Göteborgs Stad

Årsrapport för dataskyddsarbetet 2022

Förskoleförvaltningen

2022-12-21

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 GDPR
[2] Artikel 38.3 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 som rättslig grund för verksamhetens personuppgiftsbehandlingar 2022

Den fördjupade kontrollen har bestått av en kontroll av förvaltningens användning av samtycke som rättslig grund för personuppgiftsbehandlingar. Resultatet av kontrollen presenteras i sin helhet i bilaga 2.

Dataskyddsombudet har i rapporten avseende den fördjupade kontrollen haft vissa anmärkningar och därför lämnat ett antal rekommendationer till verksamheten.

Sammanfattande rekommendationer från kontrollen:

- Utred och dokumentera hur hanteringen av förvaltningens användning av medverkandeavtal följer kraven i dataskyddsförordningen.

- Utred och dokumentera frågan om hur bilder kan användas i publika sammanhang utifrån den sekretess som reglerar verksamheten.
- Utred och komplettera riktlinje för bild och film inom förskoleförvaltningen för vilka olika ändamål som bilder och filmer används i den externa kommunikationen samt säkerställa lämplig rättslig grund utifrån de olika behandlingarna.
- Komplettera riktlinje för bild och film inom förskoleförvaltningen med anvisningar om när och hur medverkandeavtal kan användas inom förvaltningen. Om behandlingar av bild och film fastställs med annan rättslig grund, komplettera med anvisningar för hur följsamhet gentemot GDPR säkerställs för den/dessa behandlingar.
- Fortsätta det arbetet som påbörjats med utbildning för rektorer och fullfölja den påbörjade kartläggningen av användning av samtycken för att få överblick och kontroll att samtycken inte används.

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.

Fördjupad kontroll (2021): Hantering av personuppgiftsincidenter

Verksamheten gavs följande rekommendationer:

- Minska personberoendet genom att tydliggöra och konkretisera rutinen så att fler inom förvaltningen har möjlighet och förutsättningar att hantera incidenter.
- Komplettera rutinen med konkreta beskrivningar/instruktioner (mallstöd) för hur en bedömning av risken för de registrerades fri- och rättigheter ska göras.
- Se över ifall rutinen täcker in de fall då en personuppgiftsincident inträffar hos ett personuppgiftsbiträde.
- Se över hur anställda informeras och hålls uppdaterade i dataskyddsfrågor.

Kommentarer och rekommendationer:

Uppföljning av denna kontroll har skett genom att frågan varit en del av de fasta kontrollpunkterna. Resultat, kommentarer och rekommendationer framgår därför av kontrollpunkt 2.

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 Förskoleförvaltningens 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.

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

Dataskyddsombudets kommentarer:

Dataskyddsombudets förståelse är att det finns god insikt om verksamhetens utmaningar inom förvaltningens dataskyddsorganisation. De risker som identifierats synes härröra från tidsbrist snarare än bristande kompetens. Under året har förvaltningen sett över och byggt upp en dataskyddsorganisation med förvaltningsövergripande representanter, som har bredare förankring inom verksamheten. Förvaltningen har även gjort förändringar i dataskyddskontaktens roll till att vara mer stödjande än operativ i arbetet med till exempel konsekvensbedömningar samt undersöker möjligheten till förstärkta resurser inom dataskyddsorganisationen. Dataskyddsombudet anser detta vara positivt och rekommenderar förvaltningen att fortsätta detta arbete.

Den risk som dataskyddsombudet främst identifierat, vilket även stämmer överens med förvaltningens egen skattning, är att dataskyddsorganisationen inte har tillräckliga resurser. Med hänsyn till förvaltningens storlek, en ökad digitaliseringstakt och att de registrerade till stor del utgör barn krävs både resurser, kunskap och medvetenhet om dataskydd hos personalen för att dataskydd ska kunna vara en integrerad del av det dagliga arbetet. Förvaltningen rekommenderas därför att fortsätta översynen av dataskyddsorganisationen och tillföra de resurser som behövs för att förvaltningen ska ha förutsättningar för att framåt bedriva ett systematiskt dataskyddsarbete. Dataskyddsorganisationen bör framåt fokusera på hur dataskydd kan bli en naturlig och integrerad del i det dagliga arbetet i alla delar av verksamheten.

2.4.2 Kontrollpunkt 2: Personuppgiftsincidenter

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

Dataskyddsombudets kommentarer:

Dataskyddsombudet genomförde förra året en fördjupad kontroll avseende hanteringen av personuppgiftsincidenter inom förvaltningen. I denna kontroll framkom förbättringsområden som dataskyddsombudet gav rekommendationer utifrån. Förvaltningen har uppgett att åtgärder har vidtagits utifrån dataskyddsombudets rekommendationer, bland annat för att minska personberoendet för att omhänderta incidenter.

Utöver dataskyddsombudets kontroll från 2021, framgår av skattningen att förvaltningen fortsatt behöver arbeta med hur och när information till registrerade ska tillhandahållas och vad denna information ska innehålla. Dataskyddsombudet rekommenderar därför förvaltningen att ta fram en rutin för detta eller att komplettera befintlig rutin för personuppgiftsincidenter med informationen. Förvaltningen behöver även säkerställa att inträffade incidenter systematiskt följs upp som en naturlig del i dataskyddsarbetet. En viktig del av att identifiera och

utreda personuppgiftsincidenter är att verksamheten tar lärdom av de bakomliggande orsakerna till incidenten samt använder lärdomarna för att nya incidenter inte ska inträffa igen och kunna utvärdera åtgärdernas effektivitet.

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:

Förvaltningen anger, likt förra året, varierande värden i sin skattning av kontrollpunkten. Förvaltningen svarar att det finns rutiner för att bedöma om det uppstår en biträdesrelation samt vem som är personuppgiftsansvarig (PUA) respektive personuppgiftsbiträde (PUB) vid anlitande av nya leverantörer samt säkerställa att det tecknas personuppgiftsbiträdesavtal innan tjänsten börjar användas. Vidare indikerar svaren att verksamheten kan bedöma hela kedjan av underbiträden samt att det finns tecknade biträdesavtal med ca 75 % av sina personuppgiftsbiträden. Rutiner saknas fortsatt för att kontrollera att anlitade personuppgiftsbiträden uppfyller villkoren enligt biträdesavtalet samt för att bedöma om andra överenskommelser eller avtal ska upprättas vid gemensam hantering av personuppgifter internt och externt inom Staden.

Skattningen visar att det finns rutiner för att teckna personuppgiftsbiträdesavtal med nya biträden, men att det för ca 25% av förvaltningens anlitade biträden alltjämt saknas reglering av personuppgiftshanteringen genom ett personuppgiftsbiträdesavtal. Efter genomgång med förvaltningen angavs att de saknade avtalen främst kan finnas för vissa appar/gratisappar och att korrekt reglering av avtalsförhållanden för kommungemensamma interna tjänster/bastjänster eventuellt saknas, beroende på hur man ska se på ansvarsförhållandet för dessa tjänster, vilket också räknats in i skattningen

Skattningen påvisar även att det fortsatt saknas rutiner och arbetssätt för att följa upp ingångna personuppgiftsbiträdesavtal. Det saknas också rutiner för att andra överenskommelser eller avtal upprättas vid gemensam eller delad personuppgiftshantering. Förskoleförvaltningen riskerar därmed att dels sakna nödvändiga avtal som krävs enligt förordningen, dels att sakna kontroll över hur biträden faktiskt hanterar verksamhetens personuppgifter. För att hantera riskerna rekommenderas förvaltningen att ta fram rutiner och arbetssätt för att kunna följa upp sina biträden. Vidare rekommenderas förvaltningen att kartlägga samtliga behandlingar där biträden används och/eller där förvaltningen har en gemensam

eller delad personuppgiftshantering, för att kunna identifiera när personuppgiftsbiträdesavtal och andra nödvändiga avtal eller överenskommelser saknas, för att kunna upprätta sådana.

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:

Förskoleförvaltningens svar på denna kontrollpunkt indikerar fortsatt omfattande höga risker som kräver omedelbara åtgärder. Skattningen visar att endast ca 25 % av de personuppgiftsbehandlingar som görs inom förvaltningen finns dokumenterade i registret och att dessa till större delen inte innehåller all den information som ska finnas med enligt dataskyddsförordningen. Vidare anges att det inte finns någon ansvarsfördelning för arbetet med registret, att det saknas rutiner för att hålla registret uppdaterat och att registret inte används som en del i det interna dataskyddsarbetet. Dataskyddsombudet har ingen anledning att göra en annan bedömning än den som förvaltningen gjort. Samma risk identifierades i årsrapporten 2021 och förvaltningen rekommenderades då att prioritera arbetet under 2022. Dataskyddsombudet noterar att så ej gjorts, men har inte kännedom om anledningen till detta. Därtill vill dataskyddsombudet särskilt poängtera att avsaknaden av ett komplett personuppgiftsregister innebär att förvaltningen inte uppfyller dess skyldighet att föra register över personuppgiftsbehandlingar enligt artikel 30 GDPR.

Verksamheten rekommenderas att snarast påbörja ett grundläggande och systematiskt arbete med sitt personuppgiftsregister för att säkerställa att de behandlingar som görs i verksamheten återfinns i registret. Detta arbete bör även omfatta att ta fram rutiner för hur registret hålls uppdaterat. Dataskyddsombudet kan inte nog understryka att grunden i ett fullgott dataskyddsarbete utgår från att verksamheten har koll på sina personuppgiftsbehandlingar. Ett komplett personuppgiftsregister är en förutsättning för att ha överblick över de personuppgiftsbehandlingar som görs i verksamheten. Avsaknad av personuppgiftsregister riskerar inte bara att inskränka de registrerades rättigheter utan riskerar även innebära att verksamhetens dataskyddsarbete inte kan bedrivas på ett effektivt sätt.

Förvaltningen har under genomgång med dataskyddsombudet angett att de ska rekrytera kompetens inom informationssäkerhet för att förstärka dataskyddsorganisationen och att arbetet med personuppgiftsregistret är prioriterat. Dataskyddsorganisationen bör därutöver också fundera på hur personuppgiftsregistret på sikt även kan användas i det löpande dataskyddsarbetet.

2.4.5 Kontrollpunkt 5: Övergripande strategi för dataskydd

Kontrollpunkten avser verksamhetens övergripande strategi för att arbeta med dataskydd.

Dataskyddsombudets kommentarer:

Förvaltningen anger att de har en övergripande strategi för arbetet med dataskydd, att de arbetar systematiskt med att integrera dataskyddsfrågorna i det övriga informationssäkerhetsarbetet och har antagit ett riskbaserat arbetssätt i dataskyddsfrågor. Däremot anges att förvaltningen saknar en informationssäkerhetspolicy som på övergripande nivå anger principer för hur man inom organisationen ska hantera personuppgifter samt att det saknas regelbundna interna kontroller för att säkerställa följsamhet gentemot GDPR. Dataskyddsombudet noterar att förvaltningen anger att de antagit ett riskbaserat arbetssätt i dataskyddsfrågor, vilket är positivt. Dock är dataskyddsombudets uppfattning att ett riskbaserat arbetssätt begränsas genom att förvaltningen saknar ett komplett personuppgiftsregister och därmed saknar överblick över 75 % av de personuppgiftsbehandlingar som görs i verksamheten.

För att lyckas med ett systematiskt dataskyddsarbete är det viktigt att samtliga medarbetare inom förvaltningen har förståelse för hur personuppgifter hanteras på ett säkert sätt. Det innebär bland annat att instruera personalen genom att ta fram policys och andra övergripande dokument. På så vis sätts ramarna för personalen om hur personuppgifter hanteras säkert. Det är därför viktigt att integrera informationssäkerhetsarbetet med dataskyddsarbetet och även kommunicera detta till personalen. Genom att genomföra egenkontroller kan verksamheten dels säkerställa följsamhet gentemot GDPR, dels identifiera var risker finns för att på så vis arbeta riskbaserat och prioritera insatser framåt. Förvaltningen rekommenderas därför att ta fram en informationssäkerhetspolicy som anger hur personuppgifter ska behandlas i bland annat IT-system, datorer och mobila enheter samt fundera på hur den kan användas i arbetet med egenkontroller i verksamheten.

2.4.6 Kontrollpunkt 6: Utbildning

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

Dataskyddsombudets kommentarer:

Förvaltningen har angett låga värden på att den allmänna kunskapsnivån inom verksamheten ger goda förutsättningar i dataskyddsarbetet samt att det finns rutiner för att följa upp och bibehålla kunskapsnivån hos medarbetarna efter genomförd utbildning. I föregående års årsrapport rekommenderade dataskyddsombudet

förvaltningen att kartlägga vilka utbildningar och andra kompetenshöjande insatser som behövs samt följa upp kunskapsnivån efter genomförda utbildningar. Det är dataskyddsombudet förståelse att förvaltningen planerar att genomföra särskild utbildning för rektorer i dataskydd samt att alla nyanställda ska gå grundutbildning i dataskydd, vilket är ett arbete som genomförs utifrån de rekommendationer som lämnades förra året. Dataskyddsombudet anser det vara positivt att förvaltningen genomför dessa åtgärder för att öka kunskapsnivån i verksamheten. Dataskyddsombudet rekommenderar även förvaltningen att följa upp kunskapsnivån efter genomförda utbildningar för att säkerställa att utbildningsinsatserna har haft avsedd effekt.

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:

Förvaltningen har genomgående angett höga värden på området integritetspolicy, förutom att registrerade enkelt kan nå den från verksamhetens samtliga digitala kanaler. Integritetspolicyn är ett sätt att uppfylla informationskraven i art. 13 och 14 GPDR. Förvaltningen anger att verksamhetens integritetspolicy uppfyller kraven på information i enlighet med GDPR, att den kontinuerligt ses över och uppdateras samt att den på ett enkelt sätt tillhandahålls de registrerade.

Dataskyddsombudet gör delvis en annan bedömning och anser att det finns brister vad gäller integritetspolicyns innehåll och utformning. Den information som framgår av integritetspolicyn är alltför vag och ospecifik. Dataskyddsombudet noterar även att det saknas information som ska tillhandahållas enligt art. 13 och 14 GDPR, till exempel rätten att inge klagomål till tillsynsmyndighet samt att förvaltningen utför många behandlingar som inte täcks av integritetspolicyn. Det är dataskyddsombudets förståelse att det för vissa behandlingar ges ut annan, mer specifik information men att det för merparten av behandlingarna saknas sådan information. Eftersom förvaltningen också saknar ett personuppgiftsregister är det dock svårt att uppskatta hur omfattande bristen är. Dataskyddsombudet rekommenderar att förvaltningen kartlägger vilka personuppgiftsbehandlingar som är tänkta att omfattas av policyn på hemsidan och komplettera med den information som saknas. För övriga behandlingar behöver det säkerställas att informationsplikten uppfylls på annat sätt. Informationen i integritetspolicyn behöver vara mer tydlig och koncis för att de registrerade bättre ska kunna förstå hur deras personuppgifter hanteras.

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:

Förskoleförvaltningen har angett låga värden på frågorna kopplat till att verksamheten har anvisningar för hur information får hanteras utifrån gjord informationsklassificering, att verksamheten informerar de registrerade direkt i kontakt vie e-post samt om det finns rutiner och anvisningar för hantering av personuppgifter i e-post, särskilt med hänsyn till känsliga och särskilt skyddsvärda personuppgifter. Vidare har förvaltningen angett att ca 50 % av verksamhetens personuppgiftsbehandlingar har informationsklassificerats samt att för ca 50 % av de personuppgiftsbehandlingar som har informationsklassificerats, är informationen aktuell.

Förvaltningen har angett höga värden på att det finns en dokumenthanteringsplan som omfattar verksamhetens samtliga processer, att det finns rutiner för att kontrollera att personuppgifter gallras i enlighet med gallringsbeslut samt att det finns rutiner för att informera medarbetare om dokumenthantering och gallring kopplat till kraven enligt GDPR.

GDPR ställer höga krav på att personuppgifter hanteras på ett tillräckligt säkert sätt. Dataskyddsombudet konstaterar att förvaltningen redan förra året rekommenderades att se över anvisningen för hur information i olika informationsklasser ska hanteras, kommuniceras och tillgängliggöras inom förvaltningens olika verksamhetsområden. Dataskyddsombudet rekommenderar förvaltningen att ta fram anvisningar för hantering av personuppgifter i e-post och lagringsytor utifrån de olika informationsklasserna samt kommunicera och tillgängliggöra dessa i verksamheten. Sådana anvisningar behöver säkerställa att hela kedjan av personuppgiftsbehandlingarna uppnår tillräcklig skyddsnivå, även i de fall när lagringsytor och verktyg används för mellanlagring/tillfällig lagring, till exempel innan uppgifterna läggs in i ett verksamhetssystem. För att göra detta krävs även att förvaltningen har koll på, och informationsklassificerar, sina personuppgiftsbehandlingar. Förvaltningen behöver också säkerställa att de registrerade får information om hur deras personuppgifter behandlas vid kontakt med förvaltningen.

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:

Förvaltningen anger att ungefär hälften av verksamhetens personuppgiftsbehandlingar har kontrollerats utifrån höga risker för de registrerade samt att det för hälften av verksamhetens personuppgiftsbehandlingar finns framtagna och fastställda konsekvensbedömningar. Då förvaltningen inte har ett komplett personuppgiftsregister och därmed har begränsad översikt över verksamhetens personuppgiftsbehandlingar är dataskyddsombudets bedömning att svaren på kontrollpunkten riskerar att inte avspegla de faktiska förhållandena inom förvaltningen.

Eftersom förvaltningen hanterar barns personuppgifter i stor omfattning är det viktigt att dels ha kunskap om vilka behandlingar som innebär hög risk, dels att genomföra konsekvensbedömningar för behandlingar som innebär hög risk. Det gäller såväl pågående som nya personuppgiftsbehandlingar. Förvaltningen anger att det finns en planering att genomföra konsekvensbedömningar för samtliga av de behandlingar som innebär hög risk, där det ännu inte gjorts. Dataskyddsombudet ser positivt på att planering gjorts och att förvaltningen därmed vidtagit åtgärder utifrån rekommendation från förra årets årsrapport. Samtidigt anges att hälften av verksamhetens personuppgiftsbehandlingar inte har kontrollerats utifrån höga risker för de registrerade. Eftersom förvaltningen saknar ett personuppgiftsregister och därmed saknar en heltäckande överblick över vilka personuppgiftsbehandlingar som utförs, framstår skattningarna som osäkra för dataskyddsombudet.

Dataskyddsombudet rekommenderar därför att förvaltningen, parallellt med arbetet med personuppgiftsregistret, kontrollerar samtliga av verksamhetens behandlingar utifrån höga risker. Förvaltningen riskerar annars att konsekvensbedömningar inte genomförs för behandlingar där det borde göras. Det är även viktigt att förvaltningen fullföljer den planering som finns, så att konsekvensbedömningar faktiskt genomförs för de behandlingar som innebär hög risk.

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:

Förskoleförvaltningen har genomgående inom kontrollpunktens olika områden skattat höga värden. Dataskyddsombudet har inte blivit involverad i några frågor gällande upphandling under året och saknar därför inblick i hur arbetet med att säkerställa dessa fungerar på förvaltningen. Däremot har dataskyddsombudet lämnat rekommendationer för utveckling av befintliga system, vilket visar på att förvaltningen involverar dataskyddsombudet i dessa frågor.

För att öka kunskapen kommer dataskyddsombudet framåt att granska förvaltningens hantering i hur dataskyddsperspektivet säkerställs i arbetet med nya IT- och digitaliseringslösningar.

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 har genomgående skattat höga värden på kontrollpunktens olika områden förutom för verksamhetens användning av cookies på webbsidor. Till exempel anges att verksamheten har dokumenterad och tydlig överblick av sina kommunikationskanaler och rutiner för att kontrollera att användningen av dessa kanaler följer GDPR.

Dataskyddsombudet har under året noterat att förvaltningen använder Facebook som en kommunikationskanal. Även om förvaltningen har fattat beslut om att stänga ner många konton, finns fortfarande förvaltningsövergripande konton som publicerar bilder på barn och lärare. Vid genomgång med förvaltningen angavs att ledningen kommer besluta om hur de förvaltningsövergripande kontona ska fortsätta att användas framåt. Ledningen har vid tiden för denna rapport ännu inte fattat beslut i frågan. Inför ett sådant beslut är det viktigt att dataskyddsombudet ges tid och möjlighet att lämna rekommendationer, så att dataskyddsperspektivet säkerställs i beslutsunderlaget.

Dataskyddsombudet avråder förskoleförvaltningen från att fortsätta behandla personuppgifter i sociala medier i de fall följsamhet mot GDPR inte kan säkerställas. Förvaltningen behöver också säkerställa användningen av cookies på de hemsidor som förvaltningen ansvarar för.

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 de behandlingar som görs i verksamheten. Dataskyddsombudet ser därför främst risker kopplat till att förvaltningen saknar ett komplett personuppgiftsregister.

2.5 Särskilda iakttagelser under året

2.5.1 Förvaltningens användning av sociala medier

Dataskyddsombudet har noterat att förvaltningen under året har fattat beslut om att de konton i sociala medier som drivs av verksamheter i kommunala förskolor och pedagogisk omsorg ska stängas ner. Beslutet gäller dock inte konton som är förvaltningsövergripande eller för öppna förskolor. Dataskyddsombudet har under året fått kännedom om kontot *Förskoleförvaltningen Göteborg* på Facebook. Det är dataskyddsombudets uppfattning att detta är ett förvaltningsövergripande konto och alltså inte omfattas av beslutet ovan. På detta konto förekommer en stor mängd personuppgifter, både gällande barnen och personalen i verksamheten. Personuppgifter förekommer både i text, såsom namn, men även i bild och film. I text förekommer även namn på de förskolor som inlägget handlar om. Dataskyddsombudet anser detta problematiskt ur flera aspekter. Personuppgifter om barn anses extra skyddsvärda i dataskyddsförordningen och uppgifter kopplat till förskoleverksamhet skyddas av sekretess. Inom förskolans verksamhet är det så kallad stark sekretess, vilket innebär att uppgifterna som huvudregel är skyddade av sekretess. Det är därför problematiskt att öppet publicera uppgifter enligt ovan ur ett sekretesshänseende.

Dataskyddsenheten har i maj 2022 lämnat uppdaterade rekommendationer om tredjelandsöverföringar efter Schrems II. Värt att notera är att Schrems-domarna handlar om just Facebook, där konstaterad tredjelandsöverföring förekommer. Det är inte den rättsliga grunden för behandlingen av personuppgifter på sociala medier som i dagsläget främst är problematisk utan den överföring av personuppgifter till USA som man utsätter de registrerade för genom att behandla deras

personuppgifter på till exempel Facebook. Denna problematik kvarstår oavsett vilken rättslig grund som behandlingen har.

Det är också värt att lyfta att det dessutom finns andra perspektiv än enbart de juridiska som är problematisk med användande av sociala medier. Att värna om medborgarnas förtroende är minst lika viktigt, eftersom ett minskat förtroende kan få allvarliga konsekvenser. En viktig del i detta arbete är att skydda de registrerades fri- och rättigheter genom att säkerställa följsamhet mot det regelverk som finns till för att skydda dessa intressen, dvs. dataskyddsförordningen. Men även andra aspekter bör vägas in när det gäller att skydda de registrerades fri- och rättigheter. Det har till exempel uppmärksammats att ett företag inom AI, har använt bilder från just sociala medier för att bygga en omfattande databas av bilder som används för ansiktsigenkänning. Genom att tillgängliggöra bilder på sociala medier förlorar förskoleförvaltningen således kontrollen över bilderna och vet inte för vilka syften de används till av andra aktörer. Eftersom förvaltningen har små barn i sin verksamhet är detta en väldigt problematisk del i användandet av sociala medier som kan medföra negativa konsekvenser för de enskilda barnen under lång tid framöver, som i dagsläget inte går att överblicka eller förutse.

I takt med att digitaliseringen ökar kommer frågan om privatliv, personuppgifter och integritet fortsatt att vara högaktuell. Dataskyddsombudet vill därför uppmana till försiktighet och se långsiktigt på arbetet med att säkerställa skyddet för de registrerades fri- och rättigheter. Dataskyddsenheten avråder förskoleförvaltningen från att fortsätta behandla personuppgifter i sociala medier i de fall följsamhet mot GDPR inte kan säkerställas.

2.6 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 4: Personuppgiftsregister
  Kartlägga och dokumentera personuppgiftsbehandlingar enligt artikel 30 i GDPR.
- Kontrollpunkt 8: E-post och dokumenthantering
  Ta fram anvisningar för hantering av personuppgifter i mejl och lagringsytor utifrån de olika informationsklasserna samt kommunicera och tillgängliggöra dessa i verksamheten.

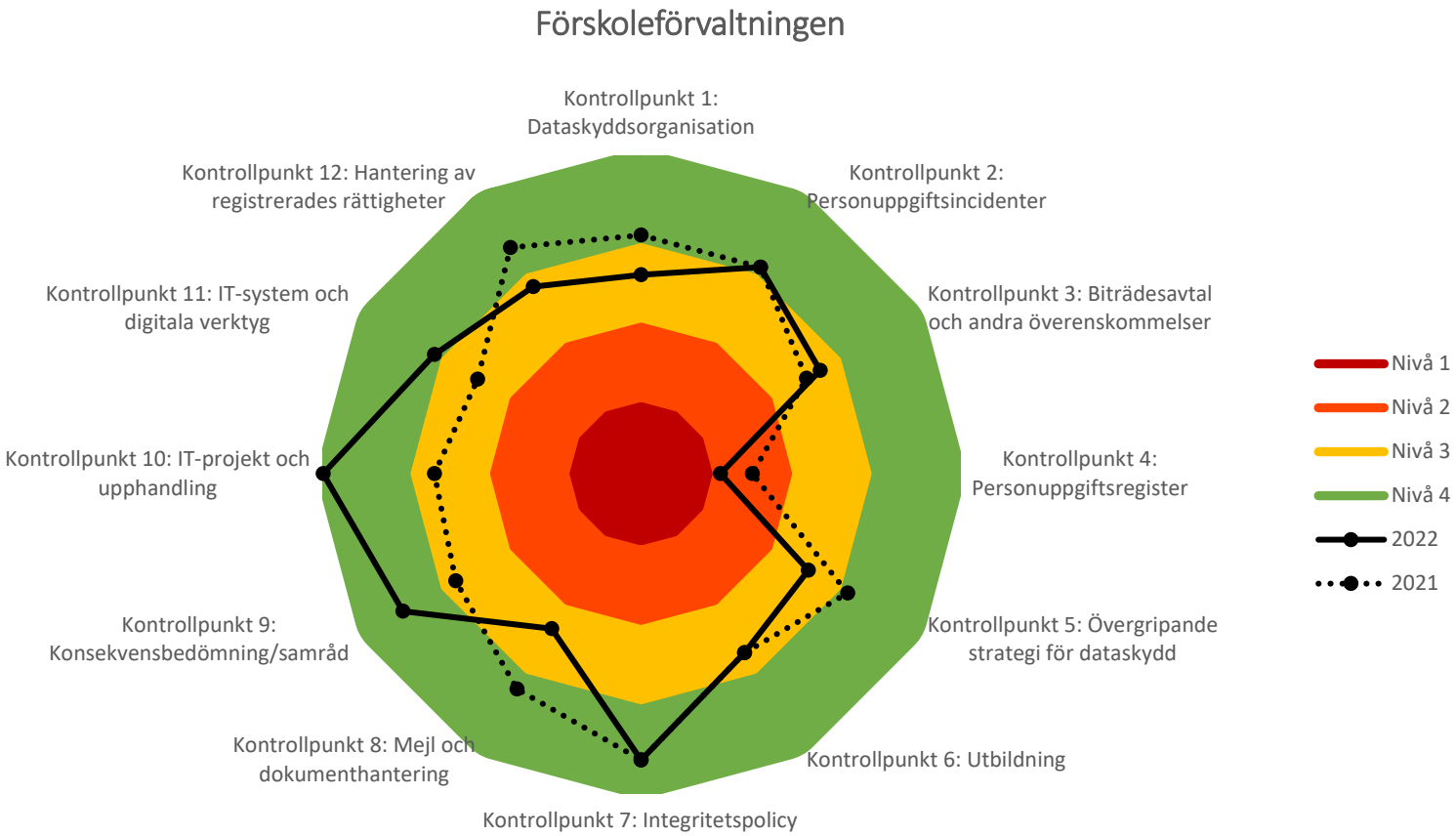
3 Bilagor

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

Bilaga 2: Fördjupad kontroll 2022, samtycke som rättslig grund för verksamhetens personuppgiftsbehandlingar

Bilaga 1

Diagram över resultat av fasta kontrollpunkter, jämfört med 2021



Fördjupad kontroll

Kontrollpunkt 12: Samtycke som rättslig grund för verksamhetens personuppgiftsbehandlingar

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 utså negativa konsekvenser om hen inte samtycker anses inte heller samtycket vara frivilligt.

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 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 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 bifoga underlag. I vissa fall har även uppföljande/kompletterande frågor och avstämningar varit nödvändiga.

Iakttagelser från kontrollen

Förskoleförvaltningen har angett att de tidigare använt samtycke för att behandla annan vuxens (t.ex. en vårdnadshavares nya partner) personuppgifter i lärplattformen Hjärntorget. När Hjärntorget hösten 2022 byttes till Unikum har hanteringen setts över och samtycke för att behandla annan vuxens personuppgifter används därför inte för Unikum. I stället används samtycke från vårdnadshavare för att bryta sekretessen enligt

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

offentlighets- och sekretesslagen och behandlingen i Unikum sker utifrån den rättsliga grunden allmänt intresse.

I övrigt anger förvaltningen att de varken behandlar anställdas eller andra registrerades personuppgifter med samtycke som rättslig grund. Tidigare har förskolor, enskilda förskoleavdelningar, måltidsservice och andra enheter haft konton i sociala medier, där det har förekommit att bilder har publicerats med samtycke som rättslig grund. Förvaltningsledningen har under 2022 fattat beslut om att dessa konton ska stängas ner, därmed ska inte samtycken längre användas inom förskoleförvaltningen. Istället ska Unikum användas för att informera vårdnadshavare om förskolans uppdrag, mål och innehåll i utbildningen samt skapa förutsättningar för barns och vårdnadshavares möjligheter till delaktighet och inflytande.

Förskoleförvaltningen anger således att samtycken inte längre används inom verksamheten som rättslig grund. Förvaltningen anger dock att de bara delvis har överblick av användningen av samtyckesblanketter i de förskolor som förvaltningen ansvarar för. Dataskyddskontakt på förvaltningen genomförde under våren 2022 en kartläggning om samtycken används inom förskolorna genom att skicka ut en enkät till rektorer. Ungefär hälften av rektorerna svarade på enkäten och kunskapsnivån om samtycke tycks variera. En slutsats som förvaltningen drog var att samtycke enligt dataskyddsförordningen och samtycke enligt offentlighets- och sekretesslagen ofta blandas ihop. En utbildningsinsats för förvaltningens rektorer är planerad att genomföras till våren 2022.

Förvaltningen anger även i sitt svar att kommunikationsavdelningen använder medverkandeavtal vid produktion av informationsmaterial och att dessa medverkandeavtal är nära besläktade med samtycken. I sitt svar till dataskyddsombudet har förvaltningen bifogat ”Riktlinje för bild och film inom förskoleförvaltningen” och hänvisar till den för när medverkandeavtalen kan användas och hur personal ska agera praktiskt vid/inför tecknande av medverkandeavtal med registrerade för att uppfylla kraven i dataskyddsförordningen. I riktlinjen finns ett stycke under rubriken ”Så här hanterar vi bilder juridiskt” som anger att avtal med de som medverkar på bild ska skrivas innan publicering sker. Av den avtalsmall för medverkandeavtal som dataskyddsombudet tagit del av framgår att ingen ersättning utgår för medverkan.

Trots att den fördjupade kontrollen avser användandet av samtycken som rättslig grund, har det under kontrollen framkommit att förskoleförvaltningen använder medverkandeavtal. Förvaltningen anger själva att detta medverkandeavtal är nära besläktat med samtycke. Dataskyddsombudet kommer därför att kommentera även användningen av medverkandeavtal vid produktion av informationsmaterial inom förvaltningen. För att kunna kommentera användning av medverkandeavtal ges också en bakgrund till avtal som rättslig grund vid behandling av personuppgifter genom bild och film.

Dataskyddsombudets rekommendationer

Samtycke som rättslig grund

Dataskyddsombudet tycker det är positivt att förskoleförvaltningen under året har sett över de behandlingar som tidigare gjorts med samtycke som rättslig grund och vidtagit åtgärder för att minska användning av samtycken. Eftersom endast hälften av de tillfrågade rektorerna svarade på förvaltningens enkät om samtycke som rättslig grund framgår att förvaltningen saknar en fullständig överblick och kontroll över användningen av samtycken inom sin verksamhet. Dataskyddsombudet rekommenderar därför förvaltningen att fortsätta den planerade utbildningsinsatsen för rektorer för att öka kunskapen om dataskyddsförordningen. Vidare är det viktigt att få överblick av användningen av samtycken i förvaltningens olika verksamheter. Dataskyddsombudet rekommenderar därför att förvaltningen fortsätter kartläggningen som påbörjats för att kunna vidta de åtgärder som krävs för att förvaltningen ska kunna ta sitt ansvar enligt GDPR. Dataskyddsombudet vill även göra ett medskick om att det är viktigt att följa upp de beslut som fattas av förvaltningsledningen. Därför bör en uppföljning göras för att kontrollera att de förskolor som tidigare angett att de använt samtycke som rättslig grund för publicering av bilder i sociala medier, istället använder Unikum som plattform och en annan rättslig grund för att informera om verksamheten till barnens vårdnadshavare.

Medverkandeavtal som rättslig grund

När personuppgifter behandlas i form av bild och film utifrån den rättsliga grunden avtal är både modellavtal och medverkandeavtal vanligt förekommande begrepp. De avser dock samma sak, det vill säga ett avtal som reglerar villkoren när någon är med på bild. Olika typer av hybridslösningar förekommer, alltså att de rättsliga grunderna samtycke och avtal kombineras på ett otillåtet sätt. Det är viktigt att tydligt skilja på de rättsliga grunderna samtycke och avtal och välja en av dessa när personuppgifter behandlas. Vid hybridslösningar riskerar verksamheten att varken uppfylla kraven för avtal eller samtycke enligt dataskyddsförordningen vilket i stället resulterar i en risk för verksamheten.

Vid användande av avtal tecknas detta vanligtvis mellan den personen som förekommer på bilden och den som tar bilden, till exempel en fotograf. Avtalet ska vara tecknat av den registrerade, alltså den vars personuppgifter som behandlas. När barn är med på bilden måste avtal tecknas med dess vårdnadshavare.

I Sverige godkänns både benefika och onerösa avtal, vilket innebär att både avtal där det utgår ersättning och avtal där det inte utgår ersättning är giltiga.

Det är dock viktigt att veta att det alltid är den som ansvarar för att teckna avtalet som ska kunna bevisa att det är giltigt. Det är de faktiska omständigheterna som spelar roll för bedömningen, inte att dokumentet benämns som och kallas för avtal. Avtal där ersättning inte ges kan uppfattas som ett kringgående av dataskyddsförordningen och kan juridiskt i stället anses vara ett samtycke.

Ur bevishänseende, alltså om det skulle uppstå en tvist om avtalets giltighet, är det lättare att hävda att avtalet är giltigt om det har utgått ersättning. Om det inte har utgått ersättning kan det vara svårare att argumentera för avtalets giltighet eftersom det går att

ifrågasätta varför en person skulle ”ge bort” en bild/sina personuppgifter utan motprestation från den andra parten. Om det är svårt att säkerställa frivillighet för ett samtycke, om det exempelvis rör sig om relationen lärare och elev, så är det inte ett alternativ att i stället välja avtal (utan ersättning) som rättslig grund. Problematiken med frivilligheten riskerar nämligen att överföras även på avtalssituationen och kan innebära att den personuppgiftsansvarige utnyttjar den ojämlika maktbalansen till sin fördel och till den registrerades nackdel. Genom avtal kan modellen/den registrerade inte längre förfoga över bilderna, till skillnad mot när samtycke används som rättslig grund, vilket kan återtas.

Sammanfattningsvis innebär detta att i de situationer då det inte finns förutsättningar för att använda samtycke på grund av att frivillighet inte kan säkerställas, finns det heller inte förutsättningar för att använda avtal utan ersättning som rättslig grund.

Dataskyddsombudet konstaterar att förvaltningen använder medverkandeavtal utan ersättning. Av ”Riktlinje för bild och film inom förskoleförvaltningen” framgår att medverkandeavtal ska tecknas innan bilden publiceras men ger ingen praktisk vägledning till personalen. Till exempel saknas dokumenterade rutiner för när medverkandeavtal kan användas och vilka överväganden som behöver göras för att bedöma om avtal kan vara en lämplig rättslig grund. Vidare saknas information om hur det faktiska tillvägagångssättet inför avtalsskrivandet ska utföras för att uppfylla kraven i dataskyddsförordningen, till exempel för att säkerställa att inte ojämna maktförhållanden föreligger. Dataskyddsombudet vill här poängtera att det som regel föreligger en ojämn maktbalans mellan förvaltning och barn, vårdnadshavare samt anställda. I riktlinjen framgår inte heller utifrån vilka olika ändamål som kommunikationen sker eller vilken rättslig grund som är tillämpbar i de olika fallen, mer än att avtal skrivs innan bilder publiceras. Eftersom kommunikation kan ske utifrån en mängd olika ändamål där förutsättningarna kan skilja sig åt bör detta beskrivas för att få en tydlig hantering av bild och film, både för de registrerade och för personalen som arbetar med bilder. Dataskyddsombudet rekommenderar därför förvaltningen att utreda utifrån vilka olika ändamål som kommunikation sker i verksamheten och därefter fastställa lämplig rättslig grund för var och en av behandlingarna samt komplettera med anvisningar om hur följsamhet gentemot GDPR säkerställs för de olika behandlingarna.

Det är även viktigt att reflektera över att personuppgifter om barn anses extra skyddsvärda i dataskyddsförordningen och att uppgifter kopplat till förskoleverksamhet skyddas av sekretess. Inom förskolans verksamhet är det så kallad stark sekretess, vilket innebär att uppgifterna som huvudregel är skyddade av sekretess. Det bör därför övervägas om det är lämpligt att över huvud taget publicera bilder på barn i verksamheten i publika sammanhang. Dataskyddsombudet saknar en utredning i denna fråga från förvaltningen.

Utifrån den dokumentation dataskyddsombudet tagit del av gällande hantering av medverkandeavtal hos förskoleförvaltningen bedöms användandet av bild och film med avtal som rättslig grund utgöra en risk för verksamheten. Detta eftersom det saknas dokumenterade rutiner som beskriver i vilka situationer medverkandeavtal kan användas och som säkerställer att den praktiska hanteringen följer reglerna i dataskyddsförordningen. Den avtalsmall som används innebär i princip att den registrerade lämnar över kontrollen av sina personuppgifter till förvaltningen utan att själv ha möjlighet att påverka användningen av bilderna, dessutom utan att få någon

ersättning. De risker som anges ovan kan innebära att förvaltningen vid användning av bild och film saknar rättslig grund för behandlingen.

Dataskyddsombudet vill även här påpeka att det i riktlinjen står att avtal ska tecknas innan publicering, en viktig distinktion är att avtal måste skrivas innan fotograferingen sker. Dataskyddsombudet noterar även att det saknas information om överföring av personuppgifter till tredje land. Eftersom förvaltningsledningens beslut att inte använda sociala medier inte gäller för hela verksamheten och det i avtalet nämns ”sociala kanaler” vill dataskyddsombudet även här påpeka att den information som ska ges till registrerade enligt art. 13 och 14 dataskyddsförordningen även gäller när avtal används som rättslig grund.

Sammanfattande rekommendationer

- Utred och dokumentera hur hanteringen av förvaltningens användning av medverkandeavtal följer kraven i dataskyddsförordningen.
- Utred och dokumentera frågan om hur bilder kan användas i publika sammanhang utifrån den sekretess som reglerar verksamheten.
- Utred och komplettera riktlinje för bild och film inom förskoleförvaltningen utifrån de olika ändamål som bilder och filmer används i den externa kommunikationen samt säkerställ lämplig rättslig grund utifrån de olika behandlingarna.
- Komplettera riktlinje för bild och film inom förskoleförvaltningen med anvisningar om när och hur medverkandeavtal kan användas inom förvaltningen. Om behandlingar av bild och film fastställs med annan rättslig grund, komplettera med anvisningar för hur följsamhet gentemot GDPR säkerställs för den/dessa behandlingar.
- Fortsätta det arbetet som påbörjats med utbildning för rektorer och fullfölja den påbörjade kartläggningen av användning av samtycken för att få överblick och kontroll att samtycken inte används.

Bilagor

- Frågor och informationsutskick

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/aktuella blankett/blanketter som används.
2. Har förskoleförvaltningen en rutin för hur man inom förvaltningen ska agera rent praktiskt vid/inför inhämtande av samtycke för att uppfylla kravet på frivillighet i dataskyddsförordningen?
    a. Om ja, beskriv hanteringen eller bifoga aktuell rutin.
3. Har förskoleförvaltningen överblick över användningen av samtyckesblanketter i samtliga förskolor som förvaltningen ansvarar för?
    a. Hur har förvaltningen gått till väga för att i del 1 av kontrollen undersöka hur den faktiska användningen ser ut på respektive förskola? (Har t.ex. fråga skickats ut till förskolornas rektorer? Har samtliga återkommit med svar?)
4. Använder förskoleförvaltningen *idag* samtycke som rättslig grund för behandling av ”extra vårdnadshavares”, eller någon annans, personuppgifter i administrativa system till exempel IST eller Unikum?
    a. Om ja, ange för vilka behandlingar samt system.
5. Har förskoleförvaltningen en rutin för när medverkandeavtal kan användas, och för hur man inom förvaltningen ska agera rent praktiskt vid/inför tecknande av medverkandeavtal med anställda eller vårdnadshavare/barn för att uppfylla kraven i dataskyddsförordningen?
    a. Om ja, beskriv hanteringen eller bifoga aktuell rutin.

Obs! Det är mycket viktigt att frågorna besvaras av eller i samråd med rätt befattningar inom förvaltningen/bolaget för att resultatet ska bli korrekt. Säkerställ även en lämplig förankring av svaren inom organisationen innan de översänds till dataskyddsombudet.

Underlaget ska ha inkommit till dataskyddsombudet **senast den 23 juni 2022.** Dataskyddsombudet kan komma att ställa kompletterande frågor i samband med sammanställande av rapporten och/eller genomföra kontroll på plats.

Har du frågor, kontakta ditt huvudansvariga dataskyddsombud.