Göteborgs Stad

Årsrapport för dataskyddsarbetet 2022

Valnämndens kansli

2022-12-22

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 skydda människors rätt till integritet, och för att värna var och ens rätt att få ha kontroll över vad som sker med uppgifter om ens person. 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 uppgifterna.

Arbetet med att säkerställa att personuppgifter behandlas enligt reglerna i GDPR behöver genomsyra arbetet inom de kommunala verksamheterna på alla olika plan. Det gäller allt från rutiner och processer för det dagliga arbetet, till arbetet med innovations- och digitaliseringslösningar för framtidens arbetssätt 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.

1.1 Göteborgs Stads dataskyddsombud

Dataskyddsenheten på Intraservice är Göteborgs Stads dataskyddsombud. 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. Dataskyddsombudet erbjuder också regelbundet utbildningar för stadens medarbetare. Rådgivning ges även till förvaltningar och bolag när dessa genomför konsekvensbedömningar, vilket är en skyldighet som följer av GDPR. Efter att ha identifierat ett särskilt behov av stöd i arbetet med konsekvensbedömningar, har dataskyddsenheten under 2022 tagit fram mallar och mallstöd för det arbetet.

Det är nämnd/styrelse som har det yttersta ansvaret för att verksamheterna följer dataskyddslagstiftningen och dataskyddsombudet ska enligt lag rapportera om detta till högsta förvaltningsnivå.[2] Dataskyddsombudet har inte mandat att fatta beslut åt verksamheterna. Det är i stället genom råd och rekommendationer som

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

dataskyddsombudet bistår verksamheterna med underlag för att dessa själva ska kunna fatta väl underbyggda beslut.

2 Granskning av dataskyddsarbetet 2022

2.1 Dataskyddsombudets kontrollfunktion

Dataskyddsombudets uppgift att övervaka den personuppgiftsansvariges efterlevnad av förordningen regleras i artikel 39 i GDPR. I Göteborgs Stad innebär en del av denna övervakning att dataskyddsombudet genomför kontroller av dataskyddsarbetet inom den personuppgiftsansvariges organisation.

Enligt dataskyddsregelverket ska dataskyddsombudet arbeta utifrån en riskbaserad metod som utgår från risker för de registrerades fri- och rättigheter. Genom att utgå från en sådan metod minskas risken för negativa konsekvenser även för verksamheten själv. Sådana konsekvenser kan omfatta bland annat skadestånd, sanktionsavgifter, försämrat varumärke eller minskad tillit för verksamheten.

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 därigenom hjälpa verksamheten att få en nulägesbild av hur de faktiskt ligger till i sitt dataskyddsarbete. Denna kartläggning kan sedan användas som ett stöd för verksamheten i sitt fortsatta arbete med dataskydd. Kontrollarbetets syfte är inte främst att peka ut brister utan ska ses som en vägledning för verksamheten och ett verktyg för att identifiera relevanta prioriteringar. Det är sedan upp till varje verksamhet att besluta om hur det interna dataskyddsarbetet ska utformas utifrån verksamhetens förutsättningar för att på bästa sätt kunna hantera identifierade risker. I det arbetet är dataskyddsombudet behjälplig med rådgivning utifrån verksamhetens behov och de risker som identifierats.

2.2 Fördjupad kontroll

2.2.1 Kontroll av integritetspolicyn 2022

Den fördjupade kontrollen har bestått av kontroll av verksamhetens integritetspolicy. Resultatet av kontrollen presenteras i sin helhet i bilaga 2.

Dataskyddsombudet har i rapporten avseende den fördjupade kontrollen haft flertal anmärkningar och därför lämnat ett antal rekommendationer till verksamheten att vidta åtgärder. Verksamheten har fått följande rekommendationer:

- Förtydliga och beskriv vilka behandlingar som utförs i verksamheten och vilka personuppgifter som behandlas.
- Förtydliga rättslig grund för behandlingarna.
- Tydliggör lagringstid för respektive behandling.
- Säkerställ att samtliga behandlingar, där personuppgifterna inte samlas in direkt från den registrerade, kompletteras med information om kategorier av personuppgifter och var personuppgifterna kommer ifrån.
- Förtydliga vad som gäller avseende de registrerades rättigheter och specificera för respektive behandling.
- Förtydliga informationen om tredjelandsöverföring.
- Säkerställ att integritetspolicyn och informationen har ett tydligt språk och inte innehåller bestämningsord såsom ”kan” och liknande.
- Säkerställ att de registrerade har tillgång till en aktuell och uppdaterad integritetspolicy och gör policyn tillgänglig på Stadens hemsida.
- Ta fram rutiner som beskriver hur integritetspolicyn hålls uppdaterad.

2.3 Årlig kontroll av dataskyddsarbetet

Verksamhetens interna dataskyddsarbete följs årligen upp genom en enkät. Enkäten består av tolv punkter (”fasta kontrollpunkter”) där varje punkt innehåller ett antal delfrågor i form av påståenden och/eller skattningsfrågor. Enkäten är avsedd att spänna över de viktigaste delarna inom dataskyddsarbetet för att på så sätt fånga in en större bredd av frågor. Metoden syftar till att få till ett långsiktigt och systematiskt arbetssätt som möjliggör uppföljning över tid.

2.3.1 Metod och risknivåer

I arbetet används en modell som består av fyra kategorier, vilka representerar fyra olika risknivåer. Verksamheten får utifrån sina svar ett värde som visar vilken risknivå verksamheten befinner sig på inom respektive kontrollpunkt. Genom att arbeta med risknivåer möjliggörs ett riskbaserat arbetssätt för både verksamhet och dataskyddsombud, då resultaten ger en bild av vad verksamheten behöver prioritera i dataskyddsarbetet framåt.[3]

Beskrivning av risknivåer

Risknivåer	Färgkod
Nivå 1. Höga risker identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten.	
Nivå 2. Risker identifierade som bedöms vara omfattande och/eller kräver omgående åtgärder.	
Nivå 3. Risker identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga.	

[3] I arbetet med enkäten har dataskyddsenheten utgått från Myndigheten för samhällsskydd och beredskaps (MSB) uppföljningsstruktur för den offentliga förvaltningens systematiska informationssäkerhetsarbete.

Nivå 4. Inga direkta risker av betydelse identifierade. Indikerar att verksamheten har ett systematiskt dataskyddsarbete.	

2.4 Valnämndens kanslis dataskyddsarbete 2022

I detta avsnitt anges vilken risknivå verksamheten befinner sig inom för respektive kontrollpunkt, baserat på verksamhetens svar på de fasta kontrollpunkterna. Under varje kontrollpunkt presenteras även dataskyddsombudets bedömning gällande verksamhetens risker utifrån de iakttagelser som dataskyddsombudet gjort under året.

2.4.1 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.

Dataskyddsombudets kommentarer:

Dataskyddsombudet har inget att invända mot förvaltningens skattning gällande den interna dataskyddsorganisationen. Dataskydd är inte ett prioriterat område inom verksamheten eftersom verksamheten har ett så specifikt utpekat syfte och bortsett från valår inte har så mycket aktivitet. Dataskyddsombudet anser att det är bra att det finns utpekade roller och ansvar för de fall då dataskyddsfrågorna blir aktuella. Det finns ett antal områden som den interna dataskyddsorganisationen måste prioritera och där det bör läggas tid och resurser under kommande år.

2.4.2 Kontrollpunkt 2: Personuppgiftsincidenter

Kontrollpunkten avser verksamhetens förutsättningar och rutiner för att identifiera och hantera personuppgiftincidenter.

Dataskyddsombudets kommentarer:

Förvaltningen har skattat fyra på alla punkter inom kontrollpunkten vilket indikerar att inga risker föreligger. Verksamheten har visserligen tagit fram en rutin för hantering av incidenter sedan förra årets granskning, men eftersom verksamheten inte har identifierat att en enda incident inträffat under året kan inte dataskyddsombudet bedöma hur den faktiska hanteringen går till. Det är ofta ovanligt att inte en enda incident inträffar, då även ett fel skickat mail ses som en

incident. Dataskyddsombudet rekommenderar att verksamheten fortsätter att informera alla medarbetare, även de som endast är anställda tillfälligt vid val, vad en incident är och hur de ska hanteras.

2.4.3 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.

Dataskyddsombudets kommentarer:

Dataskyddsombudet instämmer i förvaltningens bedömning och kvarstår i uppfattningen om att det finns mycket en del att göra när det kommer till hanteringen av biträden och biträdesavtal. Dataskyddsombuden ser framför allt en stor risk när det kommer till förvaltningens kompetens att bedöma hela kedjan av underbiträden vid anlitande av personuppgiftsbiträden. Förvaltningen har så vitt dataskyddsombudet vet enbart ett personuppgiftsbiträde där ansvarsfrågan är reglerad. Frågan arbetas inte aktivt med i dagsläget, men eftersom verksamheten har identifierat risker kopplat till det aktuella biträdet rekommenderar dataskyddsombudet att detta prioriteras under nästa år. En eventuell olaglig tredjelandsöverföring eller risk för tredjelandsöverföring innebär stora risker för de registrerade.

2.4.4 Kontrollpunkt 4: Personuppgiftsregister

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 personuppgiftsregister innefattas.

Dataskyddsombudets kommentarer:

Förvaltningen har inte dokumenterat några personuppgiftsbehandlingar i registret, vare sig i en excelfil eller i Draftit. Dataskyddsombudet har tidigare rekommenderat förvaltningen att identifiera sina behandlingar och säkerställa rättslig grund och ändamål för dem. Detta arbete har ännu inte gjorts och rekommendationen kvarstår, eftersom höga risker föreligger. Eftersom registret är ett krav enligt GDPR bör förvaltningen dokumentera sina behandlingar så fort som tillfälle ges. Det kvarstår alltså höga risker på kontrollpunkten som bör åtgärdas

omgående. Dataskyddsombudet rekommenderar att verksamheten kontaktar andra valnämnder i Sverige eftersom uppdragen är lika, och försöker identifiera vilka behandlingar som kan vara aktuella för sin egen verksamhet. Att identifiera vilka behandlingar som finns är en förutsättning för efterlevnad av förordningen.

2.4.5 Kontrollpunkt 5: Övergripande strategi för dataskydd

Kontrollpunkten avser verksamhetens övergripande strategi för att arbeta med dataskydd.

Dataskyddsombudets kommentarer:

Förvaltningens skattning på kontrollpunken ger ett relativt högt resultat. Eftersom förvaltningen inte jobbar aktivt med dataskyddsfrågor ställer sig dataskyddsombudet frågande till om det verkligen finns en övergripande strategi för arbetet med dataskydd och att verksamheten jobbar systematiskt med att integrera dataskyddsfrågorna i det övriga informationssäkerhetsarbetet. Av vikt är även att säkerställa att verksamhetens informationstillgångar identifieras och värderas utifrån behovet av konfidentialitet, riktighet och tillgänglighet i enlighet med stadens styrande dokument inom informationssäkerhet. Eftersom verksamheten uppgett en nolla på påståendet av hur stor andel av informationstillgångarna som är identifierade och värderade, d.v.s. “vet inte/kan inte besvara frågan”, rekommenderas verksamheten att se över sina informationstillgångar och göra detta arbete. Verksamheten rekommenderas också ta fram rutiner för följsamhet mot GDPR vid anordnande av event samt undersöka hur man kan inkorporera interna kontroller av GDPR till annan internkontroll.

2.4.6 Kontrollpunkt 6: Utbildning

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

Dataskyddsombudets kommentarer:

Dataskyddsombudet instämmer inte verksamhetens bedömning eftersom den generella kunskapen om dataskydd i verksamheten upplevs som låg och utbildningsinsatser krävs för att säkerställa att behandling av personuppgifter sker på ett korrekt sätt i den mån verksamheten är aktiv. Verksamheten rekommenderas att undersöka vilket utbildningsbehov som finns och hur verksamheten kan säkerställa att alla medarbetare - både fastanställda och tillfälliga - får den utbildning som krävs.

2.4.7 Kontrollpunkt 7: Integritetspolicy

Kontrollpunkten avser verksamhetens utformning samt tillhandahållande av dess integritetspolicy till registrerade (både internt och externt). Även verksamhetens rutin för att upprätthålla en aktuell integritetspolicy omfattas.

Dataskyddsombudets kommentarer:

Integritetspolicyn har varit den fördjupade kontrollen i år där dataskyddsombudet har lämnat rekommendationer, och gör bedömningen att det kvarstår risker för verksamheten att åtgärda kopplat till integritetspolicyn. Eftersom verksamheten har en gammal policy behöver den uppdateras, men det går inte att göra utan att verksamheten först identifierar vilka behandlingar man utför. Åtgärderna på kontrollpunkt 7 är därför kopplade till åtgärderna som behöver vidtas på kontrollpunkt 4, personuppgiftsregister.

Dataskyddsombudet rekommenderar vidare att förvaltningen ser över integritetspolicyn inför varje val, eftersom det främst är då de registrerades personuppgifter behandlas och informationsplikten blir aktuell. Utöver det vill dataskyddsombudet lyfta möjligheten för den registrerade att nå verksamhetens integritetspolicy. Dataskyddsombudets förståelse är att integritetspolicyn skickas med när man erbjuds jobb i valet, men den är svårare att hitta via verksamhetens egna sidor. Den finns inte med bland andra förvaltningar och bolags integritetspolicies på goteborg.se, utan den ligger flera klick bort. Dataskyddsombudet rekommenderar verksamheten att lägga upp en uppdaterad version av integritetspolicyn på samma plats som alla andra verksamheter i staden har dem.

2.4.8 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 dataskyddsförordningen. Även verksamhetens rutin för att säkerställa att gallringsrutiner för personuppgifter följs innefattas.

Dataskyddsombudets kommentarer:

Förvaltningen har uppgett övervägande låga svar på kontrollpunkten vilket har genererat färg orange. Dataskyddsombudet instämmer i bedömningen och anser att det föreligger stora risker på den här kontrollpunkten. En uppdaterad dokumenthanteringsplan med gallringsrutiner är en förutsättning för att förvaltningen ska kunna säkerställa principen om lagringsminimering enligt GPDR. Förvaltningen rekommenderas också se över medarbetarna informeras om

dokumenthantering och gallring, då det också säkerställer medarbetarnas möjlighet att själva följa GDPR. Det är också en stor risk att förvaltningen inte har någon uppfattning om hur stor andel av verksamhetens personuppgiftsbehandlingar som har informationsklassificerats utifrån stadens riktlinje om informationssäkerhet. Kopplat till kontrollpunkten om integritetspolicy ovan behöver förvaltningen också se över hur de registrerade informeras om hur deras personuppgifterna hanteras, vid den initiala kontakten med verksamheten.

Dataskyddsombudet vill, efter dialog med verksamheten, särskilt lyfta vikten av att ha rutiner för hantering av personuppgifter i e-post. Verksamheten uppger att e-post är deras främsta kommunikationsväg med registrerade och att det i dagsläget inte går att begränsa vilka personuppgifter som hanteras i e-post. Dataskyddsombudet rekommenderar verksamheten att erbjuda de registrerade en säker väg för kommunikation, och om det inte är möjligt, begränsa vilka uppgifter som behandlas i e-post genom att informera de registrerade. Känsliga personuppgifter ska inte hanteras i e-post och bör därför hanteras på något annat sätt, om kryptering inte är möjlig.

2.4.9 Kontrollpunkt 9: Konsekvensbedömning/samråd

Kontrollpunkten avser verksamhetens förutsättningar för att kunna identifiera när en konsekvensbedömning ska göras, samt rutiner kopplat till detta.

Dataskyddsombudets kommentarer:

Utifrån omfattningen på verksamheten och antalet personuppgiftsbehandlingar, särskilt antalet nya personuppgiftsbehandlingar som sker, är dataskyddsombudets uppfattning att verksamheten hittills inte arbetat med konsekvensbedömningar alls. I den mån verksamheten framöver kommer införa nya behandlingar som kan innebära stora risker för de registrerade behöver verksamheten öka sin kunskap kopplat till konsekvensbedömningar. Efter att man har identifierat och registrerat de behandlingar man redan utför, bör verksamheten också se över riskerna kopplat till dessa. Dataskyddsombudet är behjälpligt vid bedömningar och ska involveras i konsekvensbedömningar. Dataskyddsombudets bedömning är att den verkliga skattningen egentligen borde placera verksamheten på risknivå 1.

Eftersom konsekvensbedömningsarbetet är ett sätt för förvaltningen att hantera de risker som föreligger med behandlingar, är dataskyddsombudets rekommendation att verksamheten implementerar arbetet med konsekvensbedömningar i den övergripande strategin för dataskydd.

2.4.10 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.

Dataskyddsombudets kommentarer:

Eftersom dataskyddsombudet inte blivit involverad i några IT-projekt eller upphandlingar under året, saknas insyn i hur verksamheten arbetar i dessa frågor. Dataskyddsombudet vill dock lyfta, i och med att kunskapen om dataskydd generellt behöver höjas inom verksamheten, att det finns risker att dataskyddsperspektivet missas. Eftersom verksamheten har ett tydligt uppdrag och enbart aktivitet vissa år, är det dataskyddsombudets uppfattning att upphandling och nya IT-projekt inte sker så ofta. I den mån det görs är det viktigt att dataskyddsperspektivet omhändertas och de registrerades rättigheter säkerställs.

2.4.11 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 dataskyddsförordningen. Rutin för att säkerställa och kontrollera att dessa system/tjänster uppfyller kraven på dataskydd ingår även.

Dataskyddsombudets kommentarer:

Förvaltningen uppger en fyra på att det finns rutiner för tilldelning av behörigheter och åtkomst till IT-system, samt uppföljning av dessa vilket dataskyddsombudet ser positivt på. Eftersom förvaltningen svarat "vet ej/kan inte svara" på frågan om att säkerställa dataskyddsperspektivet vid införandet och användandet av kostnadsfria appar, ser dataskyddsombudet ett behov av att särskilt lyfta detta. För det fall som verksamheten har eller kommer att införa appar, behöver dataskyddsperspektivet omhändertas. Vid användning av cookies behöver verksamheten säkerställa att dessa uppfyller kraven i GDPR.

2.4.12 Kontrollpunkt 12: Hantering av registrerades rättigheter

Kontrollpunkten avser verksamhetens förutsättningar och rutiner för att hantera de registrerades rättigheter, till exempel registerutdrag eller radering.

Dataskyddsombudets kommentarer:

Dataskyddsombudet ser ingen anledning att ifrågasätta förvaltningens bedömning av kontrollpunkten. Dataskyddsombudet har inte blivit involverad i några frågor gällande registrerades rättigheter under året och saknar därför inblick i hur arbetet med att säkerställa dessa fungerar på förvaltningen. Medvetenheten gällande registrerades rättigheter är kopplat till den generella kunskapen om dataskydd och kan alltid höjas. Verksamheten rekommenderas att ta fram en rutin för att hantera en begäran om registerdrag samt ta fram en process för att kunna ta fram efterfrågad information.

2.5 Sammanfattande rekommendationer

För att på ett praktiskt plan kunna identifiera vad verksamheten behöver arbeta med inom ramen för respektive kontrollpunkt behövs en noggrann genomgång av enkätresultaten. I detta rekommenderas verksamheten att samråda med dataskyddsombudet för att se hur arbetet framåt bör utformas och vilka delar som bör prioriteras utifrån verksamhetens risker. Även för verksamheter med låga risker krävs kontinuerliga insatser för att denna risknivå ska bibehållas.

Utifrån identifierade risker rekommenderar dataskyddsombudet att förvaltningen/bolaget under 2023 prioriterar följande delar av dataskyddsarbetet:

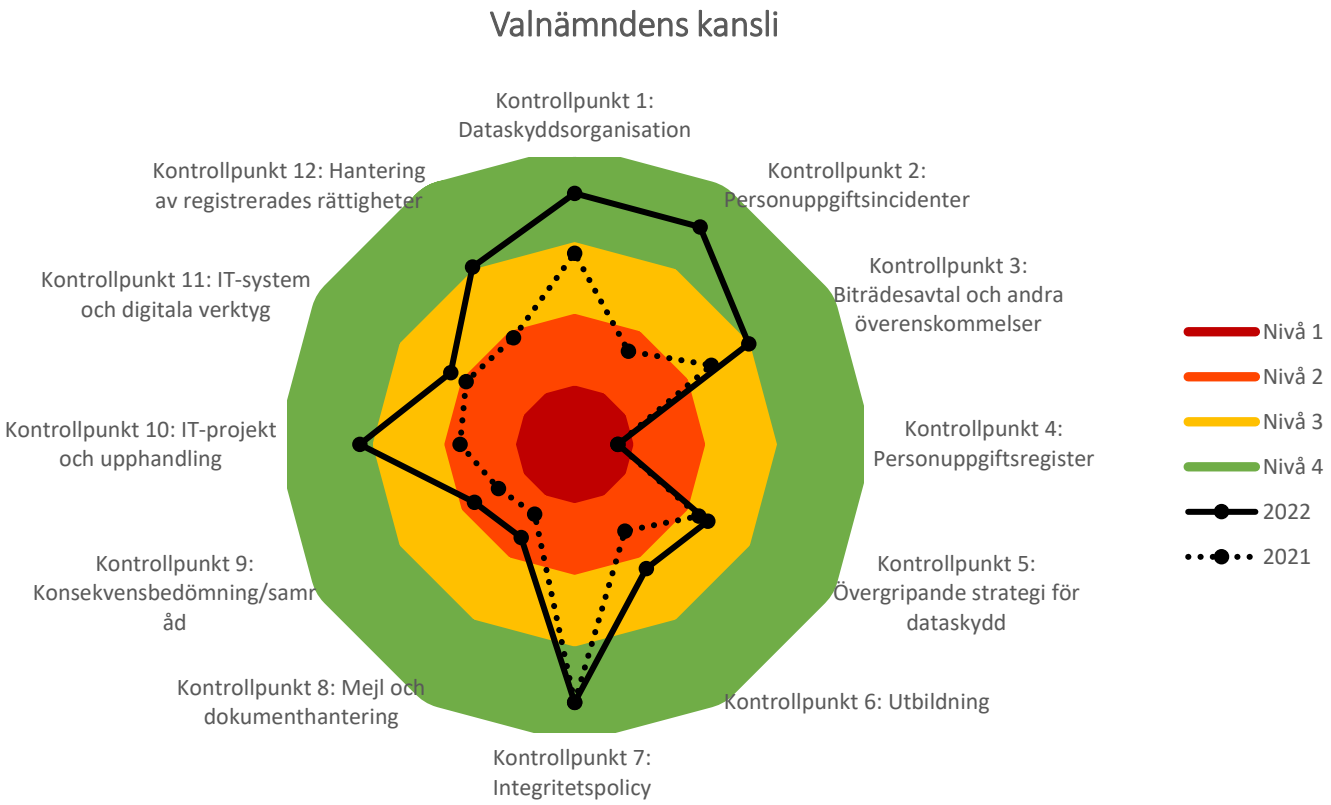
- Kontrollpunkt 4: Personuppgiftsregister
  Verksamheten rekommenderas identifiera, kartlägga och dokumentera personuppgiftsbehandlingar enligt artikel 30 i GDPR.
- Kontrollpunkt 7: Integritetspolicy
  Verksamheten rekommenderas vidta åtgärderna som framkommer i den fördjupade kontrollen, utifrån de behandlingar man identifierar enligt rekommendationerna i kontrollpunkt 4.
- Kontrollpunkt 8: Mejl och dokumenthantering
  Verksamheten rekommenderas säkerställa att det finns en uppdaterad dokumenthanteringsplan med gallringsrutiner. Dataskyddsombudet vill, efter dialog med verksamheten, särskilt lyfta vikten av att ha rutiner för hantering av personuppgifter i e-post. Verksamheten uppger att e-post är deras främsta kommunikationsväg med registrerade och att man i dagsläget inte kan begränsa vilka personuppgifter som hanteras i e-post. Dataskyddsombudet rekommenderar verksamheten att erbjuda de registrerade en säker väg för kommunikation, och om det inte är möjligt, begränsa vilka uppgifter som behandlas i e-post genom att informera de registrerade. Känsliga personuppgifter ska inte hanteras i e-post och bör därför hanteras på något annat sätt, om kryptering inte är möjlig.

3 Bilagor

Bilaga 1: Diagram över resultat av fasta kontrollpunkter, jämfört med 2021.

Bilaga 2: Fördjupad kontroll 2022 - integritetspolicy

Bilaga 1: Diagram över resultat av fasta kontrollpunkter, jämfört med 2021.



Fördjupad kontroll

Kontrollpunkt 7: Integritetspolicy

Valnämndens kansli

Bakgrund

Dataskyddsförordningen innehåller ett antal rättigheter för den registrerade, alltså den vars personuppgifter behandlas. En av dessa rättigheter är rätten till information, vilket innebär att registrerade har rätt att få information från myndigheter och bolag om hur dessa behandlar personuppgifterna som samlas in. Denna information ska som regel ges både när uppgifterna samlas in och på begäran från den registrerade. Utifrån kraven i dataskyddsförordningen ska informationen vara lättillgänglig och tillhandahållas kostnadsfritt i skriftlig form, samt vara utformad med ett klart och tydligt språk.

Ett sätt för en verksamhet att uppfylla kravet på information till registrerade är att tillhandahålla en integritetspolicy. Integritetspolicyns syfte blir då att informera registrerade om verksamhetens behandling av personuppgifter i enlighet med de krav som ställs i dataskyddsförordningen. För att integritetspolicyn ska kunna anses bidra till att en verksamhet uppfyller dess ansvarsskyldighet krävs det att policyn är utformad så att den motsvarar de krav som ställs i förordningen.

I den aktuella kontrollen har det alltså skett en granskning av verksamhetens integritetspolicy, med fokus på utformning och tillhandahållande till registrerade (både internt och externt). Även verksamhetens rutiner för att arbeta med integritetspolicyn och säkerställa att den hålls uppdaterad ingår i kontrollen. Kontrollen har genomförts i en sammanhållen del.

lakttagelser från kontrollen

Rättslig reglering och vägledning

Kravet på att ge registrerade information om behandlingen av deras personuppgifter har sin grund i artikel 5 dataskyddsförordningen (GDPR) där det anges att ”uppgifter ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade”. Vidare och mer specifika krav om hur informationen ska tillhandahållas samt vilken information som ska tillhandahållas framgår av artiklarna 12–14 GDPR. Hur dessa artiklar i sin tur ska tolkas framgår av artikel 29-gruppens vägledning om öppenhet[1] och är utgångspunkten i dataskyddsombudets kontroll och rekommendationer.

[1] Artikel 29-arbetsgruppen, *Riktlinjer om öppenhet enligt förordning (EU) 2016/*679, WP260rev.01, senast granskade och antagna den 11 april 2018.

Dataskyddsombudets rekommendationer

Generellt

Valnämndens kansli har till dataskyddsombudet skickat in dokument i form av den externa integritetspolicyn som lämnas i samband val och arbete i val. Valnämnden har ingen policy för internt bruk.

Information som ska tillhandahållas

Vilken information som ska ges till de registrerade beror på hur den personuppgiftsansvarige har samlat in personuppgifterna. Om personuppgifterna kommer direkt från den registrerade behöver det t.ex. inte lämnas information om vilka kategorier av personuppgifter som behandlingen gäller vilket det annars behöver informeras om när uppgifter kommer från någon annan än den registrerade själv.

Aktuella behandlingar, ändamål och rättslig grund

Dataskyddsombudet noterar att valnämnden i inledningen ger information i policyn som är av ett mer allmänt slag och som inte relaterar specifikt till organisationens egna personuppgiftsbehandlingar. Den första rubriken i policyn heter ”Så behandlar valnämnden dina personuppgifter”, men den information som anges under denna rubrik säger inget specifikt om hur personuppgifter behandlas i valnämnden. Även rubriken ”Syfte” ter sig missvisande i bemärkelsen att den anger generell information om vad som syftet är med själva policyn och inte vad som är syftet med valnämndens behandling av personuppgifter.

Mer ingående beskrivningar av vilka personuppgiftsbehandlingar som valnämnden hanterar ges under rubriken ”Riktlinjer”. Det listas exempel på typer av personuppgifter som behandlas, men att ange exempel är inte tillräckligt tydligt. Dataskyddsombudet betonar betydelsen av att i integritetspolicyn ange samtliga typer av personuppgifter som hanteras i verksamheten. Dataskyddsombudets bedömning är att det inte tydligt i integritetspolicyn framgår vilka behandlingar som Valnämnden utför, vilken rättslig grund som finns och vilket ändamål som är kopplat till vilken behandling. Dataskyddsombudet rekommenderar att verksamheten förtydligar vilka behandlingar som utförs.

Lagring

Utifrån integritetspolicyn är det svårt att skapa sig en bild av hur länge personuppgifterna kommer att behandlas. Valnämnden anger inga specifika gallringsfrister för några behandlingar, vilket dataskyddsombudet rekommenderar att verksamheten ändrar på. I policyn framkommer enbart att uppgifterna sparas så länge det är nödvändigt för ”*uppfylla avtalet och bevaka skyldigheter, eller med stöd i lag eller i riktlinjer*”. Generellt kan sägas att det inte är tillräckligt att informera om att personuppgifterna bevaras så länge som är nödvändigt för de berättigade ändamålen med behandlingen. Däremot kan det vara okej att i stället för specifik lagringstid ange de kriterier som bestämmer lagringstiden. Om så görs behöver kriterierna anges på ett sådant sätt att den registrerade, utifrån sin egen situation, kan bedöma lagringstiden för särskilda

uppgifter/ändamål.[2] Dataskyddsombudets bedömning är att informationen om lagringstider är alldeles för vag och behöver förtydligas.

Kategorier av personuppgifter

Avseende den externa integritetspolicyn noterar dataskyddsombudet att all insamling av personuppgifter som verksamheten gör, inte sker direkt via den registrerade. Verksamheten har uppgett exempel på andra sätt som de samlar in uppgifter, men det framkommer inte om listan är uttömmande. Dataskyddsombudet rekommenderar att verksamheten förtydligar och i de fall som personuppgifterna inte samlas in av den registrerade, behöver ange vilka kategorier av personuppgifter som bolaget behandlar och var uppgifterna kommer ifrån.

Registrerades rättigheter

Avseende de registrerades rättigheter så framgår det av vägledningen att informationen om dessa rättigheter bör vara specifik för behandlingen i fråga och innehålla en sammanfattning av vad rättigheten innebär, hur den registrerade kan gå till väga för att utöva den och vilka begränsningar som rättigheten eventuellt omfattas av. Rätten att invända mot behandlingen (i de fall rättigheten är tillämplig) måste kommuniceras till den enskilde senast vid den första kontakten. Informationen om rätten att invända ska redovisas klart och tydligt och åtskilt från annan information.[3]

I integritetspolicyn tillhandahåller Valnämnden information om vilka rättigheter de registrerade har, samt hur de kan komma i kontakt med den personuppgiftsansvarige eller dataskyddsombudet. Eftersom inte alla rättigheter är uppräknade, rekommenderar dataskyddsombudet att verksamheten uppdaterar texten med alla tillämpliga rättigheter för att den registrerade ska få all korrekt information. I händelse av att den registrerade vill rikta klagomål hänvisar Valnämnden till Datainspektionen, som numer heter Integritetsskyddsmyndigheten. Dataskyddsombudet rekommenderar valnämnden att uppdatera informationen eftersom den är felaktig.

Överföring till tredjeland

Valnämnden uppger i sin policy att de aldrig kommer överföra personuppgift till ett land utanför EU. Dataskyddsombudet rekommenderar att förvaltningen ser över denna skrivning utifrån de behandlingar som faktiskt sker av personuppgifter i verksamheten. Antingen behandlar verksamheten personuppgifterna inom EU/EES och kan ange att så sker eller så gör verksamheten inte det och då ska information i enlighet med art. 13.1 f och 14.1 f GDPR lämnas.

[2] Artikel 13.2 a och 14.2 a GDPR, samt artikel 29-arbetsgruppen, *Riktlinjer om öppenhet enligt förordning (EU) 2016/679*, WP260rev.01, senast granskade och antagna den 11 april 2018, s. 38 (bilaga).
[3] Artikel 29-arbetsgruppen, *Riktlinjer om öppenhet enligt förordning (EU) 2016/679*, WP260rev.01, senast granskade och antagna den 11 april 2018, s. 40f (bilaga).

Lättillgänglig form

Kravet på att informationen ska vara lättillgänglig innebär att de registrerade inte ska behöva leta reda på informationen. Det ska vara direkt uppenbart för dem var och hur de kan få åtkomst till informationen.

Valnämndens integritetspolicy finns tillgänglig på verksamhetens egen hemsida, men den är ett par klick bort. Det är inte heller tydligt för den registrerade hur man hittar till integritetspolicyn. Eftersom integritetspolicyn inte heller finns tillgänglig bland övriga verksamheters policy på goteborg.se, anser dataskyddsombudet att policyn inte är lättillgänglig för den registrerade. Valnämnden rekommenderas att åtgärda detta.

Klart och tydligt språk

Kravet om ett klart och tydligt språk innebär att informationen bör ges på ett så enkelt sätt som möjligt och att komplicerade meningar och språkstrukturer bör undvikas. Informationen bör vara konkret och exakt, och den bör inte vara abstrakt eller tvetydig eller kunna tolkas på olika sätt. Framför allt bör syftena med och de rättsliga grunderna för behandlingen av personuppgifterna vara tydliga. Bestämningsord som “får”, “kan”, “viss”, “ofta” och “eventuellt” bör undvikas, om man inte kan visa varför sådant språk är nödvändigt. Språket bör inte vara överdrivet formalistiskt, tekniskt eller specialiserat.

Dataskyddsombudet rekommenderar att verksamheten ser över policyn i de delar då bestämningsord förekommer, bland annat när det kommer till skrivningarna om när personuppgifter kan komma att behandlas, för vilka ändamål de behandlas och med vilka personuppgifter delas, då där förekommer ord som ”kan” exempelvis.

Rutin för uppdatering

Verksamheten har ingen rutin för att uppdatera policyn, vilket dataskyddsombudet rekommenderar att verksamheten åtgärdar.

Övrigt

Dataskyddsombudet vill särskilt lyfta att det saknas behandlingar i integritetspolicyn. Det kan vara okej att inte ha en heltäckande integritetspolicy. I de fall en personuppgiftsansvarig har väldigt många personuppgiftsbehandlingar så kan det till och med vara så att det inte är lämpligt att samla alla dessa i en integritetspolicy. En förutsättning för att detta ska vara okej är dock att all information som ska lämnas enligt art. 13-14 GDPR, lämnas till de registrerade på annat vis. Verksamheten har inte angett att så sker, varför dataskyddsombudet rekommenderar att verksamheten antingen uppdaterar sin integritetspolicy så att den är heltäckande eller säkerställer att information lämnas till de registrerade på annat vis. Om fler behandlingar läggs till i integritetspolicyn

bör verksamheten utveckla tillämpningen av en skiktad metod där den enskilde, beroende vem denne är, snabbt kan finna den information som är relevant för denne.[4]

Slutligen vill dataskyddsombudet också uppmärksamma Valnämnden på att den integritetspolicy som tillhandahållits dataskyddsombudet inte är den samma som går att hitta på verksamhetens hemsida. Dataskyddsombudet rekommenderar att verksamheten omgående gör en uppdaterad och aktuell version av integritetspolicyn tillgänglig för de registrerade.

Sammanfattade rekommendationer

- Förtydliga och beskriv vilka behandlingar som utförs i verksamheten och vilka personuppgifter som behandlas.
- Förtydliga rättslig grund för behandlingarna.
- Tydliggör lagringstid för respektive behandling.
- Säkerställ att samtliga behandlingar, där personuppgifterna inte samlas in direkt från den registrerade, kompletteras med information om kategorier av personuppgifter och var personuppgifterna kommer ifrån.
- Förtydliga vad som gäller avseende de registrerades rättigheter och specificera för respektive behandling.
- Förtydliga informationen om tredjelandsöverföring.
- Säkerställ att integritetspolicyn och informationen har ett tydligt språk och inte innehåller bestämningsord såsom ”kan” och liknande.
- Säkerställ att de registrerade har tillgång till en aktuell och uppdaterad integritetspolicy och gör policyn tillgänglig på Stadens hemsida.
- Ta fram rutiner som beskriver hur integritetspolicyn hålls uppdaterad.

Bilagor

- Frågor och informationsutskick

[4] Artikel 29-arbetsgruppen, *Riktlinjer om öppenhet enligt förordning (EU) 2016/679*, WP260rev.01, senast granskade och antagna den 11 april 2018, s. 19ff.

Information om fördjupad kontroll 2022

Kontrollpunkt 7: Integritetspolicy

Dataskyddsförordningen innehåller ett antal rättigheter för den registrerade, alltså den vars personuppgifter behandlas. En av dessa rättigheter är rätten till information, vilket innebär att registrerade har rätt att få information från myndigheter och andra verksamheter om hur dessa behandlar personuppgifterna som samlas in. Denna information ska som regel ges både när uppgifterna samlas in och på begäran från den registrerade. Utifrån kraven i dataskyddsförordningen ska informationen vara lättillgänglig och tillhandahållas kostnadsfritt i skriftlig form, samt vara utformad med ett klart och tydligt språk.

Ett sätt för en verksamhet att uppfylla kravet på information till registrerade är att tillhandahålla en integritetspolicy. Integritetspolicyns syfte blir då att informera registrerade om verksamhetens behandling av personuppgifter i enlighet med de krav som ställs i dataskyddsförordningen. För att integritetspolicyn ska kunna anses bidra till att en verksamhet uppfyller dess ansvarsskyldighet krävs det att policyn är utformad så att den motsvarar de krav som ställs i förordningen.

Granskningen avser kontrollera verksamhetens integritetspolicy, med fokus på utformning och tillhandahållande till registrerade (både internt och externt). Även verksamhetens rutiner för att arbeta med integritetspolicyn och säkerställa att den hålls uppdaterad ingår i kontrollen.

Tillvägagångssätt

Den fördjupade kontrollen kommer att genomföras i två delar. I del ett ombeds ni att skicka in dokumenterade integritetspolicys, rutiner samt besvara ett antal frågor. I del två kommer uppföljande frågor att ställas.

Dataskyddsombudet kommer sedan att sammanställa underlaget i en delårsrapport som lämnas till er i juni.

Fördjupad kontroll 2022

Kontrollpunkt 7: Integritetspolicy (del 1)

Dokumentation för er att skicka in till dataskyddsombudet:

1. Extern integritetspolicy (den policy som används för att informera medborgarna – kunder, besökare etc. – om de personuppgiftsbehandlingar som ni utför. Om ni har flera olika policys ombeds ni skicka in samtliga.)
    a. Skicka även med länkar till var informationen går att hitta så att dataskyddsombudet kan kontrollera tillgängligheten.
2. Intern integritetspolicy (den policy som används för att informera anställda/konsulter etc. om de personuppgiftsbehandlingar som ni utför. Om ni har flera olika policys ombeds ni skicka in samtliga.)
    a. Beskriv hur och när anställda/konsulter etc. får ta del av informationen.

Övrigt:

1. Har ni rutiner för att säkerställa att informationen i era integritetspolicys hålls uppdaterad?
    a. Om ja, beskriv rutinerna eller bifoga underlag där dessa framgår.
    b. Vem/vilken roll ansvarar för uppdateringen?

Underlaget ska ha inkommit till dataskyddsombudet **senast den 8 mars 2021.**

Har du frågor, kontakta ditt huvudansvariga dataskyddsombud.