Göteborgs Stad

Årsrapport för dataskyddsarbetet 2024

Arkivnämnden

2024-12-20

Innehåll

1 Dataskydd i kommunal verksamhet

Att få ta del av och hantera andra människors personliga uppgifter på ett sådant sätt som kommunala förvaltningar och bolag gör innebär att förvalta ett stort förtroende. Dataskyddsförordningen (GDPR) har tillkommit för att särskilt värna om den enskildes rätt till integritet och kontroll över vad som sker med ens personuppgifter. Rätten till en fredad privat sfär och personlig integritet är grundläggande i ett demokratiskt samhälle och är ett av fundamenten på vilket många andra av våra demokratiska rättigheter vilar. Lagstiftningen finns till för att skydda individen från skada och sätter ramarna för hur personuppgifter får behandlas i en alltmer digital värld.

Att förvaltningar och bolag hanterar personuppgifter i enlighet med gällande lag bör vara en självklarhet i syfte att visa omsorg om det förtroende som getts den som har att hantera personuppgifter. För att säkerställa följsamhet gentemot GDPR behöver dataskyddsperspektivet 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 på förvaltningar och bolag inom Göteborgs Stad. I det framåtsyftande arbetet är GDPR ett viktigt redskap för att kunna säkerställa en digitalisering som håller över tid.

2 Göteborgs Stads dataskyddsombud

Det är varje nämnd och bolag som är ytterst ansvarig för att dess verksamhet följer dataskyddslagstiftningen. För att stödja stadens nämnder och bolag i arbetet med dataskydd har ett dataskyddsombud utsetts. I Göteborgs Stad fullgör dataskyddsenheten på Intraservice uppdraget som dataskyddsombud åt stadens bolag och nämnder. Vad som är dataskyddsombudets uppgifter framgår direkt av lagstiftningen i GDPR.[1] Dataskyddsombudets viktigaste uppgift är att övervaka att stadens förvaltningar och bolag följer dataskyddslagstiftningen. Detta sker bland annat genom att samla in information om hur personuppgifter behandlas och genom att kontrollera hur bestämmelser och interna styrdokument som styr dataskyddsarbetet efterlevs. Dataskyddsombudet har också till uppgift att ge råd och information till förvaltningar och bolag i dataskyddsfrågor. Detta sker genom att dataskyddsombudet är behjälplig när frågor rörande behandlingen av personuppgifter uppkommer hos verksamheterna.

Enligt lag ska dataskyddsombudet även rapportera om arbetet till högsta förvaltningsnivå[2], och utifrån detta lämnar dataskyddsombudet årligen en rapport om den egna verksamhetens dataskyddsarbete till nämnder och bolag i Göteborgs Stad. I rapporten redogör dataskyddsombudet för de iakttagelser som gjorts under året, både stadenövergripande och, i vissa fall, verksamhetsspecifika. Rapporten innehåller även information om årets fördjupade kontroll samt resultatet från den uppföljning som genomförts avseende hur verksamheten hanterat och arbetat med de rekommendationer som lämnades i årsrapporten 2023.

Årsrapporten är avsedd att kunna användas som ett stöd för verksamheten i sitt fortsatta arbete med dataskydd. Det är upp till varje verksamhet att besluta om hur det interna dataskyddsarbetet ska utformas utifrån verksamhetens förutsättningar för att på bästa sätt hantera identifierade risker.

2.1 Stadenövergripande iakttagelser 2024

2.1.1 Ny central funktion för styrning och samordning i dataskyddsfrågor möjliggör ett stärkt dataskydd

Hur långt förvaltningar och bolag kommit i dess dataskyddsarbete skiljer sig stort åt inom Staden. Skillnaderna bedöms till stor del bero på bristande styrning och samordning i dataskyddsfrågor från centralt håll, något som lyfts av dataskydds-ombudet under flera år. Resultatet av detta är bland annat att skyddet för de registrerades personuppgifter varierar mellan verksamheterna, en ineffektiv

[1] Artikel 39 i GDPR
[2] Artikel 38.3 i GDPR

personuppgiftsincidenthantering och att hanteringen av rättigheter hanteras olika beroende på vilken verksamhet man vänder sig till.

Dataskyddsombudets förhoppning är att den nya dataskyddsfunktionen som införts på stadsledningskontoret ska bidra till att utveckla och stärka de grundläggande delarna av dataskyddsarbetet och därigenom generera ett mer enhetligt dataskydd inom Staden. Att stadsledningskontoret nu tar ansvar för att samordna dataskyddsarbetet bedöms ligga i linje med kommunstyrelsens uppdrag.

I sammanhanget vill dataskyddsombudet samtidigt poängtera att varje nämnd och bolag fortfarande är ytterst ansvariga för sina respektive personuppgifts-behandlingar. Det är därför även fortsatt upp till varje nämnd och bolag att säkerställa efterlevnad gentemot lagstiftningen. Att varje verksamhet tar det ansvaret är avgörande för att det arbete som görs inom dataskyddsfunktionen ska få genomslag och ha en positiv påverkan på dataskyddet som helhet i Staden.

2.1.2 Verksamhetens ledning avgörande för att GDPR inte ska fortsättas upplevas som ett hinder

I årsrapporten 2023 lyfte dataskyddsombudet att det inom Staden generellt bedömdes finnas en uppfattning om att det är omöjligt att följa GDPR och samtidigt driva den digitala utvecklingen framåt. Dataskyddsombudets upplevelse, utifrån de dialoger som varit under 2024, är att denna uppfattning fortfarande kvarstår och är något som i hög grad påverkar dataskyddsarbetet negativt. Dataskyddsombudet har i möten med funktioner från olika verksamheter inom Staden kontinuerligt fått höra att GDPR är något som är jobbigt och krångligt, och som blir ett hinder som försvårar deras arbete med att ta i bruk nya digitala lösningar. Som regel uttrycks detta efter eller precis inför att verksamheten ska teckna avtal, eller precis står inför att börja använda en ny digital lösning eftersom det ofta är först då som dataskyddsperspektivet beaktas. Dataskyddsombudet förstår att medarbetare i den situationen upplever GDPR som ett hinder, men ser samtidigt att GDPR inte kan klandras för de uppenbara brister i den interna styrningen som medfört att verksamheten inte arbetat med dataskyddsfrågorna i tid.

För att känslan av GDPR som något jobbigt och ett hinder inte ska fortsätta ha en negativ påverkan på dataskyddsarbetet behöver Staden som helhet arbeta för att öka medvetenheten om syftet med lagstiftningen. En del kan göras genom utbildningar, men centralt är också att det från ledningshåll inom stadens verksamheter börjar signaleras att dataskydd är något som ska beaktas och arbetas med. I den offentliga debatten hör man ofta representanter från näringslivet tala om att det offentliga måste vara modiga och testa nya saker. Dataskyddsombudets uppfattning att det modiga i dessa fall ofta handlar om att utmana den lagstiftning som styr offentlig sektor, till exempel då lagstiftningen begränsar möjligheterna att dela och/eller använda data. Lagstiftningen, inkluderat GDPR, utmålas då som ett administrativt hinder som hämmar utvecklingen. Denna bild av GDPR som ett hinder delas inte av dataskyddsombudet eftersom det inte finns någon motsättning mellan att följa lagkraven och samtidigt driva digitaliseringen framåt. Utifrån den

diskurs som råder bedömer dataskyddsombudet att det är viktigt att man på ledningsnivå har kunskap om syftet med GDPR och förståelse för att om GDPR sätter ”stopp” för en behandling eller en tjänst så finns det ett gott skäl till det. I praktiken innebär det att man på ledningsnivå behöver ta ansvar för att inte använda en digital tjänst eller inleda en behandling av personuppgifter som inte är förenlig med kraven i GDPR. En viktig del i detta är att ledningen börjar signalera en förväntan på att nya digitala lösningar ska vara långsiktigt hållbara, även utifrån ett integritetsperspektiv. På så sätt behöver verksamheter tänka på dataskydd tidigt i processen och kan förhoppningsvis undvika att hamna i situationer där GDPR enbart ses som något jobbigt eller ett administrativt hinder. Genom att integrera dataskyddsperspektivet från start i arbetet med nya tjänster och/eller vid utvecklandet av nya arbetssätt kan verksamheter hitta stabila och långsiktiga alternativ där människors grundläggande fri- och rättigheter inte äventyras. Något som blir, om möjligt, extra viktigt i takt med att användningen av ny teknik och AI ökar inom Stadens verksamheter.

2.1.3 Bristande ansvarstagande i Stadens arbete med AI medför risker för både enskilda och verksamheter

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 sig framåt glömmer att hänsyn behöver tas till den personliga integriteten och att personuppgifter behandlas på ett korrekt sätt. Som en stor offentlig aktör har Göteborgs Stad att förvalta alla invånare och besökares förtroende. Oavsett om det handlar om elever, vårdnadshavare, anställda, 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.

Under året har dataskyddsombudet kunnat se att allt fler verksamheter inom Staden börjar utforska användningen av AI. Dataskyddsombudet har under året löpande kunnat identifiera stora risker med det arbete som bedrivs på stadenövergripande nivå. Riskerna kommer dels utifrån att det från centralt håll hittills saknas styrning och samordning i hur tekniken kan, och får, användas, dels utifrån att de tekniska lösningar som har lanserats ej först kontrollerats utifrån ett informationssäkerhets- och dataskyddsperspektiv. Dataskyddsombudets bedömning är att stadsledningskontoret och Intraservice behöver ta ett större ansvar i hanteringen av dessa risker, eftersom de båda verksamheterna är starkt drivande i användningen av AI inom Staden. Särskilda rekommendationer ställs därför till de båda verksamheterna i deras respektive årsrapporter.

Dataskyddsombudet vill utifrån identifierade risker med de stadenövergripande AI-lösningar som idag finns tillgängliga inom Staden (M365 Copilot i Edge, Svea GPT etc.) betona vikten av att förvaltningar och bolag innan en ny AI-lösning tas i bruk först kontrollerar så att denna är säkerställd utifrån ett informationssäkerhets- och dataskyddsperspektiv.

3 Dataskyddsombudets iakttagelser 2024

3.1 Verksamhetens dataskyddsarbete

Regelbundna avstämningar har hållits mellan dataskyddsombudet och dataskyddskontakter under så väl vårterminen som höstterminen. Dataskyddskontakterna har löpande lyft frågor med dataskyddsombudet och har rådfrågat dataskyddsombudet kopplat till personuppgiftsincidenter. Dialog har förts kring förvaltningens strategi för dataskyddsarbete. Konsekvensbedömning kopplat till behandlingar i ”Mina meddelanden” har hanterats. Löpande dialog har ägt rum kopplat till ”Din Klinik-frågan” vilket varit en stor fråga under sommaren/hösten (se mer vid ”Särskilda iakttagelser” nedan).

3.2 Särskilda iakttagelser

I februari 2024 fattade Inspektionen om vård och omsorg (IVO) beslut om att vårdbolaget Din Klinik Väst Holding AB:s patientjournaler skulle omhändertas enligt 9 kap. 1 § patientdatalagen (2008:355). Bolaget hade tidigare försatts i konkurs. Enligt beslutet skulle patientjournalerna förvaras hos Regionarkivet i Göteborg.

Under sommaren 2024 kom det till en av regionarkivets dataskyddskontakters kännedom att det i samband med mottagandet av patientjournaler från Din Klinik Väst Holding AB också mottagits patientjournaler som inte kom från Din Klinik Väst Holding AB:s verksamhet och som därmed inte heller omfattades av IVO:s beslut om omhändertagande. Dessa handlingar tillhörde i stället andra bolag och verksamheter i den så kallade ”Din Klinik-koncernen”. Regionarkivet hade vid den här tidpunkten redan hunnit lämna ut journalhandlingar från det mottagna arkivbeståndet. Misstanke fanns om att journalhandlingar som inte omfattades av IVO-beslutet också hade lämnats ut.

Dataskyddsombudet kontaktades och förvaltningen rekommenderades att utreda frågan närmare. Dataskyddsombudet konstaterade att förvaltningen saknade rättslig grund för att behandla de personuppgifter som inte omfattades av IVO-beslutet. Dataskyddsombudet gjorde också bedömningen att det skulle kunna vara fråga om en personuppgiftsincident i de fall patientjournaler som inte omfattades av IVO-beslutet lämnats ut, och rekommenderade förvaltningen att anmäla det inträffade som en incident till Integritetsskyddsmyndigheten (IMY), att utreda det inträffade närmare och att vidta riskminimerande åtgärder. Förvaltningen anmälde det inträffade som en personuppgiftsincident till IMY. Förvaltningen rekommenderades också vidta åtgärder för att identifiera vilka handlingar som hörde till vilken verksamhet och att utkräva en ny export med endast det korrekta materialet. Dataskyddskontakten höll löpande kontakt med förvaltningen under

sensommaren och hösten då omständigheterna kring mottagna och utlämnade patientjournaler utreddes.

Dataskyddsombudet har tidigare i dialog med dataskyddskontakten rekommenderat att förvaltningen utvärderar sitt arbetssätt vad gäller mottagande av arkivbestånd och att förvaltningen vidtar åtgärder för att undvika att liknande situationer uppstår i framtiden. Rekommendationen kvarstår. Det kan t.ex. vara lämpligt att ta fram ett dokumenterat arbetssätt i frågan och medvetandegöra medarbetare om vilken hantering som ska gälla. Dataskyddsombudet är av uppfattningen att förvaltningen kan ställa krav på den som ska överlämna material, och att det inte kan fodras att förvaltningen tar emot material som förvaltningen saknar rättslig grund för. Förvaltningen rekommenderas också att ha en fortsatt dialog med berörda myndigheter för att få stöd och för att få fram ett klargörande av vad som gäller rättsligt och vad som är en korrekt och lämplig hantering i frågan.

Dataskyddsombudet rekommenderar att förvaltningen vidtar åtgärder för att få en ny korrekt export och att felaktigt mottaget material antingen återlämnas eller raderas efter dialog med den part som överlämnat materialet. Detta behöver göras eftersom det saknas rättslig grund för behandling av dessa personuppgifter. I skrivande stund har dataskyddsombudet fått information om att förvaltningen har kontaktat konkursförvaltaren och informerat denna om att förvaltningen har för avsikt att radera de felaktigt mottagna personuppgifterna. Förvaltningen har även utkrävt en ny korrekt export.

Dataskyddsombudet har också förstått att det kan finnas incidenter som inte har med det aktuella felaktigt mottagna materialet att göra, men som i stället handlar om oklarhet kring vad det är som efterfrågas i en rekvisition från vårdgivare och oklarheter kring vad som omfattas av patienternas samtycke i ett sådant fall. Vad gäller denna större fråga har dataskyddsombudet tidigare rekommenderat att förvaltningen utreder saken vidare för att ta ställning till om vad som är en lämplig hantering av så väl historiska som framtida utlämnanden. Målsättningen bör vara att ha en hantering som undanröjer oklarheter kring vad det är som efterfrågas och vad samtycket omfattar. Rekommendationen kvarstår. Även i denna del kan det vara lämpligt att ta fram dokumenterade arbetssätt i frågan och att medvetandegöra medarbetare om vilken hantering som ska gälla.

Dataskyddsombudet kommer särskilt följa upp rekommendationerna under 2025.

4 Granskning av dataskyddsarbetet 2024

4.1 Fördjupad kontroll 2024

Under våren 2023 genomförde dataskyddsenheten en informationsinsats med fokus på behandlingsregistret enligt artikel 30 i GDPR. Som uppföljning på denna informationsinsats genomförde dataskyddsenheten under hösten 2024 en fördjupad kontroll med fokus på behandlingsregistret för ett antal av stadens verksamheter (dock ej inom aktuell verksamhet).

Resultatet av kontrollen visade sammantaget på stora brister i omhändertagandet av artikel 30 i GDPR. För att alla verksamheter i Staden ska få ta del av resultaten från kontrollen har dataskyddsombudet tagit fram en stadengemensam rapport. Den stadengemensamma rapporten innehåller både generella iakttagelser från kontrollen, dataskyddsombudets bedömningar i olika sakfrågor och konkreta exempel på hur behandlingsregistret kan utformas med hänvisningar till olika rättskällor som dataskyddsombudet anser har ett generellt värde för hela Staden. Rapporten blir en form av ytterligare vägledning avseende hur arbetet med behandlingsregistret kan utformas för att skapa förutsättningar för ett funktionellt dataskyddsarbete där kraven i artikel 30 i GDPR kan uppfyllas.

Dataskyddsombudet kommer under 2025 följa upp dels att samtliga av Stadens verksamheter har tagit del av rapporten, dels hur verksamheterna avser omhänderta de generella rekommendationerna i arbetet med det egna behandlingsregistret.

4.2 Uppföljning av lämnade rekommendationer

4.2.1 Uppföljning av verksamhetens arbete med rekommenderade fokusområden 2024

Dataskyddsombudet har följt upp hur verksamheten arbetat med de fokusområden som rekommenderades för 2024. Utifrån uppföljningen lämnas rekommendationer.

Fokusområde 1: Kontrollpunkt 5 Övergripande styrning av dataskyddsarbetet

Verksamheten gavs följande rekommendationer:

Anta en övergripande strategi för dataskyddsarbetet, samt vidta åtgärder för att kunna arbeta riskbaserat.

Utvärdera på vilket sätt verksamheten kan göra interna kontroller för att säkerställa följsamhet gentemot GDPR. Identifiera områden som är meningsfulla, rimliga och möjliga att kontrollera. Sätt upp en tidsplan och genomför kontrollen/kontrollerna.

Kommentarer och rekommendationer:

Förvaltningen har uppgett följande. Arbete pågår med ett styrande dokument (arbetsnamn ”Regionarkivets anvisning för informationssäkerhet, dataskydd och skydd av arkiv”) och tillhörande bilaga (arbetsnamn ”Styrning för informationssäkerhet, dataskydd och skydd av arkiv”). Bilagan kommer att utgöra Regionarkivets övergripande strategi för dataskyddsarbetet där arbetet med medvetenhet, och beteenden inkluderas. Bilagan syftar till att ge en övergripande bild av de regler som Regionarkivet måste följa inom informationssäkerhet, dataskydd och skydd av arkiv.

Kopplat till rekommendationen om interna kontroller har förvaltningen identifierat loggar som ett område där kontroll sker. I Regionarkivets system Long-Term-Archive (LTA) och systemet Oskar är det obligatoriskt att ange åtkomstorsak i Long-Term Archive (LTA) vid sökning i arkiv som rör vård eller socialtjänst. Åtkomstorsaken loggas och det är därför möjlig att kontrollera detta. Kontroll genomförs årligen enligt ett dokumenterat arbetssätt, vilket det finns information om på Digitala navet.

Regionarkivet genomför också löpande automatiserade kontroller av checksumman för digitala arkivobjekt. De automatiserade kontrollerna av checksumma för arkiv innebär att man får ett meddelande när säkerheten äventyras kring de handlingar och filer som ingår i arkivet. Genom att man får en notis kan man återläsa eventuella förstörda filer och handlingar genom backuper. Förvaltningen har uppgett att ytterligare arbete kan göras för att tydliggöra den här arbetsprocessen så att man har bättre beredskap att faktiskt hantera situationen när ett felmeddelande kommer.

Dataskyddsombudet konstaterar att förvaltningen påbörjat att omhänderta rekommendationen om att anta en dataskyddsstrategi. Dataskyddsombudet uppmuntrar förvaltningen att fullfölja arbetet.

Vidare konstaterar dataskyddsombudet att förvaltningen har kontroller som har betydelse för reglerna om personuppgiftsbehandling och uppmuntrar förvaltningen att fortsätta detta arbete och att vid behov tydliggöra och förbättra arbetsprocesserna.

Dataskyddsombudet kommer inte att följa upp frågorna särskilt under 2025 eftersom arbete pågår, men kommer att följa förvaltningens strategiska dataskyddsarbete löpande.

Fokusområde 2: Kontrollpunkt 9 och 10 Konsekvensbedömning/samråd och IT-projekt och upphandling

Verksamheten gavs följande rekommendationer:

Utvärdera verksamhetens arbetssätt vad gäller hantering av dataskyddsfrågor inom IT-projekt och upphandling, samt tröskelanalyser och konsekvensbedömningar.

Fortsätt gå på djupet i frågor som rör verksamhetens behandlingar.

Vidta åtgärder för att säkerställa att dataskyddsperspektivet tas i beaktan på ett systematiskt sätt och i ett tidigt skede.

Vidta åtgärder för att säkerställa att behandlingar utreds innan beslut fattas, avtal tecknas och personuppgiftsbehandlingar inleds.

Vidta åtgärder för att säkerställa att dataskyddsombudets synpunkter inhämtas i god tid.

Kommentarer och rekommendationer:

Förvaltningen har uppgett att man är medveten om att man behöver tydliggöra det systematiska dataskyddsperspektivet i arbetet med IT-projekt och upphandling. Regionarkivets organisation för informationssäkerhet och dataskydd arbetar för att medvetandegöra cheferna om deras ansvar i dataskyddsfrågor och för att personuppgiftsbehandlingar ska utredas innan beslut fattas så att dataskyddsombudets synpunkter ska kunna inhämtas i god tid.

Förvaltningen kommer att arbeta för att Regionarkivets ”Anvisning för informationssäkerhet, dataskydd och skydd av arkiv” ska publiceras och implementeras.

Förvaltningen rekryterar en ny kompetens inom området och ska fortsatt arbeta för att utveckla processerna inom IT-förvaltning utifrån verksamhetens behov och lagkrav.

Dataskyddsombudet konstaterar att arbete pågår för att omhänderta rekommendationen. Eftersom arbete pågår kommer dataskyddsombudet inte att följa upp frågorna särskilt under 2025 (såvida inte något särskilt föranleder det), men kommer att följa förvaltningens utvecklingsarbete i frågorna löpande.

Grunden för att över huvud taget och på ett effektivt sätt kunna genomföra konsekvensbedömningar är att ha definierat och gjort funktionella avgränsningar av sina behandlingar. Eftersom dataskyddsombudet inte har kontrollerat förvaltningens behandlingsregister i närtid rekommenderar dataskyddsombudet att förvaltningen i första hand prioriterar arbetet med att se över behandlingsregistret under 2025. Förvaltningen rekommenderas ta del av de generella slutsatser som dataskyddsenheten har dragit inom ramen för den fördjupade kontroll som har genomförts på några av stadens förvaltningar och bolag. Förvaltningen rekommenderas att se över sitt behandlingsregister på nytt utifrån dessa generella slutsatser. Detta för att exempelvis säkerställa att förvaltningens tolkning av innehållskraven ligger i linje med dataskyddsombudets slutsatser och att ändamålen och behandlingarna är definierade på ett funktionellt sätt. Särskild uppföljning i frågan kommer att ske under 2025.

Fokusområde 3: Kontrollpunkt 11 IT-system och digitala verktyg

Verksamheten gavs följande rekommendationer:

Utvärdera verksamhetens arbetssätt gällande behörighetsstyrning och dokumentera arbetssättet för att säkerställa en enhetlig hantering.

Utvärdera hanteringen gällande målgruppsanpassad information om hur digitala verktyg får användas. Vidta behövliga åtgärder för att säkerställa att användare får tillräcklig kunskap om hur system och andra digitala verktyg får användas.

Anta ett dokumenterat arbetssätt för att systematiskt följa upp efterlevnaden.

Kommentarer och rekommendationer:

Förvaltningen har uppgett följande. En rutin har publicerat för behörighets- och åtkomststyrning. Förutom rutinen kommer en mall för behovs- och riskanalys vid behörighetstilldelning i systemstöd att tas fram. Cheferna ska få information om sitt ansvar som informationsägare och ska involveras i arbetet med att utforma mallen.

Förvaltningen har tagit fram målgruppsanpassad information till medarbetarna utifrån Regionarkivets rutin för IT-användning, i form av ett informationsblad ”Tänk på IT-säkerheten”. Detta blad sammanfattar innehållet i Regionarkivets rutin för IT-användning.

Förvaltningen har även publicerat intern information på Digitala navet om behörigheter och åtkomst till systemet Long Term Archive (LTA). Medarbetarna informeras via APT och Teamskanaler.

Dataskyddsombudet noterar att rekommendationerna har omhändertagits och vidare uppföljning kommer därför inte att ske under 2025.

4.2.2 Uppföljning av rekommendationer lämnade inom ramen för tidigare genomförda kontroller

Dataskyddsombudet har under året följt upp vilka åtgärder som vidtagits avseende tidigare års lämnade rekommendationer av gjorda kontroller.

Kontroll (2022): Samtycke om rättslig grund och användning av sociala medier

Verksamheten gavs följande rekommendationer:

Genomför en konsekvensbedömning för användning av sociala medier.

Utred och bedöm lämpligheten i att använda samtycke som rättslig grund vid behandling i sociala medier.

Se över användning av den rättsliga grunden uppgift av allmänt intresse och arkivändamål av allmänt intresse kopplat till sociala medier.

Se över och komplettera "Kanalguide för Regionarkivet – ett stödjande dokument för Regionarkivets anvisning för kommunikation" med eventuella ytterligare behövliga instruktioner.

Utred frågan om profilering.

Kommentarer och rekommendationer:

Förvaltningens har uppgett att förvaltningens bedömning är att en konsekvensbedömning inte är nödvändig då förvaltningen bara anser att ett kriterium i tillsynsmyndighetens förteckning är uppfyllt. Vidare har förvaltningen uppgett att man inte själva profilerar.

Förvaltningen har tagit ställning i frågan om användningen av den rättsliga grunden samtycke respektive uppgift av allmänt intresse och redovisar för detta i kanalguiden. Förvaltningen har angett som instruktion i en stödtext att den som samlar in samtycket ska specificera för vilket eller vilka ändamål fotografiet eller filmen kommer att användas.

Vidare har förvaltningen uppgett följande. I kärnverksamheten, där arkiv tas emot, samlas personuppgifter in enbart för arkivändamål av allmänt intresse. Förvaltningen menar att så väl insamlingen (mottagandet av arkiv) som många av de behandlingar som utförs efter insamlingen, inte är olika behandlingar för olika syften, utan olika steg i en behandlingskedja med samma slutmål: arkivändamål av allmänt intresse. Regionarkivet menar att när regionarkivet publicerar äldre handlingar från mottagna arkiv på Instagram, så görs detta med stöd av den rättsliga grunden att utföra en uppgift av allmänt intresse (att tillgängliggöra arkivhandlingar och främja användningen av arkiven).

Även om Meta skulle profilera menar förvaltningen att detta inte har några betydande konsekvenser för de registrerade. Förvaltningen uppger att man planerar att informera följare m.m. på Instagram om att deras data kan användas av Meta för profilering och uppmuntra dem att justera sina integritetsinställningar på Instagram. Dessutom kommer förvaltningen att uppmana sina följare att använda Metas onlineformulär för att invända mot att deras data används för profilering enligt Instagrams integritetspolicy. Informationen kommer att finnas på Regionarkivets webbsida ”Så behandlar Regionarkivet dina personuppgifter”.

Dataskyddsombudet ser på positivt på de åtgärder som vidtagits. Dataskyddsombudet noterar också förvaltningens bedömningar i frågan, men delar inte bedömningen att publicering av arkivhandlingar på Instagram kan göras inom ramen för arkivändamål av allmänt intresse. Dataskyddsombudet motsätter sig dock inte att det i och för sig kan finnas ett berättigat ändamål som handlar om att tillgängliggöra och främja användning av arkiv. Frågan är bara vad som utgör en proportionell personuppgiftsbehandling för detta ändamål. Dataskyddsombudet instämmer inte heller i bedömningen om att en konsekvensbedömning inte behöver göras.

Dataskyddsombudet vill uppmärksamma förvaltningen på att IMY flaggat för att en vägledning/riktlinje om offentliga myndigheters användning av sociala medier

kommer att komma. Förvaltningen rekommenderas ta del av detta material när det kommer och att vid behov anpassa sin hantering utifrån vad som sägs i det. Om det kommer klargöranden från myndigheter under 2025 som påverkar bedömningen av användningen av sociala medier, kommer dataskyddsombudet att särskilt följa upp frågan under 2025 och i annat fall följa frågan på längre sikt.

5 Rekommenderade fokusområden 2025

Dataskyddsombudet har under arbetet med årsrapporten identifierat ett antal områden som verksamheten rekommenderas att särskilt arbeta med under det kommande året. Dessa listas i punktform enligt nedan.

Detta är områden som dataskyddsombudet särskilt kommer att följa upp under året. Uppföljningen kommer ske kontinuerligt under avstämningsmöten med verksamheten, och inom ramen för den uppföljning som dataskyddsombudet genomför under hösten 2025.

Förvaltningen rekommenderas 2025 prioritera följande delar av dataskyddsarbetet:

- Kontrollpunkt 4: Register över personuppgiftsbehandlingar

Förvaltningen rekommenderas att kartlägga och dokumentera sina personuppgiftsbehandlingar enligt artikel 30 i dataskyddsförordningen. I arbetet med behandlingsregistret rekommenderar dataskyddsombudet förvaltningen att utgå ifrån dataskyddsombudets generella rapport som kommer förvaltningen till del under början av 2025.

6 Bilagor

Bilaga 1: Kontrollplan för dataskyddsarbetet 2024–2025

Göteborgs Stad

Kontrollplan för dataskyddsarbetet 2024–2025

Förvaltningar och bolag i Göteborgs Stad

2024-05-06

Innehåll

1 Bakgrund

Att få ta del av och hantera andra människors personliga uppgifter på ett sådant sätt som kommunala förvaltningar och bolag gör innebär att förvalta ett stort förtroende. Dataskyddsförordningen (GDPR) har tillkommit för att särskilt värna om den enskildes rätt till integritet och kontroll över vad som sker med ens personuppgifter. Att förvaltningar och bolag hanterar personuppgifter i enlighet med gällande lag bör vara en självklarhet i syfte att visa omsorg om det förtroende som givits den som har att hantera personuppgifter.

Det är varje nämnd och bolaget som är ytterst ansvarig för att dess verksamhet följer dataskyddslagstiftningen. För att stödja stadens nämnder och bolag i arbetet med dataskydd har ett dataskyddsombud utsetts. I Göteborgs Stad fullgör dataskyddsenheten på Intraservice uppdraget som dataskyddsombud. Dataskyddsombudet har särskild sakkunskap i dataskyddslagstiftning och arbetar bland annat för att hålla nämnden/bolaget informerade om hur verksamheten lever upp till dataskyddslagstiftningen. Vad som är dataskydds-ombudets uppgifter framgår direkt av GDPR. En av dessa uppgifter är att övervaka att stadens förvaltningar och bolag följer dataskyddslagstiftningen. När dataskyddsombudet kontrollerar efterlevnaden av dataskyddslagstiftningen sker det bland annat genom att samla in information om hur personuppgifter behandlas inom en verksamhet och genom att kontrollera hur bestämmelser och interna styrdokument som styr dataskyddsarbetet efterlevs.

1.1 Ändrad utformning av den fördjupade kontrollen 2024

Med anledning av den omorganisation som dataskyddsenheten genomgår under 2024 har den fördjupade kontrollen i år behövt anpassas till rådande förutsättningar. Detta innebär att dataskyddsombudet inte kommer att kunna genomföra kontroller inom alla Stadens verksamheter under 2024. I stället kommer kontrollen att hanteras genom stickprov och enbart genomföras inom ett urval av Stadens verksamheter. Även om alla verksamheter inte kommer kontrolleras under 2024 är dataskyddsombudets förhoppning att resultaten från kontrollen som helhet ska kunna användas av flera verksamheter och därigenom bidra till att stärka Stadens sammantagna dataskyddsarbete.

1.1.1 Uppföljning av informationsinsatsen 2023

Under våren 2023 genomförde dataskyddsenheten en informationsinsats med fokus behandlingsregistret enligt artikel 30 i GDPR. Syftet med informations-insatsen var att höja kunskapen inom området och skapa enhetlighet inom Göteborgs Stad. Som uppföljning på denna informationsinsats kommer under 2024 en fördjupad kontroll av verksamheters efterlevnad av artikel 30 i GDPR, och därigenom skyldigheten att systematiskt dokumentera alla personuppgifts-behandlingar i form av ett register, att genomföras.

2 Kontrollarbetet 2024–2025

Den övergripande och viktigaste uppgiften för dataskyddsombudet är att övervaka att organisationen följer dataskyddsförordningen. I Göteborgs Stad innebär detta bland annat att dataskyddsombudet genomför kontroller av dataskyddsarbetet inom förvaltningar och bolag. För dataskyddsombudet är kontrollarbetet ett sätt att få en bild av vilka risker och/eller brister som eventuellt föreligger inom en verksamhet. Genom kontroller kan dataskyddsombudet kartlägga verksamhetens dataskyddsarbete, och denna kartläggning kan sedan användas som ett stöd av verksamheten i dess fortsatta arbete med dataskydd. Dessa kontroller specificeras genom denna kontrollplan, som syftar till att informera personuppgiftsansvariga om upplägg och tidplan för kontrollarbetet åren 2024 och 2025. Dataskyddsombudets kontrollarbete löper över tvåårsperioder. En ny kontrollplan skickas ut årligen, vilken omfattar både innevarande och nästkommande kalenderår.

Syftet med att arbeta utefter en på förhand fastställd kontrollplan är att det ska bidra till att sätta fokus på verksamhetens dataskyddsarbete och därmed:

1. Säkerställa ett kontinuerligt dataskyddsarbete som skapar förutsättningar för efterlevnad av förordningen.
2. Uppmuntra ett riskbaserat arbetssätt och därigenom minimera risken för lagbrott.
3. Göra dataskyddsarbetet till en integrerad del i verksamhetens informationssäkerhetsarbete.

2.1 Kontrollarbetets delar

Kontrollarbetet består av tre delar som tillsammans syftar till att ge, såväl dataskyddsombud som personuppgiftsansvariga, en överblick över verksamhetens dataskyddsarbete och dess följsamhet gentemot GDPR.

Del	Beskrivning	Frekvens
Övergripande kontroll (tidigare kallad ”fasta kontrollpunkter”)	En övergripande kontroll av verksamhetens dataskyddsarbete. Verksamheten skattar det interna arbetet i en enkät uppdelad i tolv fasta kontrollpunkter.	Vartannat år
Fördjupad kontroll	En fördjupad kontroll av en eller flera utvalda kontrollpunkter.	Vartannat år
Uppföljning	Uppföljning och bedömning av hur verksamheten omhändertagit lämnande rekommendationer.	Årligen

2.1.1 Övergripande kontroll

Den övergripande kontrollen utgår från principerna om inbyggt dataskydd och dataskydd som standard (enligt artikel 25 i GDPR). Verksamhetens följsamhet mot förordningen beror till stor del på hur väl dessa principer har integrerats i ordinarie arbetsprocesser. Att principerna har en central roll i arbetet med dataskydd blir särskilt tydligt i beaktandesats (skäl) 78 i GDPR, som anger att ”skyddet av fysiska personers rättigheter och friheter i samband med behandling av personuppgifter förutsätter att lämpliga tekniska och organisatoriska åtgärder vidtas”, och därtill att den personuppgiftsansvarige, för att kunna visa att förordningen efterlevs, bör anta interna strategier och vidta åtgärder särskilt för att uppfylla principerna om inbyggt dataskydd och dataskydd som standard. Med principerna som utgångspunkt har tolv kontrollpunkter identifierats. Dessa är av både teknisk och organisatorisk karaktär och är gemensamma för alla verksamheter inom Göteborgs Stad.

Den övergripande kontrollen genomförs genom en enkät. Enkäten utgår från de tolv kontrollpunkterna där varje punkt innehåller ett antal delfrågor i form av påståenden och/eller skattningsfrågor. Resultaten från enkäten ger en generell ögonblicksbild för respektive kontrollpunkt och kan användas som vägledning för verksamheten i sitt dataskyddsarbete. Syftet är att få till ett långsiktigt och systematiskt arbetssätt, samt åskådliggöra de förändringar som vidtas över tid.

För beskrivning av de olika kontrollpunkterna, se bilaga 1.

Fasta kontrollpunkter
1. Dataskyddsorganisation
2. Personuppgiftsincidenter
3. Biträdesavtal och andra överenskommelser
4. Register över personuppgiftsbehandlingar
5. Övergripande styrning av dataskyddsarbetet
6. Utbildning
7. Informationsplikt
8. E-post och dokumenthantering
9. Konsekvensbedömning/samråd
10. IT-projekt och upphandling
11. IT-system och digitala verktyg
12. Hantering av registrerades rättigheter

2.1.2 Fördjupad kontroll

Den fördjupade kontrollen kan utgå från både staden övergripande och verksamhetsspecifika risker. I utformningen av kontrollen utgår dataskyddsombudet från de risker som identifierats, både inom enskilda verksamheter och på en övergripande nivå. Hänsyn tas även till

dataskyddsombudets resurser samt vad som bedöms kunna få störst effekt för flest verksamheter inom Staden.

2.1.3 Uppföljning av genomförda kontroller

Uppföljning av genomförda kontroller görs årligen för att se hur verksamheten har hanterat tidigare lämnade rekommendationer. Denna uppföljning kan göras både muntligen och skriftligen. Resultatet av genomförd uppföljning kommer redovisas i årsrapporten.

2.2 Tidplan för kontrollarbetet 2024–2025

I tabellerna nedan anges huvuddragen i kontrollarbetet för åren 2024–2025 för stadens förvaltningar och bolag.

2024	Aktivitet
Maj	Kontrollplan för 2024–2025 lämnas till nämnder och bolag.
Augusti – november	Fördjupad kontroll genomförs. **För 2024 har följande fokusområde för den fördjupade kontrollen fastställts:** • Kontrollpunkt 4: Register över personuppgiftsbehandlingar Kontrollen genomförs inom ett urval av Stadens verksamheter. Under augusti månad kommer information om vilka verksamheter som ingår i urvalet att tillhandahållas samtliga förvaltningar och bolag. Resultaten från kontrollen kommer redogöras för i årsrapporten samt genom särskilt informationsmöte.
November – december	Genomgång av innehåll i årsrapport med respektive förvaltning och bolag.
December	Fastställd årsrapport översänds till respektive förvaltning och bolag.

2025	Aktivitet
Februari	Kontrollplan för 2025–2026 lämnas till nämnder och bolag.
September	Övergripande kontroll genomförs.
November – december	Genomgång av innehåll i årsrapport med respektive förvaltning och bolag.
December	Fastställd årsrapport översänds till respektive förvaltning och bolag.

3 Rapportering

3.1 Årsrapport

Det är nämnd/bolag som har det yttersta ansvaret för att verksamheten följer dataskyddslagstiftningen och dataskyddsombudet ska enligt lag rapportera om detta till högsta förvaltningsnivå. Därför sammanställer dataskyddsombudet årligen en rapport om verksamhetens dataskyddsarbete. I rapporten redogörs för eventuella risker och brister som dataskyddsombudet har identifierat. I rapporten redogörs också för de råd och rekommendationer som dataskyddsombudet har lämnat. För att möjliggöra en direkt kommunikation mellan dataskyddsombud och högsta ansvarsnivå inom verksamheten ska årsrapporten tillhandahållas nämnd respektive bolagsstyrelse.

3.2 Särskilt yttrande

Dataskyddsombudet kan i vissa situationer komma att rikta ett särskilt yttrande till högsta ansvarsnivå. En sådan situation kan vara om dataskyddsombudet har identifierat höga risker för de registrerade som kräver omgående åtgärder från ansvarig nämnd/bolag. Det kan också vara om dataskyddsombudet uppmärksammar att det inom verksamheten fattats beslut som är oförenliga med dataskyddslagstiftningen och dataskyddsombudets råd.

4 Kontakt

Eventuella frågor och synpunkter på kontrollplanen hänvisas i första hand till dataskyddsenhetens enhetschef Elin Olsson Norrblom.

Frågor kan också alltid ställas till dataskyddsenheten via mejladressen; dso@intraservice.goteborg.se.

Bilaga 1 - Beskrivning av fasta kontrollpunkter

Kontrollpunkt 1: Dataskyddsorganisation

Kontrollpunkten avser verksamhetens organisatoriska förutsättningar för att kunna bedriva ett kontinuerligt dataskyddsarbete och omfattar bland annat verksamhetens dataskyddsorganisation, definierade ansvarsområden och rapporteringsvägar för involverade funktioner samt tillhandahållna resurser för arbetet.

Kontrollpunkt 2: Personuppgiftsincidenter

Kontrollpunkten avser verksamhetens förutsättningar för att identifiera och hantera personuppgiftincidenter. För att uppfylla ansvarsskyldigheten bör verksamhetens rutin för hanteringen vara dokumenterad. I de fall verksamheten är både personuppgiftsansvarig och personuppgiftsbiträde bör rutinen omfatta båda scenarier. I kontrollpunkten ingår även översyn av verksamhetens rutin för att bedöma incidenter, hantering av eventuell anmälan till tillsynsmyndigheten, samt hur rutinerna tillgängliggörs och kommuniceras inom verksamheten. Även efterlevnad av verksamhetens dokumentationsskyldighet, att alla inträffade personuppgiftsincidenter registreras, innefattas.

Kontrollpunkt 3: Biträdesavtal och andra överenskommelser

Kontrollpunkten avser verksamhetens dokumentation av biträdesavtal och andra överenskommelser gällande dataskydd och förutsätter att verksamheten har identifierat samt registrerat personuppgiftsbiträden i personuppgiftsregistret. Även verksamhetens rutiner för uppdatering och uppföljning av tecknade biträdesavtal innefattas.

Kontrollpunkt 4: Register över personuppgiftsbehandlingar

Kontrollpunkten avser verksamhetens efterlevnad av skyldigheten att systematiskt dokumentera alla personuppgiftsbehandlingar i form av ett register. Även verksamhetens arbete med, och rutin för, att säkerställa ett uppdaterat och heltäckande register innefattas.

Kontrollpunkt 5: Övergripande styrning av dataskyddsarbetet

Kontrollpunkten avser verksamhetens övergripande styrning för att arbeta med dataskydd. Tydlig styrning sätter ramarna för arbetet med dataskydd och främjar ett riskbaserat arbetssätt. Kontrollpunkten innefattar även verksamhetens arbete för att integrera dataskyddsfrågorna i det övriga informationssäkerhetsarbetet, samt hur verksamheten arbetar med egna interna kontroller för att säkerställa att dataskyddslagstiftningen efterlevs.

Kontrollpunkt 6: Utbildning

Kontrollpunkten avser verksamhetens arbete med att utbilda och upprätthålla kunskapsnivån i dataskyddsfrågor hos anställda.

Kontrollpunkt 7: Informationsplikt

Kontrollpunkten avser hur väl verksamheten uppfyller principen om öppenhet och kravet på att lämna information till de registrerade om hur deras personuppgifter behandlas. Punkten omfattar även hur verksamheten säkerställer att informationen är uppdaterad.

Kontrollpunkt 8: E-post och dokumenthantering

Kontrollpunkten avser verksamhetens rutiner för e-post och dokumenthantering. I detta är en aktuell och fastställd dokumenthanteringsplan med gallringsbeslut en förutsättning för att verksamheten ska kunna säkra följsamhet gentemot dataskyddslagstiftningen. Även verksamhetens rutin för att säkerställa att gallringsrutiner för personuppgifter följs innefattas.

Kontrollpunkt 9: Konsekvensbedömning/samråd

Kontrollpunkten avser verksamhetens förutsättningar för att kunna identifiera när en konsekvensbedömning ska göras samt genomföra denna. Även verksamhetens rutiner för arbetet med konsekvensbedömningar samt hur dataskyddsombudet involveras i arbetet ingår. Därtill tillkommer verksamhetens rutin för att hantera de risker som identifieras i konsekvensbedömningen, samt hur genomförda konsekvensbedömningar följs upp och hålls aktuella.

Kontrollpunkt 10: IT-projekt och upphandling

Kontrollpunkten avser verksamhetens organisation och rutiner för hantering av dataskyddsfrågor inom IT-projekt och upphandling. I detta ingår till exempel hur verksamheten integrerar dataskyddsfrågor i arbetet med upphandling av nya, samt utvecklingen av, befintliga system och tjänster.

Kontrollpunkt 11: IT-system och digitala verktyg

Kontrollpunkten avser verksamhetens rutiner för att säkerställa att verksamhetens personuppgiftshantering inom ramen för IT-system och digitala verktyg är förenlig med dataskyddslagstiftningen. Rutin för att säkerställa och kontrollera att dessa system/tjänster uppfyller kraven på dataskydd ingår även.

Kontrollpunkt 12: Hantering av registrerades rättigheter

Kontrollpunkten avser verksamhetens förutsättningar för att hantera de registrerades rättigheter. En förutsättning för att verksamheten ska kunna hantera de registrerades rättigheter är att man har en process och rutiner för arbetet, så att den registrerades personuppgifter enkelt kan lokaliseras vid efterfrågan. Även verksamhetens rutin för att hantera ett tillbakadragande av samtycke ingår i kontrollpunkten.