Göteborgs Stad

Årsrapport för dataskyddsarbetet 2022

Kulturförvaltningen

2022-12-30

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

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

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 integritetspolicy 2022

Den fördjupade kontrollen har bestått av en granskning av kulturförvaltningens externa och interna integritetspolicyer. Resultatet av kontrollen presenteras i sin helhet i bilaga 2.

Dataskyddsombudet har i rapporten avseende den fördjupade kontrollen haft ett flertal anmärkningar och därför lämnat ett antal rekommendationer till verksamheten. Följande sammanfattande rekommendationer har lämnats:

- Kulturförvaltningen rekommenderas ta ett helhetsgrepp i frågan om integritetspolicyerna och utreda hur frågan ska hanteras i alla olika verksamhetsdelar och kanaler för att säkerställa att informationskravet är uppfyllt.

- Kulturförvaltningen rekommenderas att förbättra strukturen i integritetspolicyerna så att det blir tydligt vilka enskilda behandlingar som finns och vilka personuppgifter som hanteras i respektive behandling, samt ändamål och rättslig grund. Lagringstiden behöver tydliggöras för respektive behandling och information lämnas om personuppgiftsbehandlingar som innebär en tredjelandsöverföring.
- Kulturförvaltningen rekommenderas säkerställa att det är lätt för registrerade att få åtkomst till informationen i integritetspolicyerna via förvaltningens webbsidor och övriga kanaler.
- Kulturförvaltningen rekommenderas att ta fram en rutin för att säkerställa att integritetspolicyerna ses över regelbundet och att informationen i dem hålls aktuell.
- Kulturförvaltningen rekommenderas att ta fram en intern integritetspolicy för att säkerställa att de anställda får information om de personuppgiftsbehandlingar som omfattar deras personuppgifter.

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 Kulturförvaltningens 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:

Verksamhetens svar avseende förutsättningarna för att kunna bedriva ett kontinuerligt och systematiskt dataskyddsarbete genererar ett resultat som visar på att det finns risker identifierade, men som inte bedöms vara brådskande, omfattande eller allvarliga.

Verksamheten anger att det stämmer bra att det finns en intern organisation för dataskyddsarbetet där roller och ansvar är tydligt definierade. De anser vidare att det stämmer bra att det finns särskilda befattningar med utpekat ansvar, att det finns möjlighet att rapportera om dataskyddsarbetet till högsta förvaltningsnivå och att de har regelbunden kontakt med dataskyddsombudet. Däremot behöver dataskydd bli en mer naturlig och integrerad del i det dagliga arbetet i alla delar av verksamheten eftersom det inte är det idag. Det anges även att den interna dataskyddsorganisationen inte har tillräckliga resurser för att kunna bedriva ett systematisk dataskyddsarbete.

Dataskyddsombudet anser att verksamheten i många delar har goda förutsättningar att bedriva ett effektivt och välfungerande dataskyddsarbete. Det finns en kompetent och engagerad intern dataskyddsorganisation som lyfter många och viktiga dataskyddsfrågor med dataskyddsombudet. Det är därför viktigt att verksamheten fortsätter stödja och prioritera det interna dataskyddsarbetet och att möjligheter ges för att förbättra arbetet ytterligare. Dataskyddsombudet rekommenderar att verksamheten ser över resursbehovet och säkerställer att ett systematiskt dataskyddsarbete kan bedrivas. Verksamheten behöver även arbeta för att dataskydd blir en naturlig och integrerad del i verksamhetens dagliga arbete.

2.4.2 Kontrollpunkt 2: Personuppgiftsincidenter

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

Dataskyddsombudets kommentarer:

Verksamheten har skattat höga värden på flera av påståenden under denna kontrollpunkt. Sammantaget genererar svaren ett högt resultat som innebär att inga direkta risker av betydelse har identifierats och indikerar att verksamheten har organisatoriska förutsättningar för att för att identifiera och hantera personuppgiftincidenter.

Verksamheten anger att de har rutiner på plats för att hantera personuppgiftsincidenter och att dessa regelbundet ses över och utvärderas. Samtliga inträffade incidenter under senaste året som inneburit en rapporteringsskyldighet har rapporterat inom angivna tidsfristen om 72 timmar till tillsynsmyndigheten. Vidare uppger verksamheten att de systematiskt följer upp inträffade personuppgiftsincidenter som en naturlig del i dataskyddsarbetet. Medarbetare informeras om vad personuppgiftsincidenter är och rutinerna för hanteringen av dessa.

Dataskyddsombudets uppfattning är att det bedrivs ett bra arbete med att identifiera och hantera inträffade personuppgiftsincidenter. Verksamheten kontaktar vid behov dataskyddsombudet när incidenter har inträffat för att stämma av den fortsatta handläggningen. Verksamheten anger att de inte har tillräckliga rutiner för när och hur information till registrerade ska tillhandahållas samt vilken information som ska lämnas. Dataskyddsombudet har bland annat i föregående års årsrapport rekommenderat verksamheten att ta fram rutiner för bedömningen av hög risk och information till registrerade. Dataskyddsombudet vidhåller den rekommendation som lämnats.

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:

Resultatet av verksamhetens skattning av dataskyddsarbetet med biträdesavtal och andra överenskommelser genererar sammantaget ett resultat som indikerar att det finns risker identifierade men att de inte bedöms vara brådskande, omfattande eller allvarliga.

Att reda ut rollerna inom dataskydd är en av de svårare men också en av de absolut viktigaste utmaningarna i dataskyddsarbetet. En personuppgiftsansvarig behöver säkerställa att samtliga personuppgiftsbiträden har identifierats och att nödvändiga avtal har tecknats.

Verksamheten anger att det finns rutiner för bedömningen om en ny leverantör är ansvarig för personuppgiftsbehandlingen eller biträde samt för tecknandet av biträdesavtal. Det finns tecknade personuppgiftsbiträdesavtal för uppskattningsvis 50% verksamhetens anlitade personuppgiftsbiträden. Dataskyddsombudet rekommenderar därför verksamheten att fortsätta kartläggningen av personuppgiftsbiträden och upprätta personuppgiftsbiträdesavtal i de fall det saknas.

Verksamheten uppger vidare att det inte finns tillräckliga rutiner för att kontinuerligt genomföra efterlevnadskontroller och för att bedöma andra typer av överenskommelse/avtal som behövs upprättas avseende gemensam/eller delad hantering av personuppgifter. Tillräckliga rutiner saknas även för att bedöma hela kedjan av underbiträden vid anlitandet av nya personuppgiftsbiträden. Dataskyddsombudet rekommenderar verksamheten att arbeta vidare med dessa frågor och ta fram nödvändiga rutiner. En rutin för dokumenteringen av hela kedjan av underbiträden behövs exempelvis för att få en bättre överblick av en behandling och på så vis kunna se om det finns risker för tredjelandsöverföring eller liknande.

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:

Verksamheten har skattat höga värden på flera av påståendena under denna kontrollpunkt. Sammantaget genererar svaren ett högt resultat som innebär att inga direkta risker av betydelse har identifierats och indikerar att verksamheten har en god efterlevnad av skyldigheten att ha ett personuppgiftsregister.

Verksamheten uppskattar att upp till 75 % av behandlingarna är dokumenterade i personuppgiftsregistret. Vidare anges att de dokumenterade behandlingarna

innehåller all obligatorisk information som krävs enligt artikel 30 i GDPR. Dataskyddsombudet rekommenderar verksamheten att fortsätta det goda arbetet för att säkerställa att samtliga behandlingar dokumenteras i personuppgiftsregistret.

Ett aktuellt och uppdaterat personuppgiftsregister kan vara ett användbart hjälpmedel i verksamhetens dataskyddsarbete. Det är därför viktigt att verksamheten fortsätter att systematiskt dokumentera alla behandlingar och att möjligheter ges för att förbättra arbetet och tillhörande rutiner ytterligare.

2.4.5 Kontrollpunkt 5: Övergripande strategi för dataskydd

Kontrollpunkten avser verksamhetens övergripande strategi för att arbeta med dataskydd.

Dataskyddsombudets kommentarer:

Resultatet av verksamhetens skattning av den övergripande strategin för arbetet med dataskydd genererar sammantaget ett resultat som indikerar att det finns risker identifierade men att de inte bedöms vara brådskande, omfattande eller allvarliga.

Verksamheten anger under denna punkt att det finns en övergripande strategi för arbetet med dataskydd och att arbetet sker systematiskt med att integrera dataskyddsfrågorna i informationssäkerhetsarbetet. Det finns därutöver ett riskbaserat arbetssätt i dataskyddsfrågor och man genomför regelbundna interna kontroller för att säkerställa följsamheten gentemot GDPR.

Verksamheten uppger dock att det inte finns rutiner för att säkerställa att styrande dokument som reglerar verksamhetens personuppgiftsbehandlingar hålls uppdaterade. Dataskyddsombudet rekommenderar att sådana rutiner tas fram. Verksamheten har därutöver endast identifierat och värderat upp till 50% av informationstillgångarna i enlighet med stadens styrande dokument och dataskyddsombudet rekommenderar att verksamheten vidtar de åtgärder som behövs inom detta område.

2.4.6 Kontrollpunkt 6: Utbildning

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

Dataskyddsombudets kommentarer:

Resultatet av verksamhetens skattning av utbildning inom dataskyddsområdet genererar sammantaget ett resultat som indikerar att det finns risker identifierade men att de inte bedöms vara brådskande, omfattande eller allvarliga.

Verksamhetens svar på enkäten i denna del indikerar att medarbetarna regelbundet ges möjlighet att delta i utbildningar och informationsinsatser inom dataskydd. Trots detta saknas det en tillräckligt god allmän kunskapsnivå inom verksamheten som i sin tur skulle kunna skapa goda förutsättningar i dataskyddsarbetet. Det saknas även rutiner för att följa upp och bibehålla kunskapsnivån hos medarbetare. Dataskyddsombudet rekommenderar verksamheten att kartlägga utbildningsnivån inom förvaltningen och undersöka vilka utbildningsinsatser man behöver fokusera på samt till vilka målgrupper utbildningarna ska ges. Verksamheten rekommenderas också ta fram och besluta om en långsiktig utbildningsplan och rutiner som gäller för alla medarbetare som kräver kunskaper i dataskydd.

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:

Resultatet av verksamhetens skattning av utformningen och tillhandahållandet av integritetspolicyn genererar sammantaget ett resultat som indikerar att det finns risker identifierade men att de inte bedöms vara brådskande, omfattande eller allvarliga.

Integritetspolicyns syfte är att informera registrerade om verksamhetens behandling av personuppgifter. Av bestämmelserna i GDPR framgår vilka krav som ställs på informationen. Verksamheten anger under denna punkt att informationen i integritetspolicyn är tydlig och lättillgänglig samt att de registrerade på ett enkelt sätt kan nå verksamhetens integritetspolicy från verksamhetens samtliga digitala kanaler. Även medarbetare informeras om hur deras personuppgifter behandlas. Utifrån resultatet av enkäten rekommenderar dataskyddsombudet verksamheten att säkerställa att kravet på information enligt GDPR uppfylls genom integritetspolicyn och att policyn uppdateras vid behov. Då dataskyddsombudet genomfört en fördjupad kontroll avseende integritetspolicyn så hänvisas dessutom till resultatet av kontrollen som presenteras i sin helhet i bilaga 2 till årsrapporten.

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:

Resultatet av verksamhetens skattning av rutiner för e-post och dokumenthantering genererar sammantaget ett resultat som indikerar att det finns risker identifierade men att de inte bedöms vara brådskande, omfattande eller allvarliga.

Verksamheten har en dokumenthanteringsplan med gallringsbeslut och det finns bland annat rutiner för att kontrollera så att handlingar gallras i enlighet med gällande gallringsbeslut. Dataskyddsombudet vill dock påminna om att det alltid är viktigt att kontinuerligt se till så att dokumenthanteringsplanen är aktuell och att den omfattar samtliga av verksamhetens processer.

Utifrån svaren framgår att verksamheten behöver informationsklassificera sina personuppgiftsbehandlingar. Dataskyddsombudet rekommenderade i årsrapporten för 2021 att verksamheten skulle informationsklassificera samtliga sina personuppgiftsbehandlingar och säkerställa att de klassningar som gjorts är aktuella. Dataskyddsombudet vidhåller den rekommendation som lämnats.

Verksamheten behöver vidare säkerställa att de registrerade, vid kontakt med förvaltningen, får information om hur deras personuppgifter hanteras. Det finns även behov av rutiner avseende hur personuppgifter ska hanteras i e-postmeddelanden.

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:

Resultatet av verksamhetens skattning av dataskyddsarbetet med konsekvensbedömningar genererar sammantaget ett resultat som indikerar att det finns risker identifierade men att de inte bedöms vara brådskande, omfattande eller allvarliga.

Syftet med konsekvensbedömningar är att förebygga risker och på så sätt även minimera riskerna vid sådana behandlingar av personuppgifter som innebär en hög risk för de registrerades fri- och rättigheter. Arbetet med konsekvensbedömningar behöver inledas i ett tidigt skede vid nya eller förändrade behandlingar och vid införanden behöver man ta höjd för att arbetet kräver tid, resurser och korrekt kompetens. Detta arbete är till stor del avhängigt den generella medvetenheten om dataskydd inom förvaltningen som helhet och dataskyddsorganisationen i stort. Detta eftersom det behöver vara tydligt vart inom verksamheten som bedömningar av behov av konsekvensbedömningar ska göras, vilka som fattar beslut om genomförandet och sedermera också beslutar om de risker som konsekvensbedömningen belyser.

Avseende konsekvensbedömningar uppger verksamheten att det finns rutiner/arbetssätt för att identifiera personuppgiftsbehandlingar med hög risk för de registrerades fri- och rättigheter och metod för att inhämta och dokumentera dataskyddsombudets synpunkter när konsekvensbedömning inte bedöms behövas genomföras. Verksamheten har därutöver rutiner för att genomföra och dokumentera konsekvensbedömningar innan behandlingen påbörjas samt för att involvera dataskyddsombudet i detta arbete. Verksamheten behöver dock se till så att det finns rutiner även för att uppdatera befintliga konsekvensbedömningar vid förändringar. Under det gångna året har verksamheten arbetat en del med tröskelanalyser och dataskyddsombudet tycker det är positivt att verksamheten börjat arbeta mer aktivt med dessa frågor. Det är därför viktigt att fortsätta de processer som påbörjats och att arbeta utifrån de rutiner som verksamheten tagit fram.

Verksamheten anger att de inte vet/inte kan besvara för hur många av sina personuppgiftsbehandlingar de genomfört konsekvensbedömning utifrån hög risk eller för att det krävs enligt Integritetsskyddsmyndighetens lista. Det finns inte heller en planering som omfattar alla de behandlingar för vilka en konsekvensbedömning krävs. Denna oklarhet är i sig en risk och dataskyddsombudet rekommenderar därför att verksamheten kartlägger de personuppgiftsbehandlingar som kan innebära en hög risk för registrerades fri- och rättigheter. Därefter bör en handlingsplan tas fram för att på sikt säkerställa att konsekvensbedömningar genomförs för samtliga behandlingar där detta krävs.

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:

Resultatet av verksamhetens skattning av dataskyddsrutiner för IT-projekt och upphandling genererar sammantaget ett resultat som indikerar att det finns risker identifierade men att de inte bedöms vara brådskande, omfattande eller allvarliga.

Verksamheten uppger att de har organisatoriska förutsättningar och rutiner för att arbeta med dataskyddsfrågor inom IT-projekt och upphandling. Dataskyddsombudet rekommenderar verksamheten att fortsätta det goda arbetet inom detta område samt att fortsätta involvera dataskyddsombudet på samma sätt som den interna dataskyddsorganisationen gjort under det gångna året.

Dataskyddsombudet vill även skicka med att det är viktigt att kontinuerligt se över och säkerställa att det finns väl fungerade rutiner för upphandlingen av nya system/tjänster. Vid upphandlingar behöver det tas med i kravställningen att det

finns en anpassning till inbyggt dataskydd och dataskydd som standard. Det är nämligen viktigt redan vid upphandlingen av exempelvis ett IT-system att ta hänsyn till integritetsskyddet och bygga in funktioner som stödjer detta. Det ska även kontrolleras vid avrop och förnyad konkurrensutsättning att detta beaktats i ramavtalet.

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:

Resultatet av verksamhetens skattning av dataskyddsrutiner för IT-system och digitala verktyg genererar sammantaget ett resultat som indikerar att det finns risker identifierade men att de inte bedöms vara brådskande, omfattande eller allvarliga.

Verksamheten har överblick över sina IT-system och digitala verktyg samt rutiner för tilldelning av behörigheter och åtkomst till dessa. Medarbetarnas behörigheter och möjlighet att komma åt uppgifter i systemen och verktygen följs regelbundet upp. Dataskyddsombudet rekommenderar dock verksamheten att kontrollera så att IT-system och digitala verktyg används på rätt sätt och att det finns rutiner för systematisk uppföljning av användningen. Eftersom IT-system och digitala verktyg är några av de främsta arbetsredskapen inom en verksamhet är det dessutom alltid betydelsefullt att säkerställa så att det finns målgruppsanpassad information om hur personuppgifter behandlas i de digitala verktygen och IT-systemen samt att denna information kontinuerligt uppdateras. I detta innefattas även att se till så att införandet och användandet av kostnadsfria tjänster så som gratis appar och sociala medier sker i överensstämmelse med reglerna i GDPR.

Verksamheten behöver även säkerställa att eventuell användning av cookies på deras webbsidor följer kraven enligt GDPR och att de registrerade får information i integritetspolicyn om denna användning. Därutöver behöver verksamheten dokumentera och ha en tydlig överblick över vilka kommunikationskanaler som används inom verksamheten.

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:

Verksamheten har skattat sig högt på denna kontrollpunkt. Resultatet av verksamhetens skattning av rutiner för att hantera de registrerades rättigheter genererar sammantaget ett högt resultat som innebär att inga direkta risker av betydelse har identifierats.

Resultatet visar att verksamheten har goda förutsättningar för att hantera de registrerades rättigheter. Dataskyddsombudet vill påminna om att det är viktigt att verksamheten även fortsättningsvis arbetar systematiskt med att se över och förbättra verksamhetens rutiner och processer för att säkerställa efterlevnaden av de registrerades rättigheter.

Svaren i enkäten indikerar att det inte finns en tillräckligt utbredd medvetenhet hos medarbetarna inom verksamheten om de rättigheter som de registrerade har och i vilka fall rättigheterna kan begränsas. Dataskyddsombudet rekommenderar att verksamheten kartlägger kunskaperna angående registrerades rättigheter för att veta om verksamhetens medarbetare har behov av en riktad utbildning inom området.

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 under 2023 prioriterar följande delar av dataskyddsarbetet:

- Kontrollpunkt 1: Dataskyddsorganisationen
  Säkerställ att den interna dataskyddsorganisationen har tillräckliga resurser för att kunna bedriva ett systematisk dataskyddsarbete.

- Kontrollpunkt 3: Biträdesavtal och andra överenskommelser
  Fortsätt kartläggningen av personuppgiftsbiträden och upprätta personuppgiftsbiträdesavtal i de fall det saknas.

- Kontrollpunkt 9: Konsekvensbedömning/samråd
  Kartlägg de personuppgiftsbehandlingar som innebär en hög risk för registrerades fri- och rättigheter och ta fram en handlingsplan för att på sikt säkerställa att konsekvensbedömningar genomförs för samtliga behandlingar där detta krävs.

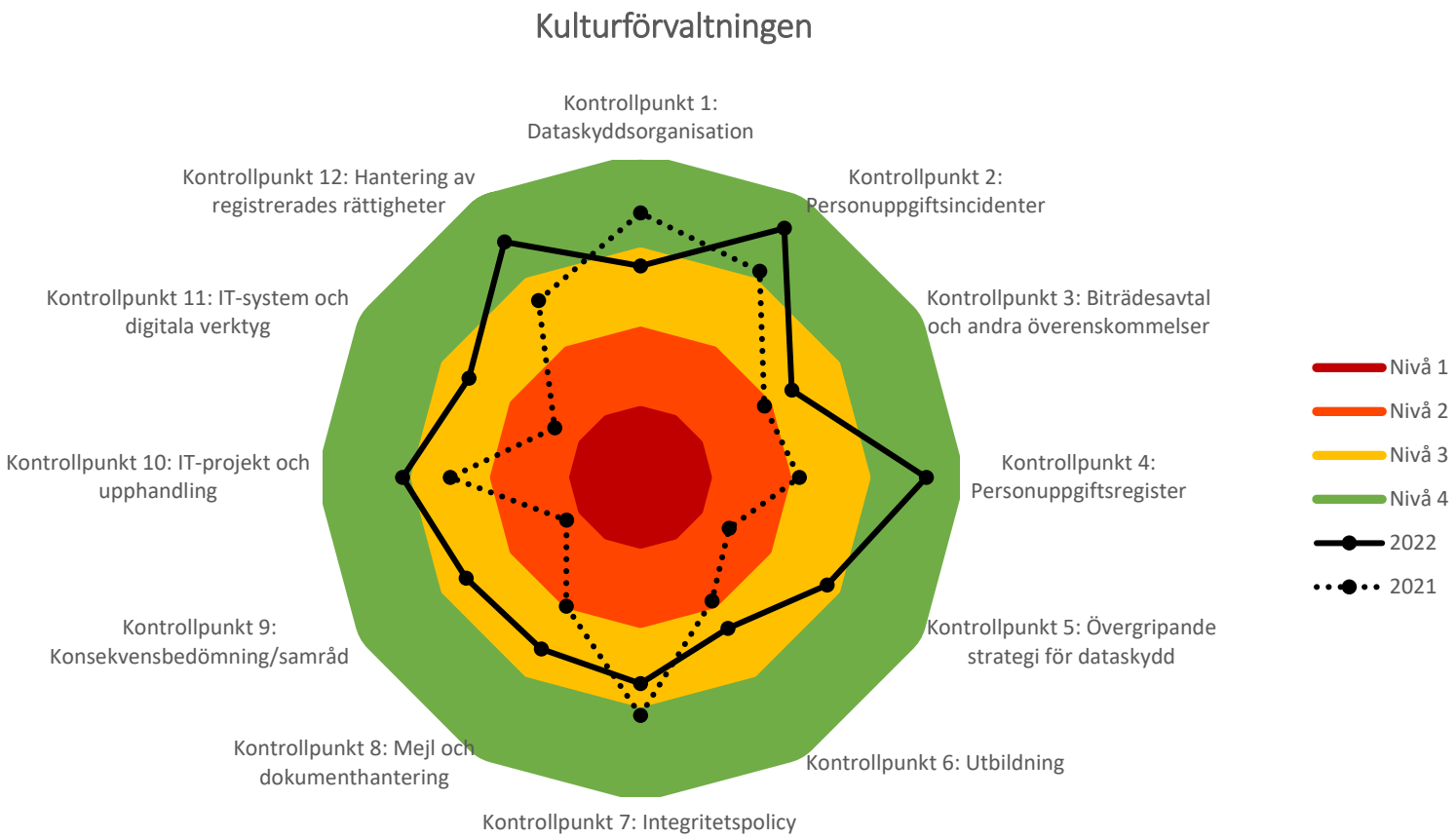
- Kontrollpunkt 11: IT-system och digitala verktyg
  Säkerställ att införandet och användandet av kostnadsfria tjänster så som gratis appar och sociala medier sker i överensstämmelse med reglerna i GDPR.

3 Bilagor

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

Bilaga 2: Fördjupad kontroll 2022

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



Fördjupad kontroll 2022

Integritetspolicy (Kulturförvaltningen)

Bakgrund

Dataskyddsförordningen (GDPR)[1] 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. Den ska också 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.

Av artikel 12 i GDPR framkommer hur information som lämnas till den registrerade ska vara utformad, medan artikel 13 i GDPR ställer krav på vilken information som ska lämnas. Ingen av artiklarna reglerar i detalj vilken form eller var informationen ska lämnas till den registrerade. I vägledningen om öppenhet och transparens[2] anser Artikel 29-gruppen att en bästa praxis innebär att en länk till dataskyddsinformationen ges eller att sådan information ges på samma sida som personuppgifterna hämtas från, när personuppgifterna samlas in online. En skiktad dataskyddsinformation bör användas om den personuppgiftsansvarige har en webbplats.

Syftet med kontrollen är att undersöka verksamhetens integritetspolicy samt rutiner för arbetet med policyn. Kontrollen har genomförts i två delar, där den första varit ett generellt frågeutskick där verksamheten ombads skicka in relevant dokumentation och den andra var ett kompletterande frågeutskick.

Det framkom av de svar som kulturförvaltningen lämnade att förvaltningen har ett stort antal webbsidor och kanaler samt att det även finns flera olika integritetspolicys. Den delen av den fördjupade kontrollen som rör extern integritetspolicy begränsas därför till att avse kulturförvaltningens integritetspolicy[3] (nedan kulturförvaltningens integritetspolicy) och bibliotekens avdelningsgemensamma integritetspolicy[4] (nedan bibliotekens integritetspolicy).

[1] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG

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

[3] Så behandlar kulturförvaltningen personuppgifter - Göteborgs Stad (goteborg.se)

[4] Så behandlar biblioteket dina personuppgifter - Göteborgs Stad (goteborg.se)

Iakttagelser från kontrollen

Extern integritetspolicy

Av artikel 5.1 a i GDPR framgår bland annat att personuppgifter ska behandlas på ett öppet sätt i förhållande till den registrerade (principen om öppenhet). Det framgår även av artikeln att uppgifter ska behandlas på ett lagligt och korrekt öppet sätt i förhållande till den registrerade (laglighet och korrekthet). Det följer vidare av artikel 5.2 att den personuppgiftsansvarige ska ansvara för och kunna visa att de principer som räknas upp i 5.1 efterlevs (ansvarsskyldighet).

I artikel 12.1 i GDPR framgår att den personuppgiftsansvarige ska vidta lämpliga åtgärder för att till den registrerade tillhandahålla all information som avses i artiklarna 13 och 14 och all kommunikation enligt artiklarna 15–22 och 34. Det avser behandling i en koncis, klar och tydlig, begriplig och lätt tillgänglig form, med användning av klart och tydligt språk, i synnerhet för information som är särskilt riktad till barn. Informationen ska tillhandahållas skriftligt, eller i någon annan form, inbegripet, när så är lämpligt, i elektronisk form. Om den registrerade begär det får informationen tillhandahållas muntligt, förutsatt att den registrerades identitet bevisats på andra sätt.

Information som måste tillhandahållas den registrerade

Dataskyddsombudet har utgått ifrån Artikel 29-gruppens vägledning om öppenhet och transparens vid granskningen av integritetspolicyn. I bilagan till vägledningen finns en lista över information som måste tillhandahållas den registrerade enligt artiklarna 13 eller 14, som dataskyddsombudet haft som utgångspunkt.

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 till exempel 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

Förvaltningen har valt att i kulturförvaltningens integritetspolicy endast beskriva exempel på behandlingar som kan förekomma och syftet med dessa. Det finns även en övergripande beskrivning av de rättsliga grunder som kan bli tillämpliga inom förvaltningens verksamheter. Utifrån den beskrivning som lämnas är det oklart vilka enskilda behandlingar som hanteras och vilka personuppgifter som ingår i dessa. Det går inte heller att utläsa ändamålet med respektive behandling och rättslig grund. I bibliotekens integritetspolicy ges en något tydligare beskrivningar av de behandlingar som sker, vilka personuppgifter som samlas in och ändamålen med behandlingarna. Däremot saknas det information om rättslig grund för behandlingarna. Mot bakgrund av dessa brister anser dataskyddsombudet att kulturförvaltningen inte uppfyller sin informationsplikt i någon av de två integritetspolicyerna som granskas, om det inte är så att kompletterande information lämnas till de registrerade på annat sätt. Dataskyddsombudet har dock inte fått del av några uppgifter om att så skulle vara fallet.

Dataskyddsombudet rekommenderar kulturförvaltningen att förbättra strukturen i integritetspolicyerna så att det blir tydligt vilka enskilda behandlingar som hanteras och

vilka personuppgifter som hanteras i respektive behandling. Det behöver även framgå ändamål och rättslig grund för respektive behandling. Informationen behöver även förtydligas avseende vilka externa mottagare, exempelvis personuppgiftsbiträden, som kan komma att ta del av personuppgifterna.

För att förvaltningen skulle kunna uppfylla informationsplikten krävs det att korrekt information gällande en specifik behandling lämnas till den registrerade vid varje insamlingstillfälle inför en ny behandling. Förvaltningen behöver därför alltid säkerställa att en registrerad får tillräcklig information hur dennes personuppgifter behandlas och vilket rättsligt stöd som finns för behandlingen.

Lagring

Det framgår av både kulturförvaltningens och bibliotekens integritetspolicys att personuppgifter inte sparas längre än vad som är nödvändigt för syftet med behandling. Någon precis angiven lagringstid per behandling har alltså inte angetts. Artikel 29-gruppen yttrar i sin vägledning att det inte räcker att den personuppgiftsansvarige generellt anger att personuppgifterna bevaras så länge som är nödvändigt för de berättigade ändamålen, utan att olika lagringstider bör anges för olika kategorier av personuppgifter och/eller olika behandlingsändamål. Dataskyddsombudet anser därför att förvaltningen inte fullgjort informationsplikten på punkten om lagringstid.

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. Kulturförvaltningens och bibliotekens integritetspolicys anger enbart vilka rättigheter den registrerade har och att förvaltningen ska kontaktas när en registrerad vill åberopa en rättighet. Rättigheterna är inte beskrivna eller specificerade för respektive behandling. Dataskyddsombudet rekommenderar att detta åtgärdas.

Överföring till tredjeland

Angående överföring till tredjeland saknas det både i kulturförvaltningens och i bibliotekens integritetspolicys information om personuppgiftsbehandlingar som innebär en tredjelandsöverföring. Dataskyddsombudet anser att detta måste framgå, annars vet den registrerade inte när dennes personuppgifter riskerar att överföras till tredjeland. Dataskyddsombudet saknar också information om relevant artikel i dataskyddsförordningen som förvaltningen stödjer sin behandling på och tillämplig överföringsmekanism. Det framkommer heller inte hur och var den registrerade kan få tillgång till eller erhålla den handling där all information framkommer. I vägledningen står det att information om tredjelandsöverföring ska vara så meningsfull som möjligt för den registrerade, vilket generellt sett innebär att tredjeländernas namn ska anges. Förvaltningen har inte fullgjort detta.

Övrigt

Av kulturförvaltningens integritetspolicy framgår att en behandling i vissa fall baseras på samtycke men det saknas dock uppgifter om hur ett samtycke kan återkallas. Dataskyddsombudet rekommenderar förvaltningen att uppdatera policyn med denna

information. Rekommendationen gäller även för bibliotekens integritetspolicy, om samtycke i något fall används inom bibliotekens verksamhet.

Dataskyddsombudet rekommenderar även förvaltningen att se till så att kontaktuppgifterna är uppdaterade, samt att det finns information som möjliggör olika typer av kommunikation med förvaltningen.

Dataskyddsombudet har förståelse för att en heltäckande integritetspolicy för en förvaltning med många olika behandlingar kommer att innehålla mycket information, vilket kan medföra en informationsutmattning för den registrerade. I det fall det finns 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 det ska vara godtagbart är dock att all information som ska lämnas enligt artikel 13–14 i GDPR ges till de registrerade på annat vis. Dataskyddsombudet rekommenderar förvaltningen att ta ett helhetsgrepp i frågan om integritetspolicyn och utreda hur denna fråga ska hanteras i alla olika verksamhetsdelar och kanaler. Förvaltningen måste säkerställa att oavsett på vilken webbsida eller kanal som den registrerade besöker så ska informationskravet vara uppfyllt. Idag har förvaltningen flera olika integritetspolicyer med olika utformningar och textinnehåll. På några av förvaltningens sidor hänvisas till Göteborgs Stads integritetspolicy i stället för till förvaltningsspecifik information. Vid en översyn av förvaltningens integritetspolicyer rekommenderas förvaltningen också utreda om de kan ta fram en gemensam struktur/mall för en policy att använda inom hela förvaltningen där information exempelvis kan ges i en skiktad integritetspolicy.[5]

Lättillgänglig

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.

Både kulturförvaltningens och bibliotekens integritetspolicys finns tillgängliga via Göteborg Stads hemsida. För att komma till kulturförvaltningens policy behövs ett klick från förvaltningens egen sida, men flera klick om man kommer via stadens hemsida. För att komma till bibliotekens policy krävs flera klick både om man kommer via stadens och förvaltningens hemsida. Enligt vägledningen bör det på varje sida av en webbplats finnas en klart synlig direktlänk till integritetspolicyn. Förvaltningen behöver i arbetet med att se över och tillgängliggöra integritetspolicyn på samtliga kanaler säkerställa att det även är lätt för registrerade att få åtkomst till informationen. Dataskyddsombudet rekommenderar även förvaltningen att se till att varje medarbetare länkar till integritetspolicyn i sin e-postsignatur eftersom det är av vikt att den registrerade får information om personuppgiftsbehandlingen vid första kontakt med förvaltningen.

Språket

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 så att den inte kan tolkas på olika sätt. Framför

[5] Se Artikel 29-gruppens riktlinjer om öppenhet s. 19 ff.

allt bör ändamålet och den rättsliga grunden 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.

De granskade integritetspolicyerna har ett ganska klart och tydligt språk. I samband med en översyn av policyerna bör dock även språket granskas. Bestämningsord används på några ställen i texten samt att vissa meningar är relativt långa vilket kan försvåra de registrerades förståelse av informationen.

Översyn av integritetspolicy

Kulturförvaltningen saknar en rutin för att se över att integritetspolicyerna hålls uppdaterade. Det finns dock en redaktionell påminnelse om att uppdatera externa publika webbsidor. För detta ansvarar redaktör/faktaansvarig. Dataskyddsombudet rekommenderar förvaltningen att ta fram en rutin för att säkerställa att integritetspolicyerna ses över regelbundet och att informationen i dem hålls aktuell i takt med ändring av lagstiftning och riktlinjer, förvaltningens uppdrag eller ändring i personuppgiftsbehandlingar. Dataskyddsombudet rekommenderar dessutom förvaltningen att stämma av behandlingarna med personuppgiftsregistret eftersom det är där alla förvaltningens behandlingar ska finnas registrerade.

Intern integritetspolicy

En intern integritetspolicy kan användas för de särskilda behandlingar som avser anställda i verksamheten, eftersom de ofta skiljer sig ifrån de behandlingar som sker av till exempel kunders eller medborgares personuppgifter.

Kulturförvaltningen uppger att alla medarbetare vid nyanställning får kort information om vad som gäller enligt dataskyddsförordningen. Vid anlitandet av konsulter skrivs personuppgiftsbiträdesavtal med leverantören. Förvaltningen saknar alltså en särskild integritetspolicy som riktar sig till anställda och har i dagsläget inte heller något sätt att säkerställa att man uppfyller informationsplikten gentemot de anställda. Dataskyddsombudet rekommenderar därför förvaltningen att ta fram verksamhetsspecifik information för anställda i syfte att säkerställa att de får information om de personuppgiftsbehandlingar som omfattar anställdas personuppgifter. Det bör även finnas rutiner för att se till så att en intern integritetspolicyn uppdateras vid behov.

Sammanfattade rekommendationer

- Kulturförvaltningen rekommenderas ta ett helhetsgrepp i frågan om integritetspolicyerna och utreda hur frågan ska hanteras i alla olika verksamhetsdelar och kanaler för att säkerställa att informationskravet är uppfyllt.
- Kulturförvaltningen rekommenderas att förbättra strukturen i integritetspolicyerna så att det blir tydligt vilka enskilda behandlingar som finns och vilka personuppgifter som hanteras i respektive behandling, samt ändamål och rättslig grund. Lagringstiden behöver tydliggöras för respektive behandling och information lämnas om personuppgiftsbehandlingar som innebär en tredjelandsöverföring.

- Kulturförvaltningen rekommenderas säkerställa att det är lätt för registrerade att få åtkomst till informationen i integritetspolicyerna via förvaltningens webbsidor och övriga kanaler.
- Kulturförvaltningen rekommenderas att ta fram en rutin för att säkerställa att integritetspolicyerna ses över regelbundet och att informationen i dem hålls aktuell.
- Kulturförvaltningen rekommenderas att ta fram en intern integritetspolicy för att säkerställa att de anställda får information om de personuppgiftsbehandlingar som omfattar deras personuppgifter.

Bilagor

- Information om fördjupad kontroll 2022
- Fördjupad kontroll 2022, Kontrollpunkt 7: Integritetspolicy (del 1)
- Fördjupad kontroll 2022, Kontrollpunkt 7: Integritetspolicy (del 2)

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 maj/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 10 mars 2022.**

Har ni frågor, kontakta ert huvudansvariga dataskyddsombud.

Fördjupad kontroll 2022

Kontrollpunkt 7: Integritetspolicy (del 2)

Utifrån vad som framkommit av svaren i del 1 har dataskyddsombudet beslutat att i den del av den fördjupade kontrollen som rör extern integritetspolicy fokusera granskningen huvudsakligen på kulturförvaltningens integritetspolicy och på bibliotekens avdelningsgemensamma integritetspolicy.

Förvaltningen ombeds nu besvara frågorna nedan dels avseende kulturförvaltningens externa integritetspolicy och bibliotekens avdelningsgemensamma integritetspolicy, dels avseende kulturförvaltningens interna integritetspolicy.

1. Omfattar de integritetspolicys som har skickats in samtliga personuppgiftsbehandlingar som personuppgiftsansvarig utför och är skyldiga att informera om?
2. Om de integritetspolicys som skickats in inte är heltäckande, får de registrerade information om behandlingen/behandlingarna på annat sätt?
    a. Om ja, beskriv hur och ange den information som ges.
    b. Om nej, ange förklaring till varför information inte ges.

Svar ska ha inkommit till dataskyddsombudet **senast den 8 juni 2022.** Dataskyddsombudet kan komma att ställa kompletterande frågor i samband med sammanställande av rapporten.

Har ni frågor, kontakta ert huvudansvariga dataskyddsombud.