Göteborgs Stad

Årsrapport för dataskyddsarbetet 2022

Arkivnämnden

2022-12-23

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 samtycke 2022

Under 2022 har dataskyddsombudet genomfört en fördjupad kontroll på temat samtycke som rättslig grund. Syfte har varit att undersöka i vilken utsträckning verksamheten använder samtycke som rättslig grund för personuppgiftsbehandlingar, samt att bedöma om verksamhetens arbetssätt vid inhämtande, och hantering av, samtycke kan anses uppfylla kraven enligt GDPR. Kontrollen har genomförts genom att verksamheten har fått svara på ett antal frågor och har fått bifoga underlag. I vissa fall har även uppföljande/kompletterande frågor och avstämningar varit nödvändiga.

Dataskyddsombudet har lämnat följande rekommendationer till förvaltningen:

- Förvaltningen rekommenderas genomföra en konsekvensbedömning för behandling av personuppgifter i sociala medier, och avråds från att fortsätta behandla personuppgifter i sociala medier i det fall denna visar att följsamhet mot GDPR inte kan säkerställas.
- Förvaltningen rekommenderas att utreda och bedöma lämpligheten i att använda samtycke som rättslig grund vid behandling i sociala medier mot bakgrund av bland annat profilering, bristande transparens etc.
- Förvaltningen rekommenderas ta fram en rutin eller instruktion som anställda kan använda som stöd i bedömningen av när och hur samtycke kan eller inte kan användas.

Den fördjupade kontrollen kan läsas i sin helhet i Bilaga 2.

2.2.2 Uppföljning av tidigare genomförda kontroller

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

Kontroll (2021): Organisatoriska förutsättningar för dataskyddsarbetet

Verksamheten gavs följande rekommendationer:

- utvärdera den interna dataskyddsorganisationen för att säkerställa att den är ändamålsenlig och fungerar som tänkt även i praktiken.
- utred vilka resurser och vilken kompetens man behöver inom verksamheten för att säkerställa dataskyddsperspektivet.

Kommentarer och rekommendationer:

Uppföljningen visar att verksamheten har vidtagit vissa åtgärder gällande de organisatoriska förutsättningarna för dataskyddsarbetet. Fortsatt uppföljning från dataskyddsombudets sida kommer ske inom ramen för de fasta kontrollpunkterna om ingen särskilt föranleder att det behöver följas upp separat. Dataskyddsombudets rekommendationer i frågan framgår ur Kontrollpunkt 1: Dataskyddsorganisationen (se längre ner vid 2.4.1).

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

2.4 Arkivnämndens 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

			X

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:

Enligt förvaltningens egen skattning av sin dataskyddsorganisation har den förbättrats märkbart jämfört med förra årets enkät.

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

I årsrapporten för 2021 skrev dataskyddsombudet att det skulle ske en särskild uppföljning av förvaltningens dataskyddsorganisation. Förvaltningen har därefter informerat dataskyddsombudet om att det skett en omorganisation av dataskyddsorganisationen. Upplägget för den nya organisationen framgår ur det styrande dokumentet *Regionarkivets anvisning för roller och ansvar inom säkerhet och dataskydd* som beslutades i december 2021 (Diarienr. AN-07544/21). I dokumentet beskrivs bland annat dataskyddskontaktens roll, men även uppdelning av ansvar genom begreppet ”informationsägare” och ”redogörare för informationssäkerhet och dataskydd”

Dataskyddsombudet ser det som positivt att förvaltningen har tagit ett helhetsgrepp kring frågan om säkerhet och dataskydd och att man klargjort roller och ansvarsområden.

Eftersom det genomförts en omorganisation under året kvarstår dataskyddsombudets rekommendation att framåt utvärdera den interna dataskyddsorganisationen för att säkerställa att den är ändamålsenlig och fungerar som tänkt även i praktiken.

2.4.2 Kontrollpunkt 2: Personuppgiftsincidenter

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

Dataskyddsombudets kommentarer:

Enligt förvaltningens egen skattning av arbetet med personuppgiftsincidenter har det förbättrats jämfört med förra årets enkät.

Utifrån förvaltningens lämnade svar och utifrån den fördjupade kontroll som genomfördes 2021 på temat personuppgiftsincidenter, är dataskyddsombudets bedömning att rekommendationen från 2021 fortfarande är aktuell. Förvaltningen behöver regelbundet följa upp och utvärdera rutinen för hantering av personuppgiftsincidenter, samt att se över och analysera tidigare inträffade incidenter för att kunna arbeta förebyggande.

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:

Enligt förvaltningens egen skattning av arbetet med biträdesavtal och andra överenskommelser har det förbättrats jämfört med förra årets enkät. Resultatet indikerar dock att det fortfarande finns risker, men dessa risker bedöms inte vara brådskande, omfattande eller allvarliga.

Eftersom förvaltningen har skattat sig lågt vad gäller rutiner för kontinuerlig kontroll av efterlevnad hos personuppgiftsbiträden och vad gäller rutiner kring uppföljning av underbiträden, rekommenderas förvaltningen att prioritera arbetet med dessa frågor.

Vidare indikerar svaren att förvaltningen behöver arbeta med frågan kring delat och gemensamt personuppgiftsansvar och ta fram rutiner för detta.

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:

Enligt förvaltningens egen skattning av arbetet med personuppgiftsregister har man gjort framsteg sedan förra årets enkät.

Förvaltningen har bifogat ett utkast på registerförteckning och har förklarat att man parallellt med arbetet att göra registerförteckningen komplett genomför en inventering av informationstillgångar i enlighet med Göteborgs Stads riktlinje för informationssäkerhet. Man har för avsikt att stämma av inventeringen av informationstillgångar mot registerförteckningen för att komplettera med information som också har relevans för registerförteckningen. Förvaltningen har uppgett att man är i dialog med Intraservice vad gäller frågan om tredjelandsöverföringar.

Dataskyddsombudet ser det som positivt att förvaltningen har kommit en bra bit på vägen med registerförteckningen och att man har en plan för arbetet framåt. Dataskyddsombudet uppmuntrar förvaltningen att fortsätta arbetet med att göra personuppgiftsregistret mer komplett i enlighet med artikel 30 i GDPR.

2.4.5 Kontrollpunkt 5: Övergripande strategi för dataskydd

Kontrollpunkten avser verksamhetens övergripande strategi för att arbeta med dataskydd.

Dataskyddsombudets kommentarer:

Enligt förvaltningens egen skattning av den övergripande strategin för dataskydd, har den förbättrats något jämfört med förra årets enkät. Resultatet indikerar dock att det fortfarande finns risker som bedöms vara omfattande och/eller som omgående kräver åtgärder.

Som tidigare nämnts under Kontrollpunkt 1: Dataskyddsorganisation (se vid 2.4.1), ser dataskyddsombudet det som positivt att förvaltningen har tagit ett helhetsgrepp kring frågan om säkerhet och dataskydd och klargjort roller och ansvarsområden. Detta är ju också något som hänger samman med den övergripande strategin för arbetet med dataskydd.

Utifrån förvaltningens lämnade svar rekommenderar dataskyddsombudet att förvaltningen framöver prioriterar arbetet med att identifiera och värdera informationstillgångar.

Förvaltningen behöver även se över rutinerna för efterlevnad av GDPR i samband med fysiska och digitala sammankomster.

2.4.6 Kontrollpunkt 6: Utbildning

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

Dataskyddsombudets kommentarer:

Enligt förvaltningens skattning av arbetet med utbildning kring dataskyddsfrågor har det förbättrats märkbart jämfört med förra årets enkät. Resultatet indikerar dock att det fortfarande finns risker, men dessa risker bedöms inte vara brådskande, omfattande eller allvarliga.

Utifrån förvaltningens lämnade svar rekommenderar dataskyddsombudet att förvaltningen kartlägger och följer upp kunskapsnivån inom förvaltningen.

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:

Enligt förvaltningens skattning av sin integritetspolicy ligger den kvar på ungefär samma nivå som vid förra årets enkät (en marginell höjning i år jämfört med förra

året). Integritetspolicyn är en del av det kontinuerliga dataskyddsarbetet. Dataskyddsombudet har tittat översiktligt på den information som ges på den externa hemsidan med rubriken *Så behandlar regionarkivet personuppgifter – Göteborgs stad* och jämfört med kraven enligt artikel 13 och 14 i GDPR.[4]

Förvaltningen behöver kontinuerligt säkerställa att integritetspolicyn hålls aktuell i de olika kanalerna som förvaltningen använder sig av och att rutinerna kopplat till integritetspolicyn följs. Förvaltningen rekommenderas att se över integritetspolicyn både utifrån innehåll, utifrån hur innehållet presenteras och utifrån vilken specifik information som ges i samband med olika behandlingar.

Med tanke på förvaltningens användning av sociala medier så blir frågan om tredjelandsöverföringar aktuell (se mer i den fördjupade kontrollen i Bilaga 2). En konkret utvecklingspunkt vad gäller integritetspolicyn är därför information om just tredjelandsöverföringar (se kraven enligt artikel 13.1.f och artikel 14.1.f i GDPR). Frågan om användning av sociala medier bör även i grunden ses över. I Schrems II-domen (juli 2020) förtydligade EU-domstolen vad som gäller för överföringar av personuppgifter till länder utanför EU/EES, så kallade tredjelandsöverföringar. Domen sade, i breda drag, att det skydd för personuppgifter som finns i USA inte är likvärdigt med det som finns i EU/EES varför den personuppgiftsansvarige antingen måste vidta extra skyddsåtgärder eller avbryta behandlingen. I Schrems II-domen prövades särskilt Facebook, men även Instagram och Youtube är exempel på sociala medier som överför personuppgifter till USA. Ingen av dessa plattformar har angett att de vidtagit några extra skyddsåtgärder och utifrån det saknar alla överföringar som görs inom dessa tjänster laglig grund. Dataskyddsenheten avråder därför förvaltningen från att fortsätta behandla personuppgifter i sociala medier i de fall följsamhet mot GDPR inte kan säkerställas.

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 GDPR. Även verksamhetens rutin för att säkerställa att gallringsrutiner för personuppgifter följs innefattas.

Dataskyddsombudets kommentarer:

Enligt förvaltningens skattning av sin e-post och dokumenthantering ligger man kvar på samma nivå som vid förra årets enkät. Resultatet indikerar att det fortfarande finns risker som bedöms vara omfattande och/eller som omgående kräver åtgärder.

[4] Göteborgs stad. Så behandlar regionarkivet personuppgifter – Göteborgs stad. Tillgänglig: Så behandlar regionarkivet personuppgifter - Göteborgs Stad (goteborg.se). (Hämtad 2022-12-01).

Av svaren framgår det att det inte genomförts någon informationsklassificering av förvaltningens personuppgiftsbehandlingar. Detta innebär en risk för att information hanteras felaktigt och saknar rätt skyddsåtgärder. Dataskyddsombudet rekommenderar därför förvaltningen att prioritera arbetet med att informationsklassa personuppgiftsbehandlingar, samt ta fram anvisningar för hur information i olika informationsklasser ska hanteras och vilka lagringsytor som får användas. Vidare rekommenderar dataskyddsombudet att förvaltningen ser över rutinerna kring gallring.

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:

Enligt förvaltningens skattning av sitt arbete med konsekvensbedömningar/samråd ligger man kvar på ungefär samma nivå som vid förra årets enkät (en marginell nivåhöjning). Resultatet indikerar att det fortfarande finns risker som bedöms vara omfattande och/eller som omgående kräver åtgärder.

Skattningen visar att förvaltningen behöver fortsätta arbetet med att få koll på behandlingar som innebär hög risk för de registrerades fri- och rättigheter. Dataskyddsombudet rekommenderar därför förvaltningen att fortsätta genomföra tröskelanalyser och identifiera behandlingar som behöver konsekvensbedömas. Därefter bör förvaltningen ta fram en handlingsplan för att på sikt säkerställa att konsekvensbedömningar faktiskt 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:

Enligt förvaltningens skattning av sitt dataskyddsarbete i IT-projekt och upphandlingar så har det förbättrats märkbart jämfört med förra årets enkät. Resultatet indikerar dock att det fortfarande finns risker, men dessa risker bedöms inte vara brådskande, omfattande eller allvarliga.

Utifrån förvaltningens lämnade svar rekommenderar dataskyddsombudet att förvaltningen ser över rutinerna kring upphandling, avrop och förnyad konkurrensutsättning, samt utveckling av befintliga verksamhetsstöd. Detta med målsättningen att säkerställa att dataskyddsperspektivet omhändertas.

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

Dataskyddsombudets kommentarer:

Enligt förvaltningens skattning av sitt dataskyddsarbete i IT-system och digitala verktyg ligger det kvar på samma nivå som förra årets enkät. Resultatet indikerar att det finns risker, men dessa risker bedöms inte vara brådskande, omfattande eller allvarliga.

Med utgångspunkt i förvaltningens lämnade svar rekommenderar dataskyddsombudet att förvaltningen prioriterar arbetet med att kartlägga de IT-system och/eller tjänster som används inom förvaltningen och vad det är för personuppgifter som behandlas i dessa.

Förvaltningen behöver också se till att dataskyddsperspektivet finns med när förvaltningen inför och använder kostnadsfria tjänster t.ex. gratisappar och sociala medier. Dataskyddsombudet påminner därför om rekommendationen kring sociala medier som har getts vid punkten 2.4.7 (Kontrollpunkt 7: Integritetspolicy).

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:

Enligt förvaltningens skattning av hanteringen av de registrerades rättigheter har arbetet förbättrats något jämfört med förra årets enkät. Resultatet indikerar dock att det finns vissa risker, men dessa risker bedöms inte vara brådskande, omfattande eller allvarliga.

Enkätsvaren visar bland annat att medarbetarnas kunskaper om de registrerades rättigheter har förbättrats sedan 2021, vilket är positivt. Förvaltningen har muntligen uppgett att man har en rutin och mall för begäran om registerutdrag. Dataskyddsombudet uppmuntrar förvaltningen att fortsätta arbetet med att hantera de registrerades rättigheter och att hålla och nya och gamla medarbetares kunskaper uppdaterade.

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 3 (Biträdesavtal och andra överenskommelser).
  Uppföljning och kontroll av personuppgiftsbiträden och underbiträden.

- Kontrollpunkt 5 och 11 (Övergripande strategi för dataskydd och IT-system och digitala verktyg).
  Identifiera och värdera informationstillgångar.

- Kontrollpunkt 8: E-post och dokumenthantering
  Informationsklassa och ta fram anvisningar för hur information i olika informationsklasser ska hanteras och vilka lagringsytor som får användas.

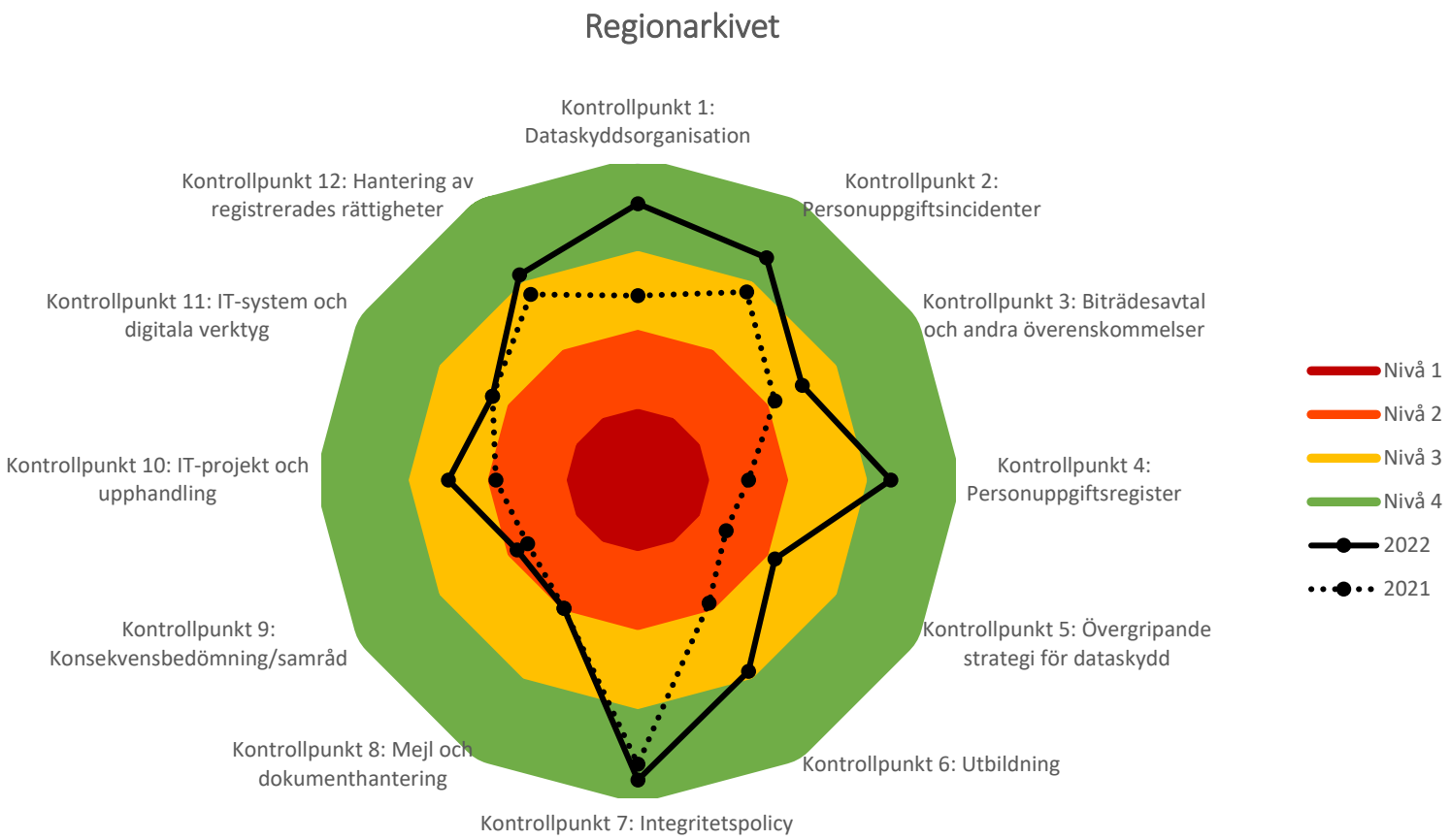
- Kontrollpunkt 9: Konsekvensbedömningar
  Genomför konsekvensbedömningar. Ta fram handlingsplan, prioritera och beta av skuld utifrån den.

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

Kontrollpunkt 12: Samtycke som rättslig grund för verksamhetens personuppgiftsbehandlingar, Arkivnämnden/Regionarkivet.

Bakgrund

Av GDPR och Europeiska dataskyddsstyrelsens (EDPB) riktlinje om samtycke[1] framgår att personuppgiftsansvariga som lutar sig mot samtycke som rättslig grund behöver säkerställa att flera kriterier är uppfyllda för att samtycket ska vara giltigt. Samtycket behöver vara en ”otvetydig viljeyttring” från den registrerade och ska vara frivilligt, specifikt och informerat (dvs. ska ha lämnats efter det att den registrerade har fått information om behandlingen). Det behöver också vara insamlat före det att behandlingen påbörjas. Samtycket måste inte, men bör vara, skriftligt eftersom den personuppgiftsansvarige har bevisbördan för att samtycket har lämnats. Samtycke anses inte vara frivilligt om det finns en ojämn maktbalans mellan den registrerade och den personuppgiftsansvarige, vilket ofta är fallet mellan myndigheter och registrerade. Det kan även finnas en ojämn maktbalans mellan t.ex. arbetsgivare och arbetstagare som påverkar möjligheten för ett frivilligt lämnat samtycke. Om den registrerade får utstå negativa konsekvenser om hen inte samtycker anses inte heller samtycket vara frivilligt. Vad gäller valet av rättslig grund bör samtycke inte var ett förstahandsval, utan man bör i förstahand överväga en annan rättslig grund.

Den registrerade har rätt att när som helst återkalla sitt samtycke. Den personuppgiftsansvarige måste säkerställa att det är lika lätt att återkalla samtycket som det är att lämna det. När samtycket är återkallat ska den personuppgiftsuppgiftsansvarige stoppa behandlingen som den registrerade tidigare har samtyckt till.

Den fördjupade kontrollen avseende samtycke har haft till syfte att undersöka i vilken utsträckning som verksamheten använder samtycke som rättslig grund för personuppgiftsbehandlingar, samt att bedöma om verksamhetens arbetssätt vid inhämtande, och hantering av, samtycke kan anses uppfylla dataskyddsförordningens (GDPR) krav. Kontrollen har genomförts genom att verksamheten har fått svara på ett antal frågor och har fått bifoga underlag. I vissa fall har även uppföljande/kompletterande frågor och avstämningar varit nödvändiga.

Iakttagelser från kontrollen

Regionarkivet har angett att samtycke som rättslig grund används för behandlingen ”Kommunikation, information och dialog”. Ändamålet är att informera om förvaltningens verksamhet genom publicering av film, foto och ljud i myndighetens kanaler. Som underlag för behandlingen har regionarkivet bilagt en samtyckesblankett och ett utdrag ur förvaltningens dokumenthanteringsplan.

[1] Riktlinje 05/2020 om samtycke enligt förordningen (EU) 2016/679, version 1.1, antagna den 4 maj 2020
.

Att använda samtycke som rättslig grund

Dataskyddsombudet ser att det för regionarkivets del i många fall är direkt olämpligt att använda sig av samtycke som rättslig grund för en behandling av bilder eller film på anställda. Detta med hänvisning till den ojämna maktbalans som råder mellan arbetsgivare och arbetstagare. På grund av detta kommer regionarkivet i många fall i stället vara hänvisade till att använda ”uppgift av allmän intresse” som rättslig grund. Men, för att denna rättsliga grund ska kunna användas behöver regionarkivet visa att behandlingen är *nödvändig* för att utföra en uppgift av allmänt intresse. I det fall en behandling kan stödjas på grunden uppgift av allmänt intresse rekommenderar dataskyddsombudet ändå att det säkerställs att ett eventuellt deltagande är frivilligt, samt att förvaltningen lämnar integritetshöjande information till de registrerade om behandlingen.

Om förvaltningen bedömer att man inte kan använda den rättsliga grunden allmänt intresse, utan är hänvisade till samtycke bedömer dataskyddsombudet att ett antal åtgärder behöver vidtas. I de underlag som lämnats till dataskyddsombudet inom ramen för kontrollen har dataskyddsombudet inte kunnat utläsa att regionarkivet har rutiner för att säkerställa kravet på frivillighet vid inhämtande av samtycke. Mot bakgrund av detta ser dataskyddsombudet att regionarkivet behöver ta fram och dokumentera en hantering som visar att man säkerställer frivillighet. Dataskyddsombudet rekommenderar därför att förvaltningen tar fram en rutin eller instruktion som förvaltningen kan använda internt som stöd i bedömningen av när samtycke kan eller inte kan användas. Detta blir också ett led i att visa ansvarsskyldighet enligt artikel 5.2 i GDPR.

Exempel på hantering

Dataskyddsenheten har sedan tidigare lämnat rekommendationer för hur den aktuella frågan kan hanteras i praktiken. Exemplet som då har getts har utgått från scenariot att en förvaltning vill informera om sin verksamhet (internt) och ha en bild på en anställd i anslutning till denna information. Om förvaltningen gör bedömningen att det inte handlar om en nödvändig behandling och allmänt intresse därför inte kan användas som rättslig grund, kan det vara så att man behöver gå vidare och inhämta ett samtycke för att kunna genomföra behandlingen. En möjlig hantering, enligt dataskyddsenheten, är då att förvaltningen skickar ut en förfrågan till en bred grupp (eller hela förvaltningen) om att frivilliga kan anmäla sig. I utskicket är det då viktigt att det finns tydlig och konkret information om publiceringen så att den anställde vet vad hen går med på. Genom denna hantering skulle kravet på frivillighet kunna anses vara uppfyllt och ett efterföljande samtycke skulle då kunna bedömas giltigt.[2]

Samtycke för publicering av personuppgifter i sociala medier

I samtyckesblanketten har förvaltningen angett att den registrerade har möjlighet att samtycka till publicering av personuppgifter i sociala medier. Dataskyddsombudet vill här lyfta att denna hantering strider mot de rekommendationer som dataskyddsombudet har lämnat gällande användningen av sociala medier som ägs av amerikanska moderbolag.

I Schrems II-domen (juli 2020) förtydligade EU-domstolen vad som gäller för överföringar av personuppgifter till länder utanför EU/EES, så kallade tredjelandsöverföringar. Domen

[2] I sammanhanget vill dataskyddsombudet dock särskilt påpeka att ett samtycke för sociala medier inte bedöms kunna uppfylla kraven enligt GDPR oavsett hur det inhämtas.

sade, i breda drag, att det skydd för personuppgifter som finns i USA inte är likvärdigt med det som finns i EU/EES varför den personuppgiftsansvarige antingen måste vidta extra skyddsåtgärder eller avbryta behandlingen. I Schrems II-domen prövades särskilt Facebook, men även Instagram och Youtube är exempel på sociala medier som överför personuppgifter till USA. Ingen av dessa plattformar har angett att de vidtagit några extra skyddsåtgärder och utifrån det saknar alla överföringar som görs inom dessa tjänster rättslig grund.

Dataskyddsombudet bedömer att regionarkivet i dagsläget inte kan använda samtycke som rättslig grund för en behandling av personuppgifter i sociala medier. Inte heller bedöms tredjelandsöverföringen kunna stödjas på ett samtycke enligt artikel 49 GDPR då behandlingen – utifrån förvaltningens beskrivning – inte handlar om ett undantag utan en del av förvaltningens kommunikationsstrategi. Dataskyddsenheten avråder regionarkivet från att fortsätta behandla personuppgifter i sociala medier där följsamhet mot GDPR inte kan säkerställas.

När det gäller just användningen av sociala medier, oaktat tredjelandsproblematiken, är dataskyddsombudets uppfattning att förvaltningen har ytterst begränsade möjligheter att tillhandahålla tillräcklig information om hur personuppgifterna behandlas inom plattformen, vilket också påverkar möjligheten att använda samtycke som rättslig grund för behandlingen. Då regionarkivet inte bedöms kunna tillhandahålla tillräcklig information om behandlingen till de registrerade, rekommenderas förvaltningen att, genom en konsekvensbedömning, utreda och bedöma möjligheten att använda sociala medier mot bakgrund av bland annat bristande transparens, profilering etc.

Dokumentation

Dataskyddsombudet ser det som positivt att förvaltningen har en samtyckesblankett genom vilken samtycket dokumenteras, men bedömer att innehållet i denna behöver ses över så att samtycket uppfyller kraven enligt GDPR. Vidare ser dataskyddsombudet det som positivt att det finns ett avsnitt i dokumenthanteringsplanen som specifikt berör frågan om hur dokumenterat samtycke m.m. ska hanteras.

Förvaltningen har uppgett att om en registrerad vill utöva sin rättighet att återta samtycket, kommer begäran om återtagande att lagras i två år innan den gallras. Från regionarkivets sida har man motiverat detta med att det kan uppstå tvister om den rättsliga grunden för behandlingen och att samtyckesblanketten därför kan fungera som bevisföremål. Denna lagring förefaller rimlig vad gäller själva samtyckesblanketten och själva dokumentationen av återtagandet av samtycket. Det måste dock vara tydligt att den behandling som framgår ur samtyckesblanketten för de ändamål som nämns där, måste upphöra så fort samtycket har återkallats, även om själva samtyckesblanketten bevaras under en längre tid. Dataskyddsombudet rekommenderar regionarkivet att förtydliga detta i framtida rutinbeskrivningar av hur behandlingen ska gå till.

Sammanfattade rekommendationer

- Förvaltningen rekommenderas genomföra en konsekvensbedömning för behandling av personuppgifter i sociala medier, och avråds från att fortsätta behandla personuppgifter i sociala medier i det fall denna visar att följsamhet mot GDPR inte kan säkerställas.
- Förvaltningen rekommenderas att utreda och bedöma lämpligheten i att använda samtycke som rättslig grund vid behandling i sociala medier mot bakgrund av bland annat profilering, bristande transparens etc.
- Förvaltningen rekommenderas ta fram en rutin eller instruktion som anställda kan använda som stöd i bedömningen av när och hur samtycke kan eller inte kan användas.

Bilagor

Utskickad information samt frågeställningar (Del 1 och Del 2).

Information om fördjupad kontroll 2022

Kontrollpunkt 12: Samtycke som rättslig grund för verksamhetens personuppgiftbehandlingar

Den rättsliga grunden samtycke ger registrerade möjlighet att frivilligt välja när och hur deras personuppgifter behandlas. När en verksamhet använder den rättsliga grunden samtycke innebär det att den registrerade har sagt ja till personuppgiftsbehandlingen som verksamheten utför. Ett samtycke ska vara frivilligt och jämlikt, vilket innebär att myndigheters möjligheter för att stödja en behandling på samtycke är mycket begränsade. Att samtycke ofta är en olämplig rättslig grund för myndigheter beror alltså på att det som regel råder ett ojämlikt maktförhållande i relationen mellan myndighet och medborgare/arbetstagare/elev/brukare etc. När en verksamhet väljer att använda samtycke som rättslig grund för en behandling ansvarar verksamheten för att samtycket är giltigt och behöver kunna visa både att den registrerade har fått relevant information och att verksamhetens arbetssätt uppfyller kraven.

Granskningen avser undersöka i vilken utsträckning som verksamheten använder samtycke som rättslig grund för personuppgiftsbehandlingar, samt bedöma huruvida verksamhetens arbetssätt vid inhämtande, och hantering av, samtycke kan anses uppfylla dataskyddsförordningens krav.

Tillvägagångssätt

Den fördjupade kontrollen kommer att genomföras i två delar. I del ett ombeds ni att besvara ett antal frågor och tillhandahålla olika former av underlag. I del två kommer uppföljande frågor att ställas och vid behov kan även en kontroll på plats hos verksamheten komma att genomföras.

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

Fördjupad kontroll 2022

Kontrollpunkt 12: Samtycke som rättslig grund för verksamhetens personuppgiftbehandlingar (del 1)

Frågor att besvara:

1. Använder ni samtycke (artikel 6.1 a GDPR) som rättslig grund för personuppgiftsbehandlingar inom er verksamhet?
2. Om ja, ange de behandlingar där samtycke används som rättlig grund och ange ändamål för respektive behandling.
    a. Om samtycke inhämtas med hjälp av samtyckesblankett ska denna/dessa bifogas.
3. Har ni dokumenterade rutiner/instruktioner kopplat till användningen av samtycke? (t.ex. administration av samtycke, rutiner för att bedöma när samtycke kan användas och rutin för tillbakadragande av samtycke)
    a. Om ja, bifoga dessa rutiner/instruktioner.
    b. Om nej, ange varför dessa rutiner/instruktioner saknas.

Observera att frågorna gäller för samtliga delar av myndigheten. Om det inom myndigheten förekommer olika samtyckesblanketter och/eller hanteringen av samtycke skiljer sig mellan verksamheter (t.ex. mellan olika skolor) vill dataskyddsombudet ta del av samtliga exempel på blanketter och rutiner/instruktioner. Detta för att dataskyddsombudet ska få en helhetsbild av myndighetens användning av samtycke som rättslig grund.

Underlaget ska ha inkommit till dataskyddsombudet **senast den 11 mars 2021.**

Har du frågor, kontakta ditt huvudansvariga dataskyddsombud.

Fördjupad kontroll 2022

Kontrollpunkt 12: Samtycke som rättslig grund för verksamhetens personuppgiftbehandlingar (del 2)

Uppföljande frågor att besvara:

1. Används samtycke som rättslig grund för behandling av anställdas personuppgifter?
    a. Om ja, beskriv i vilka typer av behandlingar och skicka in aktuell blankett som används.
2. Har grundskole/utbildningsförvaltningen överblick över användningen av samtyckesblanketter i samtliga skolor som förvaltningen ansvarar för?
    a. Hur har förvaltningen gått till väga för att undersöka hur den faktiska användningen ser ut i respektive skola? (Om t.ex. fråga har skickats ut till skolornas rektorer, har samtliga återkommit med svar?)

Svar ska ha inkommit till dataskyddsombudet **senast den xx maj/juni 2022.**

Har ni frågor, kontakta ert huvudansvariga dataskyddsombud.