Göteborgs Stad

Årsrapport för dataskyddsarbetet 2022

Grundskoleförvaltningen

2022-12-22

Innehåll

1 Dataskydd i kommunal verksamhet

Att få ta del av och hantera andra människors personliga uppgifter på ett sådant sätt som kommunala förvaltningar och bolag gör innebär att förvalta ett stort förtroende. Dataskyddsförordningen (GDPR) har tillkommit för att särskilt skydda människors rätt till integritet, och för att värna var och ens rätt att få ha kontroll över vad som sker med uppgifter om ens person. Att förvaltningar och bolag hanterar personuppgifter i enlighet med gällande lag bör vara en självklarhet i syfte att visa omsorg om det förtroende som givits den som har att hantera uppgifterna.

Arbetet med att säkerställa att personuppgifter behandlas enligt reglerna i GDPR behöver genomsyra arbetet inom de kommunala verksamheterna på alla olika plan. Det gäller allt från rutiner och processer för det dagliga arbetet, till arbetet med innovations- och digitaliseringslösningar för framtidens arbetssätt på förvaltningar och bolag inom Göteborgs Stad. I det framåtsyftande arbetet är GDPR ett viktigt redskap för att kunna säkerställa en digitalisering som håller över tid.

1.1 Göteborgs Stads dataskyddsombud

Dataskyddsenheten på Intraservice är Göteborgs Stads dataskyddsombud. Vad som är dataskyddsombudets uppgifter framgår direkt av lagstiftningen i GDPR.[1] Dataskyddsombudets viktigaste uppgift är att övervaka att stadens förvaltningar och bolag följer dataskyddslagstiftningen. Detta sker bland annat genom att samla in information om hur personuppgifter behandlas och genom att kontrollera hur bestämmelser och interna styrdokument som styr dataskyddsarbetet efterlevs.

Dataskyddsombudet har också till uppgift att ge råd och information till förvaltningar och bolag i dataskyddsfrågor. Detta sker genom att dataskyddsombudet är behjälplig när frågor rörande behandlingen av personuppgifter uppkommer hos verksamheterna. Dataskyddsombudet erbjuder också regelbundet utbildningar för stadens medarbetare. Rådgivning ges även till förvaltningar och bolag när dessa genomför konsekvensbedömningar, vilket är en skyldighet som följer av GDPR. Efter att ha identifierat ett särskilt behov av stöd i arbetet med konsekvensbedömningar, har dataskyddsenheten under 2022 tagit fram mallar och mallstöd för det arbetet.

Det är nämnd/styrelse som har det yttersta ansvaret för att verksamheterna följer dataskyddslagstiftningen och dataskyddsombudet ska enligt lag rapportera om detta till högsta förvaltningsnivå.[2] Dataskyddsombudet har inte mandat att fatta beslut åt verksamheterna. Det är i stället genom råd och rekommendationer som 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 användningen av samtycke som rättslig grund 2022

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

Dataskyddsombudet har i rapporten för den fördjupade kontrollen haft vissa synpunkter och därför lämnat ett antal rekommendationer till verksamheten att vidta vissa åtgärder.

Sammanfattade rekommendationer:

- Utreda den faktiska användningen av samtycke som rättslig grund i samtliga verksamheter/skolor för att få en heltäckande bild. I den mån samtycke är en lämplig rättslig grund behöver åtgärder vidtas för att säkerställa att detta sker på ett korrekt sätt. I de fall då samtycke är olämpligt eller onödigt behöver det säkerställas att användningen av samtycke upphör
- Ta fram en övergripande rutin för när samtycke kan användas som rättslig grund. Rutinen bör också innehålla:
    - instruktioner i hur frivillighet kan säkerställas,
    - vilken information som behöver lämnas till registrerade för att uppfylla kraven på specifikt och informerat
- Säkerställa att information om när och hur samtycken kan användas når ut till samtliga verksamheter/skolor
- Utred hur hantering av samtycke ser ut för behandling av personuppgifter vid internationellt samarbete i engelskundervisning
- Avbryta behandlingar av personuppgifter som lutar sig mot ogiltiga samtycken
- Utreda personuppgiftsansvar i de personuppgiftsbehandlingar som sker med stöd av samtycke i samverkansprojekt med Göteborgs Universitet

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.

Kontrollpunkt 1 (2021): Dataskyddsorganisation

Verksamheten gavs följande rekommendationer:

- Kartlägga dataskyddsorganisationen och upprätta/utpeka en roll som ges ett samordnande ansvar
- Utreda hur olika verksamhetsdelar kan involveras för att säkerställa att dataskyddsorganisationen representeras av och når ut till samtliga delar
- Ta fram och besluta om definierade rapporteringsvägar som säkerställer att dataskyddsfrågor når till rätt nivå inom förvaltningen.
- I arbetet rekommenderas förvaltningen att se hur andra förvaltningar i Göteborgs Stad har organiserat sig
- Utreda vilka resurser och vilken kompetens som behövs för att säkerställa dataskyddsperspektivet

Uppföljningen visar att förvaltningen har inlett arbetet med att förbättra och stärka dataskyddsorganisationen men att det faktiska genomförandet i stora delar fortsatt kvarstår. Se avsnitt 2.4.1 för ytterligare kommentarer om dataskyddsorganisationen.

Förnyad uppföljning kommer därför att ske under 2023.

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 Grundskoleförvaltningens 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.

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

2.4.1 Kontrollpunkt 1: Dataskyddsorganisation

Kontrollpunkten avser verksamhetens organisatoriska förutsättningar för att kunna bedriva ett kontinuerligt dataskyddsarbete, och omfattar bland annat verksamhetens dataskyddsorganisation, definierade ansvarsområden och rapporteringsvägar för involverade funktioner samt tillhandahållna resurser för arbetet.

Dataskyddsombudets kommentarer:

Att ha en välfungerande dataskyddsorganisation är en grundläggande förutsättning för att kunna bedriva ett systematiskt och effektivt dataskyddsarbete. En del i detta är sträva efter att göra dataskydd till en integrerad och naturlig del av det dagliga arbetet och att det på samtliga nivåer inom förvaltningen finns kunskap och medvetenhet om dataskydd. Det krävs också formella beslut i frågor rörande dataskydd och att dessa tas på rätt nivå för att ge riktning och vägledning åt förvaltningen i övrigt.

Utifrån förvaltningens egen skattning inom denna punkt finns det insatser och förändringar som behöver göras. Förvaltningen har angett höga värden kopplat till att det finns roller/befattningar med utpekat ansvar och att det finns definierade rapporteringsvägar som säkerställer att information om dataskydd når rätt. I övrigt anges lägre skattningar. Det är positivt att förvaltningen har identifierat detta som ett förbättringsområde. Dataskyddsombudet har också fått information om att det har påbörjats en skiss över hur dataskyddsorganisationen kan byggas upp inom förvaltningen. Även detta är positivt. Dataskyddsombudet ser fortfarande stora risker kopplat till bristen på en heltäckande, tydlig och formaliserad dataskyddsorganisation. Dataskyddsombudet rekommenderar därför att förvaltningen säkerställer att det påbörjade arbetet för att stärka och förtydliga dataskyddsorganisationen går från utredning till genomförande. Detta arbete bör vara prioriterat av förvaltningen.

2.4.2 Kontrollpunkt 2: Personuppgiftsincidenter

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

Dataskyddsombudets kommentarer:

Förvaltningen har på denna punkt angett varierande värden i sin skattning som sammanfattningsvis placerar förvaltningen inom nivå fyra. Det område som förvaltningen skattade lägre är att det saknas rutin för när och hur information till de registrerade ska tillhandahållas samt vilken information som ska lämnas till de registrerade.

Dataskyddsombudet genomförde förra året en fördjupad kontroll avseende hanteringen av personuppgiftsincidenter inom förvaltningen. I denna kontroll framkom att det finns förbättringsområden utifrån vilka dataskyddsombudet gav rekommendationer. Dataskyddsombudets rekommendationer till förvaltningen var då att komplettera rutinen för personuppgiftsincidenter med instruktion/metod för hur en bedömning av risken för de registrerades fri- och rättigheter kan göras, göra incidenthanteringen mindre personberoende genom att tydliggöra och konkretisera rutinen så fler kan följa den samt se över behovet av rutin/plan för att regelbundet informera de anställda om personuppgiftsincidenter och den interna incidenthanteringen.

Dataskyddsombudet har under året, särskilt vid incidenten som berörde läckta personuppgifter från Vklass och hanteringen av denna, noterat att dessa rekommendationer fortsatt är aktuella och därmed kvarstår. När inte informationssäkerhetssamordnarna var på plats blev det tydligt att det saknades en metodik att följa för incidenthantering, vilket hade kunnat undvikas genom tydliga rutiner och arbetssätt. Utifrån incidenten i Vklass rekommenderas också förvaltningen att i sin incidentrutin tydliggöra hur och när information till de registrerade ska lämnas, samt vad denna ska innehålla.

Förvaltningen rekommenderas även att genomföra informations- och utbildningsinsatser för att upplysa medarbetare inom samtliga nivåer och områden om tillvägagångssättet vid en upptäckt incident.

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 i sitt svar att verksamheten saknar rutiner för att kontinuerligt genomföra efterlevnadskontroller av anlitade personuppgiftsbiträden för att säkerställa att dessa uppfyller villkoren enligt biträdesavtalet samt att det saknas rutiner för att bedöma om andra överenskommelser/avtal behöver upprättas avseende gemensam eller annan delad hantering av personuppgifter. Vidare anges att förvaltningen har tecknade personuppgiftsbiträdesavtal med ca 75 % för sina biträden.

Skattningen visar att det finns rutiner för att teckna personuppgiftsbiträdesavtal med nya biträden, men att det saknas biträdesavtal för ca 25 % av förvaltningens anlitade biträden.

Skattningen visar även, precis som föregående år, 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. Grundskoleförvaltningen 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 och teckna avtal när personuppgiftsbiträdesavtal eller andra nödvändiga avtal eller överenskommelser saknas.

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:

Grundskoleförvaltningen har genomgående på denna punkt angett låga värden vilket indikerar att det utgör ett högriskområde för förvaltningen. Förvaltningen placerar sig inom risknivå ett, men gränsar till risknivå två.

Av skattningen kan det utläsas att förvaltningen har registrerat ca 25 % av sina personuppgiftsbehandlingar i ett register, att registret i stora delar inte innehåller all den information som ska finnas enligt GDPR, att det saknas rutiner för att hålla det uppdaterat och att registret inte används som en del i det interna dataskyddsarbetet. Detta stämmer överens med dataskyddsombudets uppfattning om var förvaltningen befinner sig i detta arbete.

Förvaltningen gjorde samma skattning i föregående års enkät och fick då rekommendationen att prioritera detta arbete eftersom det är ett grundläggande krav att ha ett aktuellt och uppdaterat register. Vid en översiktlig genomgång av rapporten tillsammans med förvaltningen angavs att arbetet har inletts och att skattningen möjligen hade varit något högre om den hade utförts idag. Även med beaktande av denna justering återstår ett stort arbete för förvaltningen i denna del som behöver genomföras under 2023. I likhet med föregående år rekommenderas förvaltningen att prioritera detta arbete.

2.4.5 Kontrollpunkt 5: Övergripande strategi för dataskydd

Kontrollpunkten avser verksamhetens övergripande strategi för att arbeta med dataskydd.

Dataskyddsombudets kommentarer:

Förvaltningen anger varierande skattningar för denna kontrollpunkt. De områden som skattas lågt är att verksamheten har en övergripande strategi för arbetet med dataskydd och arbetar systematiskt med att integrera dataskyddsfrågorna i det övriga informationssäkerhetsarbetet, att det saknas rutiner för att säkerställa att styrande dokument som reglerar personuppgiftsbehandlingar hålls uppdaterade samt att verksamheten genomför interna kontroller för att säkerställa följsamhet gentemot GDPR. Vidare anger förvaltningen att 75 % av verksamhetens informationstillgångar har värderats utifrån stadens styrande dokument, att det finns en informationssäkerhetspolicy, att verksamheten har antagit ett riskbaserat arbetssätt i dataskyddsfrågor samt att det finns dokumenterade rutiner för att efterleva kraven i GDPR vid anordnande av fysiska och digitala sammankomster.

Utifrån förvaltningens egen skattning inom denna punkt finns det fortsatt insatser och förändringar som behöver göras. Förvaltningen anger att det saknas en övergripande strategi för arbetet med dataskydd. Dataskyddsombudet instämmer i bedömningen och konstaterar att avsaknad av en heltäckande, tydlig och formaliserad dataskyddsorganisation som effektivt kan rapportera till förvaltningsledning gör att det saknas förutsättningar för tydlig och strukturerad styrning i dataskyddsfrågorna. Vidare bedömer dataskyddsombudet att det riskbaserade arbetssättet begränsas av att förvaltningen inte har dokumenterat ca 75 % av sina personuppgiftsbehandlingar, vilket riskerar innebära att förvaltningen inte har koll på personuppgiftsbehandlingar som innebär höga risker. Dataskyddsombudet rekommenderar därför att förvaltningen genomför de insatser som behövs för att få en tydlig dataskyddsorganisation på plats som, tillsammans med ledningen, kan generera en tydlig styrning i dataskyddsfrågorna.

2.4.6 Kontrollpunkt 6: Utbildning

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

Dataskyddsombudets kommentarer:

Förvaltningen har på denna punkt angett varierande värden i sin skattning. De delar som förvaltningen skattat högre är att den allmänna kunskapsnivån inom verksamheten ger goda förutsättningar i dataskyddsarbetet, att det regelbundet ges möjlighet för medarbetare att delta i utbildningar inom dataskydd samt att det inom

verksamheten regelbundet genomförs informationsinsatser för att utbilda och informera personal inom dataskydd. De områden som förvaltningen skattar lägre är att det saknas rutiner för att följa upp och bibehålla kunskapsnivån hos medarbetare efter genomförda utbildningar samt att verksamheten inte har kartlagt vilken nivå av dataskyddskunskap som olika befattningars arbete kräver för att genomföra utbildningar utifrån detta.

Dataskyddsombudet noterar att förvaltningen har angett ett högre värde gällande att den allmänna kunskapsnivån inom verksamheten ger goda förutsättningar i dataskyddsarbetet jämfört med förra året. Dataskyddsombudet har inte kunskap om vilka insatser som genomförts för att höja den generella kunskapsnivån i verksamheten. Det är dock viktigt att påpeka att denna kontrollpunkt berör alla verksamhetens delar, t. ex. alla skolor och elevhälsan. I olika frågor som dataskyddsombudet haft insyn i under året, till exempel genom den fördjupade granskningen av samtycke som rättslig grund och en incident gällande lösenordshantering i Vklass, framgår att kunskapsnivån varierar i verksamhetens olika delar. Utifrån detta gör dataskyddsombudet delvis en annan bedömning av den allmänna kunskapsnivån inom verksamheten. Dataskyddsombudet rekommenderar förvaltningen att kartlägga behovet av kunskap om dataskydd gällande specifika befattningar, men även utifrån olika delar av verksamheten för att kunna genomföra riktade utbildnings- och informationsinsatser.

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:

Vid jämförelse av förvaltningens skattning inom denna kontrollpunkt med föregående år ser det ut som att det här har skett en försämring. Mot bakgrund av att dataskyddsombudet i förra årets rapportering gjorde vissa anmärkningar och överlag ifrågasatte förvaltningens skattning är det dataskyddsombudets uppfattning att det dock snarare är så att årets skattning bättre överensstämmer med hur det ser ut i verkligheten.

Svaren i denna del indikerar att detta utgör ett riskområde för förvaltningen och att insatser krävs. Integritetspolicyn som görs tillgänglig via goteborg.se är vag, ospecifik och saknar helt uppgifter om vilka faktiska personuppgiftsbehandlingar som förvaltningen utför. Den uppfyller inte kraven enligt GDPR som enligt vägledning och praxis ska tolkas strikt. Det är dataskyddsombudets förståelse att det för ett fåtal behandlingar ges ut annan, mer specifik information men att det för merparten av behandlingarna saknas 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 också säkerställas att informationsplikten uppfylls.

2.4.8 Kontrollpunkt 8: E-post och dokumenthantering

Kontrollpunkten avser verksamhetens rutiner för e-post och dokumenthantering. I detta är en aktuell och fastställd dokumenthanteringsplan med gallringsbeslut en förutsättning för att verksamheten ska kunna säkra följsamhet gentemot dataskyddsförordningen. Även verksamhetens rutin för att säkerställa att gallringsrutiner för personuppgifter följs innefattas.

Dataskyddsombudets kommentarer:

Förvaltningen har inom denna punkt, med ett enstaka undantag, angett höga eller medelhöga värden i sin skattning. Den enda del som sticker ut som ett område där förvaltningen tydligt anser att det behövs en förbättring är att kontrollera att den genomförda informationsklassningen är aktuell. Utifrån föregående års skattning har det för denna punkt skett en klar förbättring, särskilt vad gäller att ha klassat sin information där det förra året uppskattades att ca 25 % har klassats i jämförelse med i år då ca 75 % uppskattas ha klassats. I förhållande till föregående år har det också skett en markant förbättring vad gäller att vid kontakt med registrerade direkt informera dem om hur deras personuppgifter behandlas. Utifrån de som dataskyddsombudet den senaste tiden har haft kontakt med i förvaltningen noteras det att det i dessas signaturer inte finns hänvisningar till förvaltningens integritetspolicy. Dataskyddsombudet har dock ingen insikt i hur det ser ut för medarbetare i resten av förvaltningen.

Dataskyddsombudets uppfattning är också att det saknas central överblick över hur väl dataskyddsarbetet fortlöper i verksamhetens alla delar. Det är därför i viss mån förvånande att så höga värden anges för t.ex. att kontrollera att handlingar innehållandes personuppgifter gallras i enlighet med dokumenthanteringsplanen. För att höga värden ska kunna anges krävs det att förvaltningen faktiskt har kännedom om hur det ser ut i förvaltningens alla verksamhetsdelar, inklusive skolor och elevhälsan. Dataskyddsombudet vill också understryka att alla ytor ska beaktas, t.ex. O365 och Google-miljön.

Utifrån skattningen rekommenderas förvaltningen att kontrollera att den informationsklassificering som genomförts är aktuell. Dataskyddsombudet kommer också framåt att följa upp hur dataskyddsfrågorna beaktas inom detta område.

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 har inom denna kontrollpunkt angett främst höga värden vilket genererar en placering inom riskområde fyra. Enligt skattningen finns det framtagna och fastställda konsekvensbedömningar för ca 75 % av de behandlingar där detta krävs. Det anges också att ca 75 % av alla personuppgiftsbehandlingar har kontrollerats utifrån höga risker. Eftersom förvaltningen saknar ett personuppgiftsregister och därmed saknar en heltäckande överblick över vilka personuppgiftsbehandlingar som utförs är det för dataskyddsombudet oklart hur säker förvaltningen kan vara på dessa skattningar. Dataskyddsombudet vill bl.a. lyfta att det bör finnas flera behandlingar inom personalområdet, inom elevhälsan och för förvaltningens kamerabevakning där konsekvensbedömningar krävs som ännu inte har genomförts.

I förra årets skattning uppskattades det att ca 25 % av de konsekvensbedömningar som krävs har tagits fram. Mot bakgrund av hur många konsekvensbedömningar som dataskyddsombudet varit involverad i under året, varav vissa varit pågående sedan 2020 och 2021, är det för dataskyddsombudet oklart att förvaltningen skulle ha genomfört och fastställt så pass många konsekvensbedömningar under året att den höga skattningen är befogad. Dataskyddsombudet ifrågasätter också den höga skattningen vad gäller att ha rutiner för att genomföra konsekvensbedömningar före det att behandlingar påbörjas. I flera av de konsekvensbedömningar som dataskyddsombudet involverats i under året har det varit oklart om projekt inväntat fastställda konsekvensbedömningar före det att behandlingen påbörjats. Detta utgör enligt dataskyddsombudet ett förbättringsområde för förvaltningen.

Dataskyddsombudet ifrågasätter i flera delar den angivna skattningen och rekommenderar att förvaltningen, parallellt med arbetet med personuppgiftsregistret, kartlägger vilka behandlingar som genomförs där kravet för konsekvensbedömningar är uppfyllt men sådana saknas. Förvaltningen rekommenderas sedan att ta fram en långsiktig och konkret plan för genomförandet av dessa konsekvensbedömningar. Eftersom det för flera behandlingar med hög risk i dagsläget saknas konsekvensbedömningar rekommenderas förvaltningen att prioritera detta arbete.

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:

Grundskoleförvaltningen har på denna punkt skattat sitt arbete med det högsta värdet på samtliga påståenden och placerar sig därmed inom nivå fyra.

Dataskyddsombudet har under det gånga året endast varit involverad i en upphandling som även är densamma som nämndes i föregående års rapport. Dataskyddsombudet är av uppfattningen att förvaltningen haft goda föresatser att involvera dataskyddsombudet i god tid men att så inte skett fullt ut. Enligt dataskyddsombudet saknar förvaltningen inom vissa grupper kunskap om dataskydd vilket påverkar möjligheten att iaktta dessa frågor på ett fullgott sätt och i rätt tid i fråga om upphandlingar. Dataskyddsombudet har själv fått efterfråga uppdateringar och bedömer det som oklart huruvida alla aspekter av dataskydd har säkerställts. Det är också oklart om förvaltningen på ett tillräckligt sätt involverat den egna interna dataskyddskompetensen i arbetet.

Avseende den upphandling där dataskyddsombudet har insikt i förfarandet överensstämmer därför inte dataskyddsombudets uppfattning med förvaltningens i och med de svar som angetts i enkäten. Hur det har sett ut i eventuellt andra upphandlingar kan dataskyddsombudet inte uttala sig om eftersom förvaltningen i så fall inte har involverat dataskyddsombudet.

Dataskyddsombudet rekommenderar att förvaltningen säkerställer att det finns rutiner och processer som täcker in och tydliggör hur och när dataskydd ska beaktas i upphandlingar och i IT-projekt. Dataskyddsombudet rekommenderar också att det säkerställs att personer med dataskyddskompetens från den egna förvaltningen, och dataskyddsombudet i de fall då det är lämpligt, involveras vid upphandlingar som innefattar personuppgiftsbehandlingar.

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 inom denna punkt skattat samtliga påståenden med det högsta värdet vilket indikerar att i princip inga risker finns och att det inte finns några förbättringar att göra. Detta utgör en markant förbättring vid jämförelse med föregående års skattning. Skattningen indikerar att det finns dokumenterade rutiner för tilldelning av behörigheter, att dessa regelbundet följs upp samt att användning

och system regelbundet kontrolleras utifrån förvaltningens antagna rutiner och riktlinjer. Det anges också att det finns rutiner för att säkerställa dataskyddsperspektivet vid införande av kostnadsfria tjänster samt att det finns heltäckande dokumentation över samtliga system och digitala verktyg. Det finns även målgruppsanpassad information till dem som använder digitala verktyg och användningen av cookies följer kraven enligt GDPR. Slutligen anges att det finns överblick över kommunikationskanaler och att det sker kontroller för att tillse att användningen följer GDPR.

Dataskyddsombudet har ingen tydlig inblick i förvaltningens arbete med IT-system och digitala verktyg under det gångna året och anser det oklart att det ska ha skett en så pass markant förbättring i förhållande till föregående år. Särskilt mot bakgrund av förvaltningens organisatoriska utmaningar samt den höga digitaliseringstakten. Dataskyddsombudet anser det också finnas frågetecken kring skattningen av påståendet om överblick över digitala kanaler samt kontroller av dessa. I detta inkluderas bl.a. Kulturskolans användning av sociala medier, förvaltningens användning av LinkedIn och Youtube samt enskilda skolors och klassers användning av sociala medier – även i de fall konton är privata. Här vill dataskyddsombudet också särskilt lyfta Svenska Balettskolan som har en omfattande närvaro på sociala medier.

Dataskyddsombudet rekommenderar att förvaltningen säkerställer att det regelbundet går ut tydlig information till samtliga verksamheter/skolor om användningen av sociala medier. Det rekommenderas också att förvaltningen upphör användandet av sociala medier i de fall följsamhet mot GDPR inte kan säkerställas. Dataskyddsombudet kommer framåt att följa upp hur arbetet fortlöper inom detta område.

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:

Förvaltningen har generellt skattat sitt arbete med registrerades rättigheter högt eller medelhögt. Det område som skattas lägre är att förvaltningen saknar dokumenterade rutiner för tillbakadragande av samtycke från en registrerad. Till exempel anges att verksamheten har en dokumenterad rutin för att hantera begäran om registerutdrag, att det finns en dokumenterad process för att hitta och få tillgång till efterfrågad information vid begäran om registerutdrag samt att verksamheten kan säkerställa att en begäran om registerutdrag hanteras inom 30 dagar.

Dataskyddsombudet har inte blivit involverad i frågor gällande registerutdrag under året och saknar därför inblick i hur arbetet med hanteringen av sådana

begäranden fungerar på förvaltningen. Dock bör påpekas att medvetenheten gällande registrerades rättigheter är kopplat till den generella kunskapen om dataskydd och de behandlingar som görs i verksamheten. Utan överblick av alla behandlingar som sker inom verksamheten, ser dataskyddsombudet en risk att förvaltningen missar behandlingar som görs inom verksamheten vid handläggning av registerutdrag. Det medför även risk för att alla begäranden inte kan behandlas likartat och att de registrerade därmed inte får samma information i registerutdragen, till exempel gällande ändamålen med behandlingen. Dataskyddsombudet ser därför främst risker kopplat till att förvaltningen saknar ett komplett personuppgiftsregister.

Utöver registerutdrag har dataskyddsombudet även lämnat rekommendationer inom ramen för den fördjupade kontrollen avseende samtycke som rättslig grund. Eftersom samtycke som rättslig grund förekommer inom förvaltningen behöver det finnas rutiner för hur återkallande av samtycke ska hanteras för de behandlingar där samtycke används.

2.5 Särskilda iakttagelser under året

2.5.1 Personuppgiftsincident i Vklass

Personuppgiftsincidenten i Vklass har redan berörts i rapporten men mot bakgrund av incidentens omfattning och den uppmärksamhet som den genererade ser dataskyddsombudet att det finns skäl att lyfta vissa aspekter särskilt.

Hanteringen av personuppgiftsincidenten i Vklass sätter enligt dataskyddsombudet ljuset på vissa övergripande förbättringsområden inom förvaltningen. Främst ser dataskyddsombudet att hanteringen hade underlättats av en tydligare och synligare dataskyddsorganisation som regelbundet lyfter upp dataskydds- och integritetsfrågor till en högre nivå inom förvaltningen. Förvaltningen behöver enligt dataskyddsombudet också höja den generella medvetenheten om dataskydd och digital integritet och säkerställa att den når ut till samtliga delar.

Förvaltningen hanterade incidenten enligt gängse krishanteringsrutiner vilka, enligt dataskyddsombudets uppfattning, inte tog dataskyddsperspektivet i beaktande i tillräcklig utsträckning. GDPR innehåller detaljerade regler kring hur personuppgiftsincidenter ska hanteras, vilket inte gjordes fullt ut. Detta gäller särskilt den information som gick ut till de registrerade. Incidenten anmäldes inte heller i enlighet med delegationsordningen vilket indikerar bristande kunskap om organisationen. Dataskyddsombudets uppfattning är att krishanteringsrutinerna främst är framtagna för hantering av frågor kopplade till fysisk säkerhet, inte digital. Mot bakgrund av den höga digitaliseringstakten och då personuppgifter är en högt värderad vara (vilket ju blev mycket tydligt när de läckta personuppgifterna sedan lades ut till försäljning) behöver förvaltningen säkerställa att det finns en hög generell medvetenhet kring risker kopplat till personuppgifter och integritet. Särskilt eftersom grundskoleförvaltningen hanterar personuppgifter i mycket stor

omfattning tillhörande barn, som anses vara extra skyddsvärda, och som inte sällan är av känslig karaktär.

Dataskyddsombudet vill därför uppmana förvaltningen att framåt prioritera arbetet med dataskydd för att säkerställa skyddet för elevers, medarbetares och vårdnadshavares personuppgifter.

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/bolaget under 2023 prioriterar följande delar av dataskyddsarbetet:

- Kontrollpunkt 1: Dataskyddsorganisation
- Kontrollpunkt 4: Personuppgiftsregister
- Kontrollpunkt 9: Konsekvensbedömningar/samråd

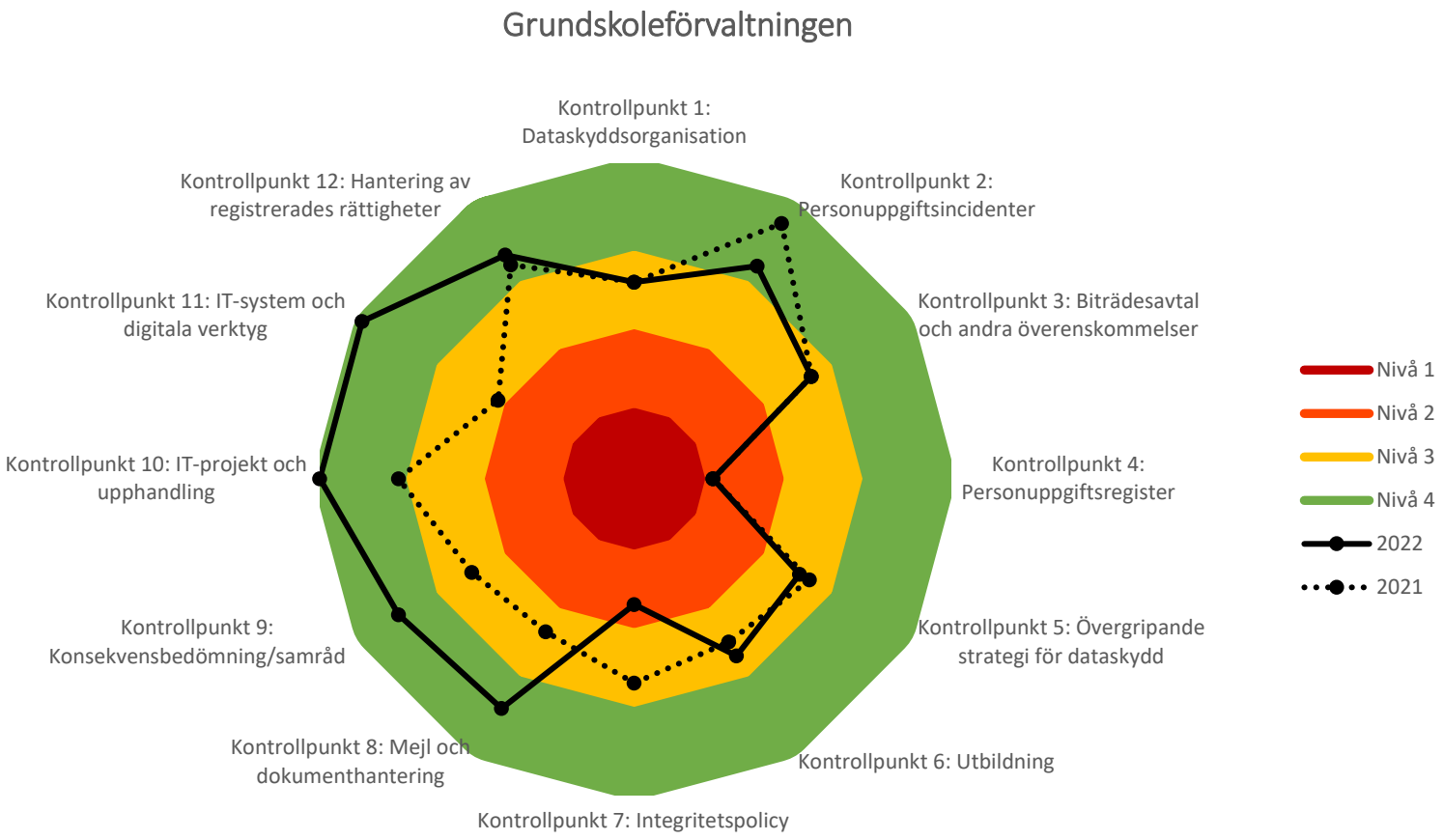
3 Bilagor

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

Grundskoleförvaltningens användning av samtycke

Grundskoleförvaltningen anger i svar till dataskyddsombudet att samtycke som regel inte används som rättslig grund för behandling av personuppgifter i förvaltningen. Det förekommer endast undantagsvis och då främst vid behandling av personuppgifter i form

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

av bild, film och ljud. i undersökningen av den faktiska användningen av samtycke och samtyckesblanketter vände sig grundskoleförvaltningens informationssäkerhetssamordnare till skolornas administratörer och bad dem att skicka in exempel på samtyckesblanketter. De nio svar som inkommit har bifogats i svaret till dataskyddsombudet. Det framgår inte av svaren om eller hur och när samtyckesblanketterna faktiskt används i de olika skolorna eller om det finns pågående personuppgiftsbehandlingar med dessa samtycken som rättslig grund. Det framgår inte heller ifall de skolor som svarat är de enda som använder samtycke som rättslig grund eller om de var de enda som återkom med svar. Vid genomgång med förvaltningen angavs att förvaltningen anser sig överlag ha god insikt i användningen av samtycke, men att ett visst mörkertal ändå kan finnas. Förvaltningen rekommenderas att utreda den faktiska användningen av samtycke för att få en heltäckande bild.

Dataskyddsombudets rekommendationer

Av de svar som inkom och de blanketter som bifogats (varav ett svar inte innehöll en blankett för samtycke enligt GDPR utan vad som verkar vara information kameraövervakning) konstaterar dataskyddsombudet att majoriteten av de inskickade underlagen inte uppfyller de grundläggande kraven enligt GDPR. Dataskyddsombudet kommer nedan att bedöma och kommentera ett urval av de inlämnade blanketterna.

Frivilligt lämnat

Av de svar och blanketter som inkommit kan det i flera fall ifrågasättas om kravet på att ett samtycke ska vara frivilligt lämnat är uppfyllt. För flera av dem innehåller blanketten enbart en fråga eller ett konstaterande i stil med ”Mitt barn får fotograferas/vara med på bild” där vårdnadshavare ska kryssa i ja eller nej. Eftersom det inte framgår hur bilderna ska användas eller varför de tas gör dataskyddsombudet bedömningen att det är oklart huruvida samtyckena i dessa fall uppfyller kravet om frivillighet.

Förvaltningen har även inkommit med en blankett som används av en skola för ett internationellt samarbete för att dela elevarbeten och vara i kontakt med deltagare. Om samtycke inte lämnas anges det att eleven inte kan delta i projektet utan enbart får uppdrag i engelskundervisningen i skolan. Detta tolkar dataskyddsombudet som att ett nekat samtycke leder till negativa konsekvenser vilket blir problematiskt utifrån kravet på frivillighet. Enligt blanketten var projektet aktuellt under vårterminen 2022 och det är därför oklart om samtycket ligger till grund för pågående personuppgiftsbehandlingar. Förvaltningen rekommenderas att utreda detta. Förvaltningen rekommenderas också att ta fram en rutin för samtyckeshantering som inbegriper hur frivillighet säkerställs.

Specifikt och informerat

För de samtycken som lämnats in som enbart består av en fråga eller påstående om att eleven får fotograferas/vara med på bild saknas i princip allt som ett giltigt samtycke ska innehålla. Det anges inte till vad bilderna ska användas, hur länge de ska användas, hur ett samtycke återkallas eller annan information om personuppgiftsbehandlingen. Dessa är alltså varken specifika eller informerade. Personuppgiftsbehandlingarna som sker med stöd av denna grund saknar därför lagliga förutsättningar och rekommendationen är att de

avbryts. Här vill dataskyddsombudet notera att personuppgiftsansvarig inte kan byta rättslig grund under en pågående behandling.[2]

Förvaltningen har även lämnat in en blankett som används för medverkan i projekt om elevers språkutveckling och lärande som utförs av Göteborgs Universitet. Informationen i denna blankett är kortfattad och otydlig. Det framgår motstridig och otydlig information om vilka personuppgifter som de registrerade samtycker till att behandlas. Ändamålet med insamlingen beskrivs i generella ordalag som innebär en risk för ändamålsglidning, det vill säga att insamlade uppgifter används till något annat än dess ursprungliga ändamål. Det framgår inte heller vem det är som är personuppgiftsansvarig för personuppgiftsbehandlingen eller hur den registrerade kan återkalla sitt samtycke och vem/vilka hen då kontaktar. Samtycket uppfyller enligt dataskyddsombudet inte kravet på att vara informerat. Det framgår inte heller annan relevant information om personuppgiftsbehandlingen varför informationsskyldigheten enligt artikel 13/14 GDPR är inte heller uppfylld. Dataskyddsombudet rekommenderar att grundskoleförvaltningen utreder ansvaret för personuppgiftsbehandlingen för att därefter kunna vidta eventuella åtgärder. Enligt blanketten sker samverkansprojektet under läsåren 2020 till 2023 och det får därför antas vara aktiva personuppgiftbehandlingar. Kopplat till samverkansprojekt och samarbeten generellt rekommenderas förvaltningen att ta fram rutiner för hur samtycken i dessa fall ska utformas och administreras, för att göra det tydligt för de registrerade vilken aktör som är ansvarig och säkerställa en korrekt hantering.

Informationsinsatser och rutiner/instruktioner

Utifrån de inlämnade underlagen är det dataskyddsombudets uppfattning att den generella kunskapsnivån om vad ett samtycke är och hur det kan användas är låg. Mot bakgrund av förvaltningens svar på frågorna i del 1 görs bedömningen på central nivå att samtycke oftast inte går att förlita sig på och att allmänt intresse i de flesta fall är den lämpligare grunden. Dataskyddsombudet instämmer i denna bedömning men noterar att bedömningen inte verkar fullt ut ha nått förvaltningens skolor. Att inhämta generella, kortfattade och därmed ogiltiga samtycken i början på terminer angående ”fotografering i anslutning till skolans verksamhet” (som exempel) är onödigt eftersom det inte leder till att förvaltningen har en rättslig grund för att få behandla bilder på elever, utan utgör enbart meningslös administration. Eftersom det helt saknas information i dessa typer av samtycken är det för dataskyddsombudet oklart om bilderna ska användas på ett sätt som kräver ett samtycke eller om det går att luta sig mot allmänt intresse. Dataskyddsombudet rekommenderar att förvaltningen utreder hur denna typ av personuppgifter behandlas i skolorna och att relevanta åtgärder därefter vidtas för att säkerställa följsamhet mot GDPR. Dataskyddsombudet rekommenderar att förvaltningen säkerställer att information om hur och när samtycken kan användas når ut till alla förvaltningens verksamheter/skolor. Både för att säkerställa lagenlighet och för att undvika ett eventuellt resursslöseri.

I svar på frågor till del 1 i kontrollen har förvaltningen angett att det för närvarande saknas styrdokument för samtycke och att planer inte finns för att ta fram allmänna rutiner/instruktioner. Det som i stället planeras är riktade instruktioner för de verksamheter där samtycke bedöms som nödvändigt. Dataskyddombudet instämmer till

[2] Riktlinjer 05/2020 om samtycke enligt förordning (EU) 2016/67 (version 1.1, 4 maj 2020), s. 26

viss del i detta. Det behövs visserligen konkreta instruktioner till de verksamheter där samtycke rimligen kan användas men utifrån den oklarhet som i dagsläget tycks finnas behöver det enligt dataskyddsombudet finnas tydlig styrning i hur och när samtycke kan användas generellt.

Sammanfattande rekommendationer

- Utreda den faktiska användningen av samtycke som rättslig grund i samtliga verksamheter/skolor för att få en heltäckande bild. I den mån samtycke är en lämplig rättslig grund behöver åtgärder vidtas för att säkerställa att detta sker på ett korrekt sätt. I de fall då samtycke är olämpligt eller onödigt behöver det säkerställas att användningen av samtycke upphör
- Ta fram en övergripande rutin för när samtycke kan användas som rättslig grund. Rutinen bör också innehålla:
    - instruktioner i hur frivillighet kan säkerställas,
    - vilken information som behöver lämnas till registrerade för att uppfylla kraven på specifikt och informerat
- Säkerställa att information om när och hur samtycken kan användas når ut till samtliga verksamheter/skolor
- Utred hur hantering av samtycke ser ut för behandling av personuppgifter vid internationellt samarbete i engelskundervisning
- Avbryta behandlingar av personuppgifter som lutar sig mot ogiltiga samtycken
- Utreda personuppgiftsansvar i de personuppgiftsbehandlingar som sker med stöd av samtycke i samverkansprojekt med Göteborgs Universitet

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 grundskoleförvaltningen 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? (Har t.ex. fråga skickats ut till skolornas rektorer? Har samtliga återkommit med svar?)

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 9 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 huvudansvarige dataskyddsombud.