fungera så som det är tänkt – måste ha en strukturerad och systematisk hantering av sin information.

[40] Digitala navet infördes i slutet av 2023 och ersatte Stadens intranät i LIS-miljö. Visma Ciceron DoÄ infördes i början av 2024. Dokumentationssystemet ReVy är under avveckling.
[41] Regelverket för allmänna handlingar återfinns i tryckfrihetsförordningens 2 kapitel och i offentlighets- och sekretesslagen (OSL). I normalfallet är en handling som inkommer till eller upprättas hos en myndighet en allmän handling. Den omfattas då av offentlighetsprincipen, vilket innebär att envar har rätt att ta del av den såvitt den inte omfattas av sekretess.

Det finns också formella regler för hur en myndighet ska hantera sina allmänna handlingar, dels via lag, dels via regler och anvisningar från den arkivmyndighet en myndighet lyder under.[42]

Generell utveckling kopplat till informationshantering i Staden och hos stadsrevisionen

Stadsrevisionen har historiskt sett inte skiljt sig från många andra kommunala verksamheter i landet och inom Staden i det att man sparat och bevarat en stor mängd information och handlingar under lång tid. Detta innebär i sig inte något formellt fel. Handlingar som utgör allmänna handlingar ska bevaras i enlighet med vad som är beslutat enligt gällande lag och gällande arkivregler. Handlingar som inte utgör allmänna handlingar eller omfattas av gallringsbeslut ska dock som huvudregel rensas eller gallras. Detta följer av att arkivbildningen i annat fall riskerar att växa okontrollerat, vilket medför kostnader och risk för en ineffektiv arkivhantering. Det bildas en ”arkivskuld” bestående av information och handlingar som vid någon punkt måste hanteras av verksamheten. Detta måste då göras formellt riktigt i förhållande till regelverken för allmänna handlingar. Stadsrevisionen har haft en sådan ”arkivskuld” som i fråga om handlingar i pappersform hanterats under 2024. Även handlingar i elektronisk form har hanterats, detta arbete pågår dock fortfarande.

Göteborgs Stad har i samband med införandet av det nya IT-systemet Ciceron DoÄ som ersättning för det äldre diariesystemet LIS valt att införa ett nytt övergripande arbetssätt för handlingshantering. Ett av syftena med det är att minska och effektivisera den samlade handlingshanteringen. Arbetssättet innebär att den som ansvarar för ett ärendes handläggning också ansvarar för att de handlingar som tillhör ärendet registreras och hanteras i systemet. Det är en avgörande skillnad mot äldre arbetssätt då särskilda yrkeskategorier (registratorer, diarieförare eller arkivarier) ansvarade för hantering av handlingarna i förhållande till regelverken för detta. Detta innebär också att arbetssätt för hantering av information i en verksamhets olika processer behöver ses över och utvecklas i många fall.

Detta gäller även för stadsrevisionen och då särskilt granskningsprocessens arbetssätt i fråga om dokumentation som har varit och

[42] Hanteringsreglerna enligt lag finns främst i OSL och arkivlagen. Den arkivmyndighet Stadsrevisionen lyder under är arkivnämnden (gemensam nämnd - Göteborgs Stad och Västra Götalandsregionen.)

fortfarande är föremål för utveckling. Formellt styrande dokument för handlingshantering såsom informationshanteringsplan (tidigare dokumenthanteringsplan) har också setts över och uppdaterats 2024. Nytt gallringsbeslut för revisionsdokumentation har utarbetats och godkänts av arkivmyndigheten. Gallring av pappersarkiv för arkivläggning hos arkivmyndigheten har genomförts, liksom faktiskt överföring av arkivet till myndigheten. Översyn av arkivförteckning och arkivbeskrivning pågår.

Stadsrevisionens införande av Visma Ciceron

Stadsrevisionen har infört det nya stadsgemensamma IT systemet Visma Ciceron DoÄ för ärende- och dokumenthantering 2024. Införandet har skett som en av de tidiga införandeverksamheterna i Staden under den stadsgemensamma införandeplan som gäller. En erfarenhet av detta har varit att systemet dragits med en del brister och justerings/utvecklingsbehov vid införandet. Ansvaret för detta vilar på huvudprojektet för införande av systemet vid intraservice och leverantören Visma. Det har inneburit en hel del utmaningar för stadsrevisionens egen lokala införande- och förvaltningsorganisation. Det har också inneburit vissa utmaningar för övriga medarbetare att ta till sig och använda systemet på avsett sätt.

Stadsrevisionen har hanterat dessa utmaningar genom olika stödjande åtgärder. Införandet av systemet har krävt en översyn av arbets- och synsätt för i första hand granskning och dokumentation av denna. Ett särskilt arbete har drivits inom revisionsavdelningarna för att stödja införande och användning av systemet. En rad stödjande dokument har också utarbetats såsom:

- Anvisning för gallring av handlingar av tillfällig eller ringa betydelse kopplat till granskning.
- Anvisning för personuppgiftsminimering vid upprättande av granskningsmaterial.
- Anvisning för rensning och gallring av granskningsunderlag.
- Anvisning för lagringsplatser för revisionsdokumentation under 2024.
- Anvisning för benämning av revisionsdokumentation i Ciceron
- Anvisning för arbetsmaterial i SharePoint.

Visma Ciceron fortsätter att utvecklas i takt med att fler verksamheter i Staden inför det. Det kommer dock sannolikt att dröja innan systemet fungerar väl och fullt ut med Stadens målsättningar för det.

En iakttagelse är att stadsrevisionen kommer att behöva fortsätta sitt utvecklingsarbete kopplat till informations- och handlingshantering inom och utom Visma Ciceron. Det är en nödvändig utveckling framåt, men i detta kan det ändå konstateras att man kommit en god bit framåt under 2024.

Behörighetshantering

Stadsrevisionen har utvecklat och stärkt sina rutiner för behörighetshantering i IT-system under året. Behörigheter kopplas i första hand till anställning och fokus har därför varit att upprätta tydliga checklistor som används vid anställning respektive avslutande av anställning. Upplägg av ny behörighet ska numera också alltid godkännas av ansvarig chef.

Tillämpning av framtagna rutiner

Stadsrevisionen har sedan tidigare (2023) framtagit rutiner för utlämnande av registerutdrag och hantering av PU-incidenter.

Rutinerna har tillämpats praktiskt under 2024 och då befunnits ändamålsenliga. I fråga om registerutdrag har rutinen använts vid ett tillfälle och i fråga om PU-incident har rutinen använts vid sex tillfällen och sex incidenter. En av dessa incidenter bedömdes anmälningspliktig till IMY och anmälan gjordes inom föreskriven tid. Anmälan föranledde ingen vidare åtgärd från IMY:s sida.

Samtliga PU-incidenter uppstod i den kommungemensamma IT-miljön och rapporterades av intraservice till stadsrevisionen.

SLA och PUB-avtal med intraservice

I 2023 års DSO rapport uppmärksammades att stadsrevisionen inte tecknat Service Level Agreement (SLA) respektive personuppgiftsbiträdesavtal (PUB-avtal) med intraservice avseende de kommungemensamma tjänster verksamheten använder. Det är väsentligt att detta finns på plats och Stadsrevisionen har via DSA vid upprepade tillfällen under 2024 begärt att intraservice ska presentera de uppgifter som krävs för att kunna upprätta dessa handlingar på det sätt som krävs.

Underhandskontakt med intraservice i inledningen av 2025 visar att det pågått ett arbete där under 2024 för att ta fram en webbaserad modell för SLA per kommungemensam tjänst via Stadens tjänstekatalog. Stadsrevisionen kommer att utvärdera om det går att sluta SLA denna väg.

I fråga om PUB-avtal är det mer oklart vilka underlag för detta som intraservice kan presentera i dagsläget. Innehållet i ett korrekt utformat

PUB-avtal styrs av DSF artikel 28. Grundtanken är att PUA alltid har ansvaret för de PU-behandlingar som görs för dennes räkning även om de görs av någon annan (som då är personuppgiftsbiträde - PUB). PUA måste därför både lämna instruktioner till PUB och ha kontroll över att dessa instruktioner följs. Det är också av avgörande betydelse att PUA har information om (och godkänner) vilka eventuella underbiträden PUB använder (alla underleverantörer för hela eller delar av kommungemensamma tjänster.)

EDPB har nyligen antagit ett yttrande som handlar om artikel 28 ska tolkas och konstaterar där bland annat att:[43]

- Yttrandet handlar om situationer där PUA förlitar sig på en eller flera PUB och underbiträden.

- PUA alltid bör ha information om identiteten (dvs. namn, adress, kontaktperson) för alla PUB, underbiträden osv. lättillgänglig så att de på bästa sätt kan fullgöra sina skyldigheter enligt artikel 28 i DSF.

- PUA:s skyldighet att kontrollera om (under)biträdena har ”tillräckliga garantier”[44] bör gälla oavsett risken för de registrerades rättigheter och friheter, även om omfattningen av en sådan kontroll kan variera, särskilt på grundval av de risker som är förknippade med behandlingen.

- Att även om det ursprungliga personuppgiftsbiträdet bör se till att det föreslår underentreprenörer med tillräckliga garantier, så ligger det slutliga beslutet och ansvaret för att anlita en viss underentreprenör kvar hos PUA.

Att godkänna det utkast till PUB-avtal som intraservice tagit fram och som exempelvis inte innehåller information om vilka underbiträden som används för de olika kommungemensamma tjänsterna skulle därmed innebära ett direkt åsidosättande av DSF:s krav på stadsrevisionen i egenskap av PUA.

---

[43] EDPB - Opinion 22/2024 on certain obligations following from the reliance on processor(s) and sub-processor(s) den 9 oktober 2024.
[44] ”Tillräckliga garantier” syftar på DSF:s krav på det är PUA:s ansvar att tillse att PU behandlingar som utförs av PUB för PUA:s räkning sker i enlighet med DSF:s regelverk.

Intraservice driver sedan 2023 ett internt projekt för att etablera ett systematiskt informationsarbete i den egna förvaltningen.[45] Flera aktiviteter har genomförts under 2024 och projektet avses pågå till och med andra kvartalet 2026. Projektet syftar till att:

”etablera ett systematiskt arbete med informationssäkerhet på Intraservice. Arbetet är omfattande och berör stora delar av förvaltningens övriga arbete. Leveranserna ska, när det är möjligt, utformas så att även andra förvaltningar och bolag i staden kan använda dem.”[46]

Projektet torde, mot bakgrund av stadsrevisionens tidigare och återkommande iakttagelser om brister i intraservice hantering av informationssäkerhetsfrågor av olika slag, vara både välkommet och angeläget. Förhoppningsvis kommer projektets arbete att primärt stärka intraservice arbete i dessa frågor.

Det kan då i sin tur förhoppningsvis på sikt ge bättre förutsättningar för Stadens övriga verksamheter, som utnyttjar kommungemensamma tjänster, att lösa in de bitvis komplexa kravbilder som gäller för varje verksamhets informationssäkerhets- och dataskyddsarbete.

Kompetensutveckling

Det behövs inte bara ändamålsenliga IT-system och arbetssätt för att upprätthålla en god informationssäkerhet och ett fullgott dataskydd, det behövs också kunskap hos användarna.

Stadsrevisionens verksamhet är kunskapsintensiv till sin natur vilket medför att förutsättningarna för att vanemässigt lära nytt och reflektera är väl förankrade i organisationskulturen. Detta är positivt då det kommer till att utbilda och fortbilda medarbetarna. Stadsrevisionen har också under de gångna åren genomfört flera satsningar för att höja den generella kunskapsnivån runt informationssäkerhet och dataskydd.

Granskning relaterad till informationssäkerhet, dataskydd och krisberedskap är också kompetensutvecklande för de medarbetare som

[45] Etablera systematiskt informationssäkerhetsarbete (ESI).
[46] Citerad (kursiverad) beskrivning i informationsmaterial från projektet.

genomför sådan granskning. Stadsrevisionen har genomfört flera granskningar inom området under 2024.[47]

Det är dock särskilt viktigt att de som leder stadsrevisionens verksamhet har tillräckliga kunskaper för att förstå vilka krav som ställs på en offentlig verksamhet i fråga om dataskydd i dagsläget. Av denna anledning rekommenderade jag stadsrevisionen 2023 att man skulle prioritera att höja kunskapsnivån rörande DSF:s regelverk och tillämpning av det för ansvariga chefer.

Under 2024 har avdelningscheferna för revisionsavdelningarna utbildats på rekommenderat sätt vilket är positivt. Från 2025 kommer emellertid en ny organisation att etableras hos stadsrevisionen. Organisationsförändringen innebär att två revisionsavdelningar blir tre varvid två nya avdelningschefer kommer att tillsättas[48]. Det är mycket viktigt att den nya grupperingen av avdelningschefer också tillägnar sig nödvändiga kunskaper om DSF:s regelverk och tillämpningen av det.

Det är också mycket viktigt att fortsätta att synliggöra både informationshanterings- och informationssäkerhets- respektive dataskyddsfrågor för organisationens övriga medarbetare. Återkommande iakttagelser från IMY rörande PU-incidenter visar att den mänskliga faktorn är den dominerande orsaken då incidenter inträffar. Detta kan bara motverkas genom kunskap, insikt och genomtänkta arbetssätt hos varje verksamhet och medarbetare. Det är också varje PUA:s ansvar att säkerställa att medarbetare ges rätt förutsättningar så att DSF:s regelverk kan upprätthållas. Det är i detta sammanhang också viktigt att notera att systematisering och tillgängliggörande av styrande och stödjande dokument är en viktig förutsättning för att det ”ska vara lätt att göra rätt”.

Stadsrevisionen har under 2024 och tidigare tagit fram mycket material inom informations- och dataskyddsområdet som bedöms kunna organiseras på ett tydligare sätt. Detta bör stadsrevisionen hantera framåt

[47] Granskade verksamheter 2024 har varit: Göteborgs Stads Parkerings AB, Higab AB, Älvstranden Utveckling AB, Gryaab AB, Göteborgs Hamn AB, Göteborgs Spårvägar AB, Göteborgs Stads Kollektivtrafik AB, Inköp- och upphandlingsnämnden, Kretslopp och vattennämnden och Nämnden för Intraservice.
[48] En ny avdelningschef är redan tillsatt.

genom att se över hur gällande styrande och stödjande dokument bäst tillgängliggörs för organisationen på ett logiskt och tydligt sätt.

Pågående och framåtriktat arbete

Även om mycket arbete gjorts under 2024 krävs fortsatt arbete under kommande år. Detta gäller generellt för att fortsätta stärka stadsrevisionens informationshantering liksom förutsättningarna för informationssäkerhet och dataskydd.

Specifikt behöver arbetet utveckla och anpassa arbetssätt för dokumentation av granskning i förhållande till lagkrav och utvecklade rutiner inom och utom Visa Ciceron att fortsätta. Vidare behöver det påbörjade arbetet att harmonisera informationssäkerhetsarbetet mot Stadens (nya) riktlinje för informationssäkerhet att fortsätta. Prioriterade åtgärdsområden i fråga om detta är:

- Genomföra ny informationsklassning enligt Stadens nya modell.
- Genomföra översyn av befintligt register över PU-behandlingar (artikel 30-register).
- Ta fram kontinuitetsplanering.
- Ta fram rutin för informationssäkerhetsincidenter.

Ytterligare åtgärdsområden kommer att omhändertas successivt.

Stadsrevisionens verksamhetsplan för 2025 lyfter att fortsatta satsningar på utveckling av informationssäkerhetsarbetet kommer att ske. Där anges också att stadsrevisionen avser att undersöka möjligheten att använda AI-baserad teknik i verksamheten.

Som redogjorts för under avsnitt 1 i rapporten är det mycket viktigt att ha god kontroll över vad IT-system gör med information som innefattar PU. Detta gäller i synnerhet i fråga om AI-baserad teknik. Det bedöms vara av mycket stor betydelse att stadsrevisionen noga beaktar integritetsrättsliga risker och regler innan man driftsätter eventuella AI-baserade verktyg i verksamheten. Det finns också, som redogjort för ovan, mycket vägledning i dessa frågor via exempelvis IMY och DIGG som bör följas. Grundläggande är att användning av AI-baserad teknik är föremål för styrning från ledningens sida för att säkerställa att gällande lagregler för PU-behandling och informationshantering följs vid användning av tekniken.

3. Sammanfattande kommentar och rekommendationer

För att sammanfatta iakttagelserna i denna rapport kan det på en övergripande nivå konstateras att den tekniska utvecklingen ställer ökande krav på den som är PUA. Ökad effektivitet genom ökad digitalisering innebär också ökade krav på att PUA alltid har kontroll över den teknik som används och att de registrerades rättigheter kan tillgodoses. Det är viktigt att förstå detta och att den integritetsrättsliga regleringen ytterst är en skydds- och rättighetslagstiftning som varje PUA är skyldig att följa och anpassa sin verksamhet efter.

För att formellt summera rapporten 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 under 2024 lämnat råd i fråga om konsekvensbedömning av dataskydd inför införandet av det kommungemensamma IT-systemet Visma Ciceron DoÄ.

Jag har under 2024 inte haft något aktivt samarbete eller samråd med IMY.

I 2023 års DSO -rapport lämnade jag följande rekommendationer:

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.

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.

Som redogjorts för i avsnitt 2 ovan kan jag konstatera att stadsrevisionen följt rekommendationerna. De ska därför anses som omhändertagna.

Beträffande iakttagelser runt stadsrevisionens informationssäkerhets- och dataskyddsarbete 2024 kan jag konstatera att utvecklingen är positiv och organisationens generella dataskyddsmognad får sägas öka över tid.

Det är emellertid viktigt att arbetet att utveckla informationshantering, informationssäkerhet och dataskydd framåt fortgår. Kopplat till detta lämnar jag följande rekommendationer:

Stadsrevisionen rekommenderas att se över hur gällande styrande och stödjande dokument avseende informationssäkerhet och dataskydd bäst tillgängliggörs för organisationen på ett logiskt och tydligt sätt.

Stadsrevisionen rekommenderas att säkerställa att den nya grupperingen av avdelningschefer i den nya organisationen tillägnar sig nödvändiga kunskaper om DSF:s regelverk och tillämpningen av dem.

Stadsrevisionen rekommenderas att säkerställa att användning av AI-baserad teknik inte implementeras i verksamheten utan tillfredställande styrning från ledningens sida så att gällande lagregler för PU-behandling och informationshantering följs vid användning av tekniken.

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