



Årsrapport för dataskyddsarbetet 2024

Grundskolenämnden

2024-12-20

Innehåll

1	Dataskydd i kommunal verksamhet	3
2	Göteborgs Stads dataskyddsombud.....	4
2.1	Stadenövergripande iakttagelser 2024	4
2.1.1	Ny central funktion för styrning och samordning i dataskyddsfrågor möjliggör ett stärkt dataskydd	4
2.1.2	Verksamhetens ledning avgörande för att GDPR inte ska fortsättas upplevas som ett hinder	5
2.1.3	Bristande ansvarstagande i Stadens arbete med AI medför risker för både enskilda och verksamheter.....	6
3	Dataskyddsombudets iakttagelser 2024.....	7
3.1	Verksamhetens dataskyddsarbete.....	7
3.2	Särskilda iakttagelser..... Fel! Bokmärket är inte definierat.	
4	Granskning av dataskyddsarbetet 2024.....	9
4.1	Fördjupad kontroll 2024	9
4.2	Uppföljning av lämnade rekommendationer	9
4.2.1	Uppföljning av verksamhetens arbete med rekommenderade fokusområden 2024	9
4.2.2	Uppföljning av rekommendationer lämnade inom ramen för tidigare genomförda kontroller	12
5	Rekommenderade fokusområden 2025	13
6	Bilagor	14

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 framtidsyftande 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 förvaltningsnivå², 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 dataskyddsombudet 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, utmålades 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 integritetssperspektiv. 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

Grundskoleförvaltningen har under året tagit fram en handlingsplan för dataskyddsarbetet 2024 som förankrats med förvaltningsledning och beslutats av direktören. Handlingsplanen utgår från de fokusområden som dataskyddsombudet uppmärksammade i årsrapporten 2023. Utifrån fokusområdena har förvaltningen identifierat de åtgärder som krävs utifrån respektive fokusområde för att kunna utarbeta en mer systematisk och strategisk inriktning i dataskyddsarbetet. För dataskyddsorganisationen är det främst aktiviteter i form av framtagande av rutiner som tidigare saknats, för register för personuppgiftsbehandlingar handlar det dels om att ta fram en rutin som redogör för roller och ansvar, dels inleda arbetet enligt ett riskbaserat arbetssätt och för konsekvensbedömningar handlar det om att identifiera behandlingar allteftersom behandlingsregistret tas fram. Förvaltningen har även följt upp och återrapporterat arbetet till nämnden. Dataskyddsombudet ser väldigt positivt på att förvaltningen tagit fram en egen handlingsplan för årets dataskyddsarbete och att den är förankrad i förvaltningsledningen.

Dataskyddsombudet rekommenderar förvaltningen att fortsätta med detta arbetssätt så att det blir en naturlig del i förvaltningens fortsatta strategiska dataskyddsarbete. Dataskyddsombudet ser även positivt på att nämnden har involverats och fått uppföljning av det arbete som bedrivits under året. Det ska samtidigt lyftas fram att dataskyddsombudet under flera år lyft just frågan om dataskyddsorganisation som varit eftersatt hos förvaltningen. Detta eftersom det strategiska arbetet med dataskyddsfrågor och uppföljningen av årsrapporten stått tillbaka för andra praktiska frågor, precis som förvaltningen själva lyfter i handlingsplanen. Dataskyddsombudets bedömning är därmed att förvaltningen har saknat en långsiktig strategi inom dataskydd. De åtgärder som vidtagits under året är en början för att få till ett strukturerat dataskyddsarbete och kan därmed utgöra en grund för ett mer långsiktigt arbete. Utifrån förvaltningens storlek kommer det dock ta tid att fullt ut implementera den nya dataskyddsorganisationen, något som dataskyddsombudet också uppfattar är förvaltningens bedömning. Det krävs ett fokuserat och långsiktigt arbete för att säkerställa dels att dataskyddsorganisationen förankras inom förvaltningen, dels att förvaltningen följer upp hur väl den fungerar i praktiken för att vid behov kunna revidera om något inte upplevs få önskad effekt. Dataskyddsombudet anser sammantaget att de steg som tagits under året är positiva och rekommenderar förvaltningen att fortsätta med arbetet, samtidigt som det kvarstår mycket arbete för att få dataskyddsorganisationen att fungera i praktiken.

Dataskyddsombudet har under året haft regelbundna avstämningar med förvaltningens centrala dataskyddsfunktion. Ett arbete har bland annat bedrivits för att uppdatera den rutin som finns för utredning av personuppgiftsincidenter. Dataskyddsombudet har uppfattat att den centrala frågan i arbetet med rutinen för

personuppgiftsincidenter är att fastställa ansvarsfördelningen inom förvaltningen vid utredning av personuppgiftsincidenter. Detta bedömer dataskyddsombudet synliggör de problem som en otydlig dataskyddsorganisation och styrning i dataskyddsfrågor medför och ytterligare stärker dataskyddsombudets uppfattning att förvaltningen aktivt behöver fortsätta arbetet med implementering av den nya dataskyddsorganisationen. Vidare har ett första utkast för en konsekvensbedömning av Google workspace for education tagits fram, men är ännu inte färdigställd. Förvaltningen har även arbetat med andra konsekvensbedömningar under året, till exempel för digitala nationella prov och för behandlingar där samverkan sker med socialtjänst. Dataskyddsombudet rekommenderar förvaltningen att ha ett fokuserat arbete med de konsekvensbedömningar som är pågående och säkerställa att dessa färdigställs. Förvaltningen har under året efterfrågat dataskyddsombudets råd i samband med hanteringen av ca 10 personuppgiftsincidenter då osäkerhet kring bedömningen uppstått. Utifrån förvaltningens storlek och antal registrerade, är det därmed många incidenter som förvaltningen hanterar på egen hand utan att rådfråga dataskyddsombudet. Förvaltningen rekommenderas att fortsätta involvera dataskyddsombudet i samband med incidenthanteringen, särskilt då det uppstår osäkerhet kring bedömning av en incident.

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: Dataskyddsorganisation

Verksamheten gavs följande rekommendationer:

Säkerställ att det nya arbetssättet efterlevs, komplettera anvisningen med de rutiner som krävs för att anvisningen i praktiken ska kunna efterlevas samt utvärdera hur arbetssättet i praktiken fungerar. Fokus bör vara på att under året skapa en ändamålsenlig och välfungerande dataskyddsorganisation inom förvaltningen.

Kommentarer och rekommendationer:

Grundskoleförvaltningen har under året tagit fram rutin för konsekvensbedömningar, rutin för förvaltningens arbete med behandlingsregistret och rutin för tecknande och översyn av personuppgiftsbiträdesavtal. Vidare har förvaltningen tagit fram en checklista för egenkontroll som komplement till anvisningen för Grundskoleförvaltningens dataskyddsorganisation och tillhörande stödjande dokument. Dessa dokument utgör tillsammans med förvaltningens anvisning för dataskyddsorganisation grunden i ett ledningssystem för dataskydd. Förvaltningens fortsatta arbete med implementering och utvärdering av dataskyddsorganisationen kommer framgå av handlingsplanen för dataskyddsarbetets inriktning 2025.

Dataskyddsombudet anser att det är positivt att förvaltningen påbörjat ett arbete med att få till stånd en ändamålsenlig dataskyddsorganisation och tagit fram rutiner som bedömts nödvändiga för att den ska kunna efterlevas. Dataskyddsombudet rekommenderar förvaltningen att fortsätta arbetet med implementering och utvärdering av den nya dataskyddsorganisationen under kommande år. Även om en omfattande utvärdering kan vara svår att göra i detta skede, bör förvaltningen ändå fokusera på huruvida det ledningssystem för dataskydd som finns har gett avsedd effekt avseende ansvarsfördelning och om den nya dataskyddsorganisationen är känd inom förvaltningen. Vidare bör förvaltningen även i en utvärdering fundera över om det saknas rutiner för att arbetet ska fungera i praktiken och/eller om det saknas ansvarsområden som behöver täckas in i anvisningen för dataskyddsorganisation.

Fokusområde 2: Register över personuppgiftsbehandlingar

Verksamheten gavs följande rekommendationer:

Göra en översyn av befintligt register. Gå igenom hur de dokumenterade behandlingarna är definierade och för respektive behandling kontrollera att informationen uppfyller kraven enligt artikel 30 i GDPR. En förutsättning för att arbetet ska kunna genomföras på ett kvalitativt sätt är att förvaltningen tillsätter tillräckliga resurser för arbetet.

Kommentarer och rekommendationer:

Förvaltningen har bedömt att det på kort tid inte är realistiskt att ta fram ett heltäckande behandlingsregister. Förvaltningen har istället under 2024 vidtagit åtgärder för att systematiskt kunna arbeta med behandlingsregistret och inleda inventeringsarbetet utifrån ett riskbaserat arbetssätt. Under höstterminen har ett arbete inletts med att inventera de behandlingar som ligger under avdelningen Styrning och lednings ansvar. Inventeringen följer ett riskbaserat arbetssätt där de verksamheter som behandlar många och känsliga uppgifter om elever kommer först. Förvaltningen har tagit fram en implementeringsplan för detta arbete och avsatt resurser för arbetets genomförande. Erfarenheterna från arbetet på avdelningen, tillsammans med den rutin för registerförteckning över

personuppgiftsbehandlingar som förvaltningen tagit fram, ska ligga till grund för förvaltningens vidare arbete med behandlingsregistret.

Dataskyddsombudet anser det vara positivt att förvaltningen påbörjat ett strukturerat arbete med behandlingsregistret. Detta är något som dataskyddsombudet efterfrågat under flera år. De inledande steg som nu tagits är därmed enligt dataskyddsombudets uppfattning en förutsättning för att kunna ta fram ett heltäckande register. Dataskyddsombudet vill i sammanhanget lyfta fram att det enligt GDPR är ett krav att ha ett komplett behandlingsregister. Samtidigt är det även en förutsättning för att överhuvudtaget kunna bedriva ett systematiskt och riskbaserat dataskyddsarbete. Avsaknad av ett behandlingsregister innebär även stora risker för de registrerade. Dataskyddsombudet rekommenderar därför förvaltningen att under kommande år tillsätta resurser i arbetet, för att under 2025 ta fram ett behandlingsregister som omfattar den absoluta majoriteten av förvaltningens behandlingar. I arbetet bör förvaltningen utgå från den stadengemensamma rapport som dataskyddsombudet tagit fram i samband med årets fördjupade kontroll avseende behandlingsregister för att säkerställa att registret uppfyller kraven i artikel 30 i GDPR.

Fokusområde 3: Konsekvensbedömningar/samråd

Verksamheten gavs följande rekommendationer:

Arbeta parallellt med översynen av behandlingsregistret med att identifiera behandlingar utifrån höga risker och ta fram en handlingsplan för genomförandet av konsekvensbedömningar för dessa behandlingar.

Kommentarer och rekommendationer:

Förvaltningens åtgärder är att parallellt med det inventeringsarbete som rör behandlingsregistret identifiera personuppgiftsbehandlingar som innebär höga risker. Arbetet har påbörjats på avdelningen för Styrning och ledning höstterminen 2024. Avdelningschefen ska efter avslutat arbete ta fram en avdelningsspecifik strategi för att hantera en eventuell ”konsekvensbedömningsskuld”. Erfarenheterna från arbetet ska även ligga till grund för förvaltningens vidare strategi för det riskbaserade arbetet med konsekvensbedömningar.

Dataskyddsombudet har inga invändningar mot hur förvaltningen valt att hantera frågan under året. Däremot rekommenderar dataskyddsombudet även i denna del att förvaltningen säkerställer att det finns tillräckliga resurser för att kunna omhänderta detta omfattande arbete. Det är ett krav enligt GDPR att genomföra konsekvensbedömningar för de behandlingar som innebär höga risker. Dataskyddsombudet förväntar sig därför, i likhet med behandlingsregistret, att förvaltningen under kommande år tar fram strategier för hur ”skulden” för konsekvensbedömningar ska hanteras allteftersom behandlingsregistret blir klart. I arbetet bör förvaltningen ha ett riskbaserat arbetssätt, så att behandlingar med högst risker prioriteras först.

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): Kontroll av användningen av samtycke som rättslig grund

Verksamheten gavs följande rekommendationer:

Förvaltningen har tagit fram en grundmall för samtycke i de fall samtycke som rättslig grund kan komma ifråga samt tillsett att den nya rutinen för hantering av ljud, film och bild i läroplattformen Vklass adresserar frågan om samtycke då det tidigare rådde missförstånd kring frågan på just detta område. Dataskyddsombudet rekommenderar förvaltningen att i stort arbeta med rekommendationerna som lämnades under 2022.

Kommentarer och rekommendationer:

Uppföljningen visar att verksamheten fortfarande har förbättringsområden inom denna kontroll. Förvaltningen har under året fokuserat på de fokusområden som dataskyddsombudet lyfte fram i årsrapporten 2023. Dataskyddsombudet rekommenderar förvaltningen att i samband med upprättande av behandlingsregister, identifierar de behandlingar där samtycke används. I de fall samtycken används behöver förvaltningen bedöma om samtycke är en lämplig rättslig grund för behandlingen och vidta åtgärder för att säkerställa att det sker på ett korrekt sätt. I de fall då samtycke är olämpligt eller onödigt behöver det säkerställas att användningen av samtycke upphör för aktuell behandling.

När förvaltningen är klar med sitt behandlingsregister behöver förvaltningen, om samtycke används som rättslig grund, vidta ytterligare åtgärder för att säkerställa att det sker på ett korrekt sätt. Det arbetet bör bedrivas utifrån lämnade rekommendationer i den fördjupade kontrollen 2022.

5 Rekommenderade fokusområden 2025

Dataskyddsombudet rekommenderar, utifrån gjorda iakttagelser och resultaten av uppföljningen, verksamheten att under 2025 fortsätta prioritera arbetet med de kontrollpunkter som rekommenderas för 2024. 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 under 2025 prioritera följande delar av dataskyddsarbetet:

- Kontrollpunkt 1: Dataskyddsorganisation

Fortsätt det påbörjade arbetet med att implementera den nya dataskyddsorganisationen och utvärdera hur arbetssättet i praktiken fungerar. Utvärderingen bör fokusera på om ledningssystemet för dataskydd har gett avsedd effekt avseende ansvarsfördelning och om den nya dataskyddsorganisationen är förankrad inom förvaltningen. Vidare bör förvaltningen även följa upp om det saknas rutiner för att arbetet ska fungera i praktiken och/eller om det saknas ansvarsområden som behöver täckas in i anvisningen för dataskyddsorganisation.

- Kontrollpunkt 4: Register över personuppgiftsbehandlingar

Fortsätt det påbörjade arbetet med behandlingsregister och tillsätt resurser i arbetet, för att säkerställa att förvaltningen under 2025 har förutsättningar för att fram ett behandlingsregister som omfattar den absoluta majoriteten av förvaltningens behandlingar. Utgå från rekommendationerna i den stadengemensamma rapporten som tagits fram i samband med årets fördjupade kontroll avseende behandlingsregister för att säkerställa att registret uppfyller kraven i artikel 30 i GDPR.

- Kontrollpunkt 9: Konsekvensbedömningar/samråd

Arbeta parallellt med översynen av behandlingsregistret med att identifiera behandlingar utifrån höga risker och ta fram en handlingsplan för genomförandet av konsekvensbedömningar för dessa behandlingar.

6 Bilagor

Bilaga 1: Kontrollplan för dataskyddsarbetet 2024–2025



Kontrollplan för dataskyddsarbetet 2024–2025

Förvaltningar och bolag i Göteborgs Stad

2024-05-06

Innehåll

1	Bakgrund	3
1.1	Ändrad utformning av den fördjupade kontrollen 2024	3
1.1.1	Uppföljning av informationsinsatsen 2023	3
2	Kontrollarbetet 2024–2025	4
2.1	Kontrollarbetets delar	4
2.1.1	Övergripande kontroll	5
2.1.2	Fördjupad kontroll	5
2.1.3	Uppföljning av genomförda kontroller	6
2.2	Tidplan för kontrollarbetet 2024–2025	6
3	Rapportering	7
3.1	Årsrapport	7
3.2	Särskilt yttrande	7
4	Kontakt	7
	Bilaga 1 - Beskrivning av fasta kontrollpunkter	8

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 dataskyddsombudets 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 informationsinsatsen var att höja kunskapen inom området och skapa enhetlighet inom Göteborgs Stad. Som uppföljning på denna informationsinsats kommer under 2024 en fördjupad kontroll av verksameters efterlevnad av artikel 30 i GDPR, och därigenom skyldigheten att systematiskt dokumentera alla personuppgiftsbehandlingar 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

dataskyddsbudets 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 personuppgiftsincidenter. 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.