Göteborgs Stad

Årsrapport för dataskyddsarbetet 2023

Förskolenämnden

2023-12-21

Innehåll

1 Inledning

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. Rätten till en fredad privat sfär och personlig integritet är grundläggande i ett demokratiskt samhälle och är ett av fundamenten på vilket många andra av våra demokratiska rättigheter vilar. Dataskyddsreglerna styr hur personuppgifter får samlas in, användas och hanteras för att säkerställa att uppgifterna används korrekt och rättvist. Lagstiftningen finns till för att skydda individen från skada och sätter ramarna för hur personuppgifter får behandlas i en alltmer digital värld. Dataskydd handlar i grunden om att skapa ett socialt hållbart samhälle.

1.1 Dataskyddsombud i Göteborgs Stad

I Göteborgs Stad fullgör dataskyddsenheten på Intraservice uppdraget som dataskyddsombud för förvaltningar och bolag. Vad som är dataskyddsombudets uppgifter framgår direkt av lagstiftningen. Dataskyddsombudet ska ge råd, rekommendationer och informera om frågor som rör behandlingar av personuppgifter. Dataskyddsombudet har även i uppdrag att oberoende granska verksamheternas arbete med dataskyddsfrågor för att säkerställa att dataskyddslagstiftningen efterlevs.

Enligt lag ska dataskyddsombudet rapportera till högsta förvaltningsnivå och i Göteborgs Stad innebär det att dataskyddsombudet rapporterar direkt till nämnder och styrelser. Dataskyddsombudet lämnar årligen en rapport om verksamhetens dataskyddsarbete till varje nämnd och bolag i Göteborgs Stad. I rapporten redogör dataskyddsombudet för de iakttagelser som gjorts och det kontrollarbete som genomförts. För 2023 bestod kontrollarbetet av en granskning av fasta kontrollpunkter och i årsrapporten presenteras resultaten från denna tillsammans med dataskyddsombudets bedömning. Årsrapporten innehåller även resultaten från dataskyddsombudets årliga uppföljning av verksamhetens hantering av lämnade rekommendationer från tidigare genomförda kontroller.

Årsrapporten är avsedd att kunna användas som ett stöd för verksamheten i sitt fortsatta arbete med dataskydd. Det är 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.

2 Särskilda iakttagelser 2023

2.1 Stadenövergripande

2.1.1 Förutsättningar för en hållbar digitalisering

Fokus på ny teknik och AI har en enorm potential för att göra våra liv bättre, men den digitala utvecklingen blir inte hållbar utan begränsningar. Utan tydlig styrning i arbetet med digital innovation är risken att det går fort och att man i sin iver att röra sig framåt glömmer att hänsyn behöver tas till den personliga integriteten och att personuppgifter behandlas på ett korrekt sätt. Verksamheter i Göteborgs stad behöver tydligt ha med sig integritetsaspekten vid framtagandet av innovativa och nya lösningar inom till exempel AI. Arbetet med att säkerställa att personuppgifter behandlas enligt reglerna i dataskyddslagstiftningen 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 inom Göteborgs Stad.

Som en stor offentlig aktör har Göteborg som stad att förvalta alla invånare och besökares förtroende. Oavsett om det handlar om elever, vårdnadshavare, brukare inom socialtjänst, eller någon annan kategori av kommuninvånare, så ska man kunna känna sig trygg med att användandet av innovativ teknik sker med respekt för den personliga integriteten och de regelverk som finns för att skydda enskildas personuppgifter. I takt med att tekniken tar en allt större plats i våra liv ökar också riskerna för att spåra och övervaka människor. På det rättsliga området har detta fört med sig att regleringarna på EU-nivå blir fler och alltmer komplexa. För att utvecklingen ska kunna ske på ett långsiktigt hållbart sätt är det nödvändigt att varje verksamhet förstår de regelverk som finns, och varför de finns. Man kan naturligtvis se det som en balansakt, men som dataskyddsombud vill vi vara extra tydliga med att balansen alltid behöver vara lagd till de enskilda registrerades fördel och aldrig får innebära att verksamheter tummar på det regelverk som finns till för att skydda personuppgifter. Verksamheterna behöver följa dataskydds-lagstiftningen på samma sätt som man behöver följa all annan lagstiftning.

Dataskyddsombudet bedömer att det inom Staden finns en felaktig uppfattning om att det är omöjligt att följa GDPR och samtidigt driva den digitala utvecklingen framåt. Det finns också en felaktig uppfattning om att GDPR är en lagstiftning som inte är obligatorisk att följa. Dataskyddsombudet vill därför särskilt lyfta att dessa uppfattningar är problematiska och medför risker i form av att dataskydds-perspektivet förbises i digitaliseringsarbetet. Fokus behöver därför skiftas från att betrakta reglerna i dataskyddslagstiftningen som hinder, till att i stället fokusera på syftet med lagstiftningen och använda den som en grund att utgå från i utvecklingen av innovations- och digitaliseringslösningar. Ett sådant fokus kommer gynna enskilda individer och samtidigt medföra en mer hållbar och rättssäker digitalisering i samhället på lång sikt.

2.2 Verksamhetsspecifika

2.2.1 Hantering av personuppgifter i Office 365

Dataskyddsombudet har uppmärksammat att förvaltningen på sitt intranät har väldigt få och kortfattade rutiner kopplat till hanteringen av personuppgifter i tjänsterna för Office 365.

Eftersom förvaltningen hanterar barns personuppgifter som är extra skyddsvärda och som inom förskolan omfattas av sekretess utgör detta en risk. Som exempel hade förvaltningen en incident under året kopplat till användningen av Sharepoint. En medarbetare inom förskoleförvaltningen sparade ner ett dokument som innehöll personuppgifter gällande barn på en gemensam yta på Sharepoint. Informationen blev således tillgänglig för medarbetare som egentligen inte skulle haft tillgång till informationen.

För att en säker hantering ska kunna tillämpas är det viktigt att förvaltningen har arbetssätt och utförliga rutiner för hur personuppgifter får hanteras. Det är även viktigt att rutinerna görs tillgängliga för hela förvaltningen så att uppgifterna hanteras på ett enhetligt sätt. Förvaltningen rekommenderas därför att utreda vilka personuppgifter som ska/får hanteras i de olika tjänsterna för Office 365. Förvaltningen rekommenderas även ta fram rutiner och arbetssätt så att hanteringen sker på ett enhetligt sätt inom förvaltningen.

3 Granskning av dataskyddsarbetet 2023

3.1 Kontroll av fasta kontrollpunkter

Under 2023 har dataskyddsombudet kontrollerat verksamhetens dataskyddsarbete utifrån de tolv fasta kontrollpunkterna. Kontrollen har genomförts 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.

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.[1]

Risknivå	Beskrivning	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 bedriver ett systematiskt dataskyddsarbete.	

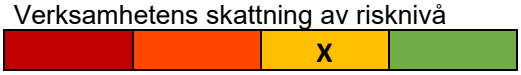
3.2 Resultat från kontrollen 2023

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. För beskrivning av respektive kontrollpunkt se bilaga 2.

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

3.2.1 Kontrollpunkt 1: Dataskyddsorganisation

Verksamhetens skattning av risknivå



Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger risker som behöver åtgärdas, men att dessa inte är brådskande, omfattande eller allvarliga.

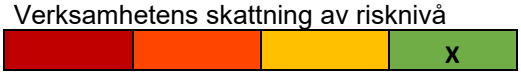
Dataskyddsombudet delar till viss del verksamhetens bedömning, men gör till skillnad ifrån verksamheten bedömningen att det inom kontrollpunkten förekommer risker som är omfattande och kräver åtgärder.

Förvaltningen har under föregående år 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 ser detta som positivt. Dataskyddsombudets bedömning är dock att förändringarna inte har fått det genomslag som hade varit önskvärt. Dataskyddsombudets uppfattning är att dataskyddskontakterna får genomföra ett väldigt stort operativt arbete för hela förvaltningen. Detta är en utmaning som förvaltningen måste ta i beaktande om förvaltningen ska kunna få till en hållbar situation för dataskyddskontakterna och i förlängningen ett hållbart dataskyddsarbete.

I förra årets årsrapport identifierade dataskyddombudet (liksom förvaltningen) att det inte fanns tillräckligt med resurser för att bedriva ett dataskyddsarbete på ett effektivt sätt. I årets skattning har resultatet förbättrats men det föreligger fortsatt risker enligt förvaltningens skattning. En av förvaltningens dataskyddskontakter har även under hösten lämnat sin anställning på förvaltningen och det är i nuläget ovisst om tjänsten kommer att tillsättas på nytt. Dataskyddsombudet väljer därför att lyfta frågan kring resurser med hänsyn till förvaltningens storlek, den pågående digitalisering samt att förvaltningen hanterar personuppgifter gällande små barn. En sådan hantering kräver resurser, kunskap och en medvetenhet hos personalen för att kunna bedriva ett integrerat dataskyddarbete. Efter muntlig avstämning med förvaltningen har det framkommit att det pågår ett arbete kring dataskyddskontaktens roll, men att det ännu inte har fattats något beslut. Likt föregående år rekommenderar därför dataskyddsombudet förvaltningen att fortsätta översynen av dataskyddsorganisationen och tillföra de resurser som behövs för att förvaltningen ska ha förutsättningar för att framåt bedriva ett systematiskt dataskyddsarbete. Förvaltningen bör framåt fokusera på hur dataskydd kan bli en naturlig och integrerad del i det dagliga arbetet i alla delar av verksamheten.

3.2.2 Kontrollpunkt 2: Personuppgiftsincidenter

Verksamhetens skattning av risknivå



Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att verksamheten bedriver ett systematiskt dataskyddsarbete inom ramen för kontrollpunkten och att inga risker av betydelse föreligger.

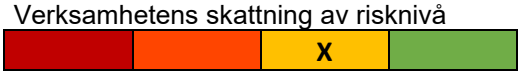
Dataskyddsombudet delar till stor del verksamhetens bedömning. Dataskyddsombudet gör dock till skillnad ifrån verksamheten bedömningen att det ändå föreligger risker inom kontrollpunkten, även om dessa inte bedöms som omfattande, brådskande eller allvarliga.

Dataskyddsombudet har identifierat följande riskområden där verksamheten behöver vidta åtgärder:

Dataskyddsombudet uppfattning är att förvaltningen har ett fungerande arbetssätt gällande hanteringen av personuppgiftsincidenter. Dataskyddsombudet ser dock att förvaltningen behöver utbilda och informera sina medarbetare i en större utsträckning, dels vad en personuppgiftincident är, dels vad förvaltningen har för rutiner för när en personuppgiftsincident sker. Det är viktigt att kunskapen finns inom alla delar av förvaltningen. Förvaltningen har även skattat sig lägre på denna punkt vilket torde indikera på att det finns ett behov av att arbeta vidare med frågan. Efter muntlig avstämning med förvaltningen har det framkommit att det pågår ett arbete inom förvaltningen med att utbilda sina medarbetare, vilket dataskyddsombudet ser som positivt. Dataskyddsombudet rekommenderar därför förvaltningen att fortsatt arbeta med sina utbildningsinsatser samt kartlägga var utbildningsbehov finns. Det är även viktigt att utförliga rutiner finns på plats inom förvaltningen för att arbetet inte ska bli personbundet.

3.2.3 Kontrollpunkt 3: Biträdesavtal och andra överenskommelser

Verksamhetens skattning av risknivå



Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger risker som behöver åtgärdas, men att dessa inte är brådskande, omfattande eller allvarliga.

Dataskyddsombudet delar verksamhetens bedömning om att det finns risker som behöver åtgärdas, men gör precis som verksamheten bedömningen att de inte är omfattande, brådskande eller allvarliga.

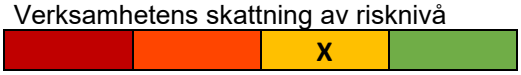
Trots detta finns det ändå områden där verksamheten behöver genomföra åtgärder.

Förvaltningen anger (liksom föregående år) 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 50% av sina personuppgiftsbiträden. Förra året skattade förvaltningen att det fanns avtal tecknade med ca 75% av personuppgiftbiträdena. Årets resultat är alltså en försämring i jämförelse med föregående år. Förvaltningen anger vid muntlig avstämning att man är osäker på varför det har skett en försämring. Det kan bero på ökad medvetenhet inom förvaltningen eller en felaktig skattning. Oavsett orsak behöver förvaltningen fortsatt arbeta med att kartlägga och teckna biträdesavtal där detta behövs.

Skattningen påvisar även att det (liksom föregående år) saknas rutiner och arbetssätt för att följa upp ingångna personuppgiftsbiträdesavtal. Förskoleförvaltningen riskerar därmed att dels sakna nödvändiga avtal som krävs enligt förordningen, dels att sakna kontroll över hur biträden faktiskt hanterar verksamhetens personuppgifter. Rekommendationen kvarstår därmed från förra året att förvaltningen rekommenderas att ta fram rutiner och arbetssätt för att kunna följa upp och kontrollera sina biträden. Förvaltningen bör även 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.

3.2.4 Kontrollpunkt 4: Register över personuppgiftsbehandlingar

Verksamhetens skattning av risknivå



Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger risker som behöver åtgärdas, men att dessa inte är brådskande, omfattande eller allvarliga.

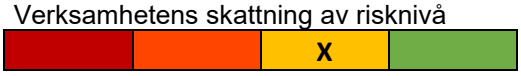
Dataskyddsombudet delar till viss del verksamhetens bedömning, men gör till skillnad ifrån verksamheten bedömningen att det inom kontrollpunkten förekommer risker som är omfattande och kräver omgående åtgärder.

Dataskyddsombudet är medveten om att förvaltningen har påbörjat arbetet med behandlingsregistret under året och därmed påbörjat arbetet med att identifiera förvaltningens behandlingar. Av det underlag som dataskyddsombudet har tagit del av framstår arbetet som ambitiöst. Förvaltningen har själv skattat att ca 50% av förvaltningens behandlingar ingår i behandlingsregistret, vilket är en ökning med ca 25%. Dataskyddombudet ser den utveckling som skett som positiv.

Förvaltningen har dock ett gediget arbete framför sig och det är därför viktigt att de medarbetare som arbetar med registret får resurser till att göra detta. Både när det gäller avsatt tid samt insyn i förvaltningens olika verksamhetsgrenar. Dataskyddsombudet rekommenderar förvaltningen att prioritera detta arbete eftersom detta utgör en direkt risk eftersom förvaltning därmed inte uppfyller kravet enligt artikel 30 GDPR. Om ett register inte finns på plats riskerar även förvaltningen att inskränka de registrerades rättigheter och förvaltningen kan inte bedriva ett effektivt dataskyddsarbete. Förvaltningen har vid muntlig avstämning angett att man kommer att prioritera detta arbete under 2024, vilket dataskyddsombudet ser som positivt. Dataskyddsombudet rekommenderar även förvaltningen att ta fram ett arbetssätt och rutiner för att kontinuerligt uppdatera behandlingsregistret med de behandlingar som tillkommit och förändrats.

3.2.5 Kontrollpunkt 5: Övergripande styrning av dataskyddsarbetet

Verksamhetens skattning av risknivå



Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger risker som behöver åtgärdas, men att dessa inte är brådskande, omfattande eller allvarliga.

Dataskyddsombudet delar verksamhetens bedömning om att det finns risker som behöver åtgärdas, men gör precis som verksamheten bedömningen att de inte är omfattande, brådskande eller allvarliga.

Trots detta finns det ändå områden där verksamheten behöver genomföra åtgärder.

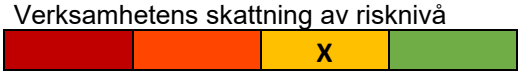
Även om förvaltningens samlade värde på sin skattning är relativt högt, finns det många frågor inom kontrollpunkten där förvaltningen har skattat ett lägre värde. Förvaltningen har angett att det finns en övergripande strategi för arbetet med dataskydd och att de arbetar systematiskt med frågorna. Förvaltningen har dock skattat sig lägre på frågan om förvaltningen arbetar med ett riskbaserat arbetssätt. Dataskyddsombudet delar denna bedömning med förvaltningen eftersom förvaltningen inte har ett komplett behandlingsregister. Utan ett komplett behandlingsregister är det svårt att få en bra överblick inom verksamheten och därmed identifiera var de största riskerna finns. Förvaltningen rekommenderas därför att fortsatt prioritera behandlingsregistret (se rekommendation ovan) och därefter med hjälp av registret aktivt bedriva ett riskbaserat arbetssätt.

Dataskyddsombudets uppfattning är att det finns ett strukturerat arbetssätt inom förvaltningens dataskyddsorganisation. Det saknas dock enligt skattningen dokumenterade arbetssätt för hur förvaltningen hanterar personuppgifter på en övergripande nivå. Även regelbundna interna kontroller gällande efterlevnad av GDPR saknas inom förvaltningen. Dataskyddsombudet rekommenderar därför förvaltningen att ta fram dokumenterade arbetssätt för hanteringen av

personuppgifter på övergripande nivå samt införliva ett arbetssätt som kontrollerar efterlevnaden av dessa.

3.2.6 Kontrollpunkt 6: Utbildning

Verksamhetens skattning av risknivå



Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger risker som behöver åtgärdas, men att dessa inte är brådskande, omfattande eller allvarliga.

Dataskyddsombudet delar verksamhetens bedömning om att det finns risker som behöver åtgärdas, men gör precis som verksamheten bedömningen att de inte är omfattande, brådskande eller allvarliga.

Trots detta finns det ändå områden där verksamheten behöver genomföra åtgärder.

Efter tidigare rekommendationer från dataskyddsombudet om att kartlägga vilka utbildningar och andra kompetenshöjande insatser som behövs har förvaltningen påbörjat en utbildningsinsats. Dataskyddsombudet har även fått information om att förvaltningen tillsammans med avdelningen för HR håller på att arbeta för att alla nyanställda ska genomgå någon typ av grundutbildning. Dataskyddsombudet ser detta som positivt. Trots vidtagna åtgärder har dock förvaltningen skattat sig lägre vad gäller den allmänna kunskapsnivån inom förvaltningen. Förvaltningen har även skattat sig lägre vad gäller att det inte finns dokumenterande arbetssätt för att bibehålla kunskapsnivån och att verksamheten inte i så stor utsträckning har kartlagt vilken kunskapsnivå som de olika befattningarna inom förvaltningen kräver.

Dataskyddsombudet rekommenderar därför förvaltningen att följa upp kunskapsnivån efter genomförda utbildningar för att säkerställa att utbildningsinsatserna har haft avsedd effekt. Dataskyddsombudet rekommenderar även förvaltningen att kartlägga var kunskapen behövs för att kunna rikta sina utbildningsinsatser till rätt mottagare.

3.2.7 Kontrollpunkt 7: Informationsplikt

Verksamhetens skattning av risknivå

Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger risker som behöver åtgärdas, men att dessa inte är brådskande, omfattande eller allvarliga.

Dataskyddsombudet delar till viss del verksamhetens bedömning, men gör till skillnad ifrån verksamheten bedömningen att det inom kontrollpunkten förekommer risker som är omfattande och kräver omgående åtgärder.

Förvaltningens skattning jämfört med föregående års skattning är betydligt lägre. Det ska även tilläggas att förvaltningen i och med sin skattning är på gränsen till att ytterligare falla ner en risknivå.

Dataskyddsombudets bedömning är att det inom kontrollpunkten finns omfattande risker som behöver prioriteras. Dataskyddsombudet rekommenderar därför förvaltningen i likhet med föregående år att uppdatera sin integritetpolicy på hemsidan. Förvaltningen utför många behandlingar som inte täcks av integritetpolicyn. Detta är speciellt kritiskt eftersom förvaltningen ofta vid konsekvensbedömningar hänvisar till sin integritetspolicy som ett sätt att uppfylla informationsplikten. Dataskyddsombudet har förstått att det för vissa behandlingar ges information på annat sätt, men dataskyddsombudets uppfattning är att det för merparten av behandlingarna saknas sådan information. Dataskyddsombudet rekommenderar att förvaltningen kartlägger vilka personuppgiftsbehandlingar som är tänkt 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.

Utifrån de omfattande krav som ställs på personuppgiftsansvariga att tillhandahålla registrerade korrekt, enkel och konkret information om de personuppgifter som behandlas anser dataskyddsombudet att det finns större risker inom detta område än vad förvaltningens skattning ger uttryck för. Dataskyddsombudet bedömer därför även att förvaltningen framåt behöver göra en ordentlig översyn av hur förvaltningen hanterar och uppfyller informationsplikten som helhet.

3.2.8 Kontrollpunkt 8: E-post och dokumenthantering

Verksamhetens skattning av risknivå

Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger risker som behöver åtgärdas, men att dessa inte är brådskande, omfattande eller allvarliga. Dataskyddsombudet delar till viss del verksamhetens bedömning, men gör till skillnad ifrån verksamheten bedömningen att det inom kontrollpunkten förekommer risker som är omfattande och kräver omgående åtgärder.

Förra året rekommenderade dataskyddsombudet förvaltningen att ta fram anvisningar för hantering av e-post och lagringsytor utifrån de olika informationsklasserna samt kommunicera och tillgängliggöra dessa i verksamheten. Förvaltningen har under året tagit fram en rutin kopplat till e-posthanteringen som finns tillgänglig på förvaltningens intranät. Av rutinen framgår att vissa personuppgifter som omfattas av sekretess, som är skyddsvärda

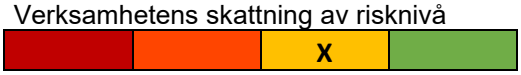
och/eller känsliga enligt GDPR kan skickas via e-post, en förutsättning är dock att mejlet krypteras. Desto känsligare personuppgifter som hanteras desto större krav behöver ställas på säkerheten. Dataskyddsombudet saknar en bedömning från förvaltningen sida huruvida krypteringslösningen som ska användas uppfyller vissa säkerhetskrav. Det är därför viktigt att förvaltningen gör en analys och dokumenterar sina slutsatser. Även hanteringen av sekretessbelagda uppgifter i e-post behöver utredas eftersom hanteringen kan innebära ett röjande av sekretessen gentemot leverantören. Innan ovanstående frågor har utretts av förvaltningen avråder dataskyddsombudet förvaltningen att behandla känsliga, särskilt skyddsvärda och sekretessbelagda personuppgifter via e-post.

Förvaltningen har skattat sig lägre vad gäller dokumenterande arbetssätt för att kontrollera att handlingar som innehåller personuppgifter gallras enligt gällande gallringsbeslut samt att informera medarbetare om dokumenthantering och gallring kopplat till kraven i GDPR. För att förvaltningen ska kunna uppfylla principen om lagringsminimering i GDPR är det viktigt att förvaltningen säkerställer att personuppgifter inte behandlas längre än nödvändigt samt att kunskap finns inom verksamheten. Dataskyddsombudet rekommenderar därför förvaltningen att ta fram rutiner för gallring.

Skattningen visar vidare att det inom kontrollpunkten föreligger risker kopplat till informationsklassificering och avsaknaden av dokumenterade arbetssätt för hur information i olika informationsklasser ska hanteras och vilka lagringsytor som får användas. Utifrån de risker som en oreglerad informationshantering innebär rekommenderas förvaltningen framåt se över huruvida det finns dokumenterade arbetssätt/anvisningar för hur information i olika informationsklasser ska hanteras och vilka lagringsytor som får användas. Om dokumenterade arbetssätt saknas rekommenderas förvaltningen ta fram detta.

3.2.9 Kontrollpunkt 9: Konsekvensbedömning/samråd

Verksamhetens skattning av risknivå



Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger risker som behöver åtgärdas, men att dessa inte är brådskande, omfattande eller allvarliga.

Dataskyddsombudet delar till viss del verksamhetens bedömning, men gör till skillnad ifrån verksamheten bedömningen att det inom kontrollpunkten förekommer risker som är omfattande och kräver åtgärder.

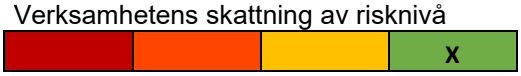
Dataskyddsombudets uppfattning är att förvaltningen gör konsekvensbedömningar inför nya och förändrade behandlingar. Dataskyddsorganisationen inom förvaltningen har även involverat andra funktioner i arbetet med framtagandet av konsekvensbedömningar, vilket dataskyddsombudet ser som positivt.

Förvaltningen har angett att det finns konsekvensbedömningar framtagna för ca 50% av förvaltningens behandlingar som innebär höga risker. Av de som inte är framtagna och som innebär höga risker finns det en dokumenterad planering att genomföra ca 50%. Förra året angav förvaltningen att det fanns planering för att genomföra konsekvensbedömningar för samtliga av de behandlingar som innebär höra risker men som ännu inte hade gjorts. Årets skattning är därmed en försämring jämfört med föregående år.

Eftersom förvaltningen saknar ett komplett behandlingsregister och därmed saknar en heltäckande överblick över vilka personuppgiftsbehandlingar som utförs, framstår skattningarna som osäkra för dataskyddsombudet. Dataskyddsombudet rekommenderar (liksom föregående år) att förvaltningen parallellt med arbetet med personuppgiftsregistret, kontrollerar samtliga av verksamhetens behandlingar utifrån höga risker och tar fram en handlingsplan för arbetet med konsekvensbedömningar. 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.

3.2.10 Kontrollpunkt 10: IT-projekt och upphandling

Verksamhetens skattning av risknivå



Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att verksamheten bedriver ett systematiskt dataskyddsarbete inom ramen för kontrollpunkten och att inga risker av betydelse föreligger.

Dataskyddsombudet har under året inte involverats i någon fråga kopplad till kontrollpunkten, varför ingen övergripande bedömning kan göras i frågan.

Förvaltningen rekommenderas därför att fortsatt arbeta för att bibehålla de goda förutsättningar som finns enligt skattningen samt involvera sitt dataskyddsombud vid nya projekt och/eller i samband med upphandlingar.

3.2.11 Kontrollpunkt 11: IT-system och digitala verktyg

Verksamhetens skattning av risknivå

Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger risker som behöver åtgärdas, men att dessa inte är brådskande, omfattande eller allvarliga.

Dataskyddsombudet delar till viss del verksamhetens bedömning, men gör till skillnad ifrån verksamheten bedömningen att det inom kontrollpunkten förekommer risker som är omfattande och kräver omgående åtgärder.

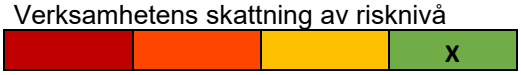
Likt föregående år har förvaltningen skattat sig högt på de flesta av frågorna inom kontrollpunkten. De kontrollpunkter som förvaltning har en lägre skattning på är verksamhetens användning av cookies samt uppföljning av medarbetares behörigheter. Förvaltningen har vid muntlig avstämning angett att det i nuläget pågår ett arbete där förvaltningen bland annat ser över rektorernas behörigheter då de inom vissa frågor samarbetar med varandra. Dataskyddsombudet rekommenderar förvaltningen att i samband med arbetet säkerställa att inte fler behörigheter än nödvändigt tilldelas. Det är även viktigt att förvaltningen förhåller sig till tillämplig sekretesslagstiftning.

Dataskyddsombudet rekommenderar vidare förvaltningen att inom ramen för kontrollpunkten säkerställa användningen av cookies på de hemsidor som förvaltningen ansvarar för samt se över de rutiner som finns kopplat till uppföljning av medarbetarnas behörigheter. När det gäller användningen av cookies har dataskyddsombudet sedan tidigare tagit fram ett informationsmaterial som tillhandahållits stadens verksamheter. Informationsmaterialet redogör för gällande lagkrav och innehåller exempel på hur en cookieruta kan utformas. Förvaltningen rekommenderas utgå från detta i arbetet.

Dataskyddsombudet har även noterat vid genomgång av förvaltningens kommunikationskanaler att förvaltningen även i år använder flera sociala medier. Trots att förutsättningarna för överföringar till amerikanska leverantörer har ändrats finns fler aspekter att ta hänsyn till än enbart tredjelandsproblematiken. Förvaltningen rekommenderas bland annat att kartlägga vilka behandlingar och vilka personuppgifter som behandlas av verksamheten kopplat till användningen av sociala medier, utreda om profilering sker och identifiera vilka ansvarsförhållanden som råder mellan förvaltningen och sociala medieplattformarna för de olika behandlingarna. Vidare rekommenderas förvaltningen att utföra och dokumentera noggranna riskanalyser samt se över för vilka behandlingar kopplat till användningen av sociala medier som kräver en konsekvensbedömning. Dataskyddsombudets uppfattning är att det inte går att utesluta att användningen av sociala medier sannolikt kan leda till en hög risk för de registrerades fri- och rättigheter. Dataskyddsombudet avråder förvaltningen från publiceringar på sociala medier i de fall följsamhet mot GDPR inte kan säkerställas.

3.2.12 Kontrollpunkt 12: Hantering av registrerades rättigheter

Verksamhetens skattning av risknivå



Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att verksamheten bedriver ett systematiskt dataskyddsarbete inom ramen för kontrollpunkten och att inga risker av betydelse föreligger.

Dataskyddsombudet delar till stor del verksamhetens bedömning. Dataskyddsombudet gör dock till skillnad ifrån verksamheten bedömningen att det ändå föreligger risker inom kontrollpunkten, även om dessa inte bedöms som omfattande, brådskande eller allvarliga.

Dataskyddsombudet har identifierat följande riskområden där verksamheten behöver vidta åtgärder:

Förvaltningen har skattat sig lägre på frågan om det inom verksamheten finns en utbredd medvetenhet om vilka rättigheter de registrerade har enligt GDPR. Om medarbetarna inte har kunskap om de registrerades rättigheter ser dataskyddombudet en risk med att dessa inte hanteras i enlighet med förordningen. Dataskyddsombudet rekommenderar därför att förvaltningen vidtar de rekommendationer som lämnades under kontrollpunkt sex, utbildning.

Förvaltningen har i övrigt skattat högre värden på resterande frågor. Dataskyddsombudet ställer sig dock frågande till hur förvaltningen tillgodoser rätten till registerutdrag på ett likvärdigt sätt inom förvaltningen när ett komplett behandlingsregister saknas. Många av behandlingarna saknar ett på förhand definierat ändamål och dataskyddsombudet ser därför en risk med att registerutdragen inte innehåller samma information om till exempel ändamål. Dataskyddombudet ser därför att förvaltningen fortsatt behöver arbeta med behandlingsregistret för att kunna tillgodose de registrerades rätt till information om behandlingen av deras personuppgifter.

3.3 Uppföljning

3.3.1 Uppföljning av rekommendationer lämnade inom ramen för tidigare genomförda kontroller

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

Kontroll (2022): Samtycke som rättslig grund för verksamhetens personuppgiftsbehandlingar

Verksamheten gavs följande 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 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.

Kommentarer och rekommendationer:

Av uppföljningen på dataskyddsombudets fördjupande granskning från 2022 framgår att förskoleförvaltningen har fattat beslut om att ha ett officiellt konto på Meta och Linkedin. Förskoleförvaltningen publicerar där bilder och filmer på barn och vuxna. Innan publicering sker gällande barn och/eller vårdnadshavare upprättas ett medverkandeavtal.

Dataskyddsombudet har efter den fördjupande granskningen uppmanat förvaltningen att vidta vissa åtgärder. Dataskyddsombudet uppmanade bland annat förvaltningen att utreda om förvaltningens användning av medverkandeavtal följer kraven i GDPR. Förvaltningen har i uppföljningen redogjort för sina ställningstaganden och avvägningar. Dataskyddsombudet har identifierat risker kopplat till den sekretess som föreligger inom förskolan, den rättsliga grund som förvaltningen har angivit samt omsorgsplikten som är ett krav utifrån GDPR.

Sekretess
Av offentlighets- och sekretesslagen 23 kap 1§ framgår det att det föreligger sekretess inom förskolan för uppgift om den enskildes personliga förhållanden. Förvaltningen har angett att ett medverkandeavtal bryter den sekretess som råder inom förskolan. Dataskyddsombudet har på intranätet tagit del av förvaltningens medverkandeavtal. Dataskyddsombudet uppfattning är att det inte framgår av medverkandeavtalet att personuppgifterna överhuvudtaget omfattas av sekretess och att ingånget avtal skulle innebära att man bryter den sekretess som föreligger. Den registrerade kan omöjligt utläsa att så skulle vara fallet, vilket i sig är anmärkningsvärt.

Det är även viktigt att påtala att förvaltningen inte kan ”avtala bort” sekretessen. Den enskilde kan dock enligt offentlighets- och sekretesslagen samtycka till att uppgifterna lämnas ut. Om den enskilde samtycker till att uppgifterna lämnas ut, sker dock samtycket för just det specifika tillfället och för ett tydligt angivet ändamål. Det står alltså inte förvaltningen fritt att förfoga över uppgifterna vid ytterligare tillfällen. Då måste ett nytt samtycke inhämtas.

Rättslig grund
Förvaltningen har angett att det övergripande syftet för förvaltningens externa kommunikation är att bidra till förvaltningens kommunikationsmål, att öka allmänhetens förtroende och kunskap om förskolan. Förvaltningen har även angett att den rättsliga grund som är tillämplig för behandling av personuppgifter i externa kommunikationskanaler är dataskyddsförordningens artikel 6.1e, uppgift av allmänt intresse.

För att förvaltningen ska kunna stödja sig på den rättsliga grunden allmänt intresse krävs det stöd i lag eller annan författning, till exempel skollagen eller i nämndens reglemente. Behandlingen måste även vara nödvändig och proportionerlig.

Förvaltningen har i uppföljningen inte hänvisat till något uttryckligt stöd. Dataskyddsombudet kan inte heller utifrån skollagen utläsa att extern kommunikation via sociala medier är någonting som ingår i förvaltningens uppdrag. En nämnds reglemente kan utgöra sådant författningsstöd, men en förutsättning är dock att det är tydligt angivet att det är en uppgift som nämnden har att utföra. Förvaltningen behöver därför se över och hänvisa till vilken grund som förvaltningen grundar behandlingen på.

Om förvaltningen inte finner stöd i lag eller annan författning kan behandlingen inte utgöra allmänt intresse enligt förordningens mening. Förvaltningen behöver då utreda om någon annan rättslig grund är tillämplig. Om förvaltningen inte finner tillämplig rättslig grund är behandlingen inte tillåten och dataskyddsombudet avråder då förvaltningen att fortsätta behandlingen.

Omsorgsplikt
Om förvaltningen använder sig av sociala medier behöver förvaltningen säkerställa att personuppgiftsbehandlingen följer reglerna i GDPR. Förvaltningen behöver först och främst identifiera vem som är personuppgiftsansvarig för de behandlingar som innefattar publicering av bilder på barn/vårdnadshavare. Det gäller både i förhållande till leverantören av Meta och Linkedin. Om leverantören är personuppgiftsbiträde ska ett personuppgiftsbiträdesavtal finnas på plats som reglerar ansvaret mellan aktörerna. För att säkerställa att förvaltningen uppfyller sin ansvarsskyldighet och omsorgsplikt enligt GDPR behöver även eventuella underleverantörer kontrolleras. För att tredjelandsöverföring ska vara lagenlig behöver även underleverantörer vara certifierade enligt ramverket eller ha en annan grund för överföring.

Slutligen bör även den personuppgiftsansvariges möjlighet att uppfylla omsorgsplikten vid val av leverantör vägas in. Meta, som levererar flera av de sociala medieplattformarna, har vid flera tillfällen det senaste året belagts med sanktionsavgifter för felaktig hantering av personuppgifter. Överträdelserna gällde bland annat olaglig överföring av personuppgifter till USA, bristande säkerhetsåtgärder och olaglig behandling av personuppgifter.

Sammantagen bedömning

Utifrån ovanstående rekommenderas förvaltningen att:

- Se över nuvarande medverkandeavtal och utreda huruvida förvaltningens hantering av sekretessbelagda personuppgifter är rättsenligt.
- Se över rättslig grund. För att allmänt intresse ska vara tillämpligt måste förvaltningen finna stöd i lag för behandlingen samt redogöra för varför behandlingen är nödvändig och proportionerlig.
- Omhänderta de rekommendationer som lämnas inom ramen för kontrollpunkt 11 kopplat till användningen av sociala medier om förvaltningen avser publicera bilderna i dessa kanaler.

Fram tills ovanstående punkter har omhändertagits avråder dataskyddsombudet förvaltningen att fortsätta publicera bilder på barn och vårdnadshavare i sociala medier. Uppföljning kommer ske igen under 2024.

4 Rekommenderade fokusområden 2024

Utifrån höga föreliggande risker för de registrerades fri- och rättigheter har dataskyddsombudet identifierat ett antal områden som verksamheten rekommenderas att särskilt arbeta med under det kommande året. Dessa listas i punktform enligt nedan. Detta är områden som dataskyddsombudet särskilt kommer att följa upp framåt. Uppföljningen kommer ske löpande under det kommande året, i dialog med verksamheten.

Utifrån identifierade risker är dataskyddsombudets sammanfattande rekommendationer till nämnden att under 2024 prioritera följande delar av dataskyddsarbetet:

- Kontrollpunkt 4: Register över personuppgiftsbehandlingar

Fortsätt arbetet med att uppdatera befintligt register. Gå igenom de dokumenterade behandlingarna och kontrollera att informationen uppfyller kraven enligt artikel 30 i GDPR.

- Kontrollpunkt 7: Informationsplikt

Dataskyddsombudet rekommenderar förvaltningen att säkerställa att informationsplikten enligt artikel 13 och 14 GDPR i stort uppfylls. Som ett led i detta rekommenderas förvaltningen att kartlägga vilka behandlingar som registrerade ska få information om genom förvaltningens integritetpolicy. Därefter rekommenderas förvaltningen att komplettera integritetpolicyn med information om dessa behandlingar. Förvaltningen rekommenderas även att säkerställa att det lämnas information för de behandlingar som inte är tänkta att omfattas av integritetpolicyn.

- Fördjupad kontroll: Samtycke som rättslig grund för verksamhetens personuppgiftsbehandlingar

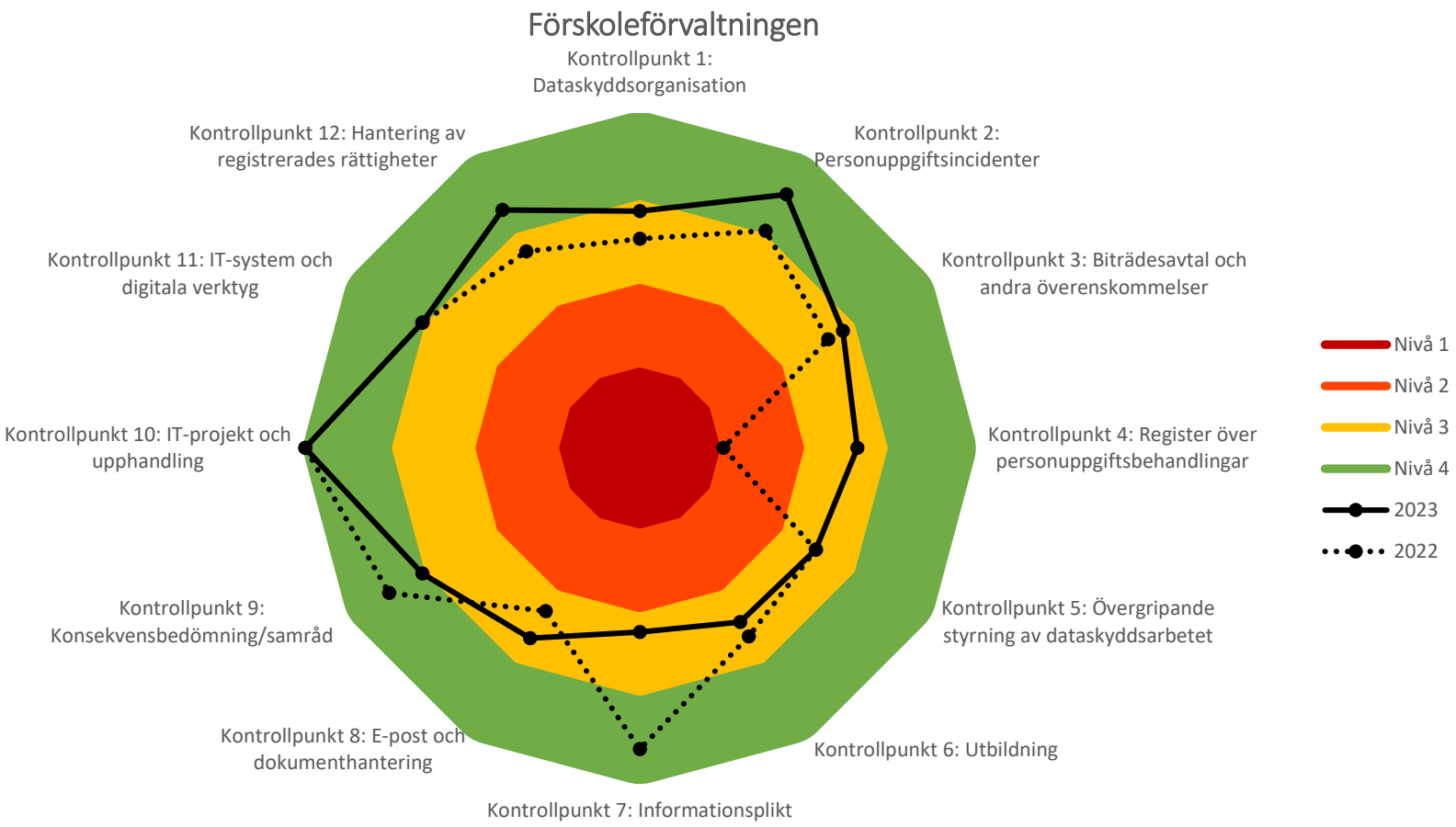
Omhänderta de rekommendationer som lämnats under punkt 3.3.1 kopplat till medverkandeavtal, hantering av sekretessbelagda personuppgifter, rättslig grund samt ansvarsförhållanden.

5 Bilagor

Bilaga 1: Diagram över resultat av fasta kontrollpunkter, jämfört med 2022.

Bilaga 2: Kontrollplan för dataskyddsarbetet 2023–2024.

Bilaga 1: Diagram över resultat av fasta kontrollpunkter, jämfört med 2022.



Göteborgs Stad

Förskoleförvaltningen

Kontrollplan för dataskyddsarbetet 2023–2024

2023-02-06

Innehåll

1 Bakgrund

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 värna om den enskildes rätt till integritet och kontroll över vad som sker med ens personuppgifter. 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 personuppgifter.

Det är varje nämnd och bolaget som är ytterst ansvarig för att dess verksamhet följer dataskyddslagstiftningen. För att stödja stadens nämnder och bolag i arbetet med dataskydd har ett dataskyddsombud utsetts. I Göteborgs Stad fullgör dataskyddsenheten på Intraservice uppdraget som dataskyddsombud. Dataskyddsombudet har särskild sakkunskap i dataskyddslagstiftning och arbetar bland annat för att hålla nämnden/bolaget informerade om hur verksamheten lever upp till dataskyddslagstiftningen. Vad som är dataskydds-ombudets uppgifter framgår direkt av GDPR. En av dessa uppgifter är att övervaka att stadens förvaltningar och bolag följer dataskyddslagstiftningen. När dataskyddsombudet kontrollerar efterlevnaden av dataskyddslagstiftningen sker det bland annat genom att samla in information om hur personuppgifter behandlas inom en verksamhet och genom att kontrollera hur bestämmelser och interna styrdokument som styr dataskyddsarbetet efterlevs.

1.1 Ny utformning av kontrollarbetet

För att ytterligare stärka kvaliteten i verksamheternas dataskyddsarbete kommer dataskyddsombudets kontrollarbete att framgent löpa över tvåårsperioder. Tidigare har kontrollarbetet planerats årsvis, vilket ändras från och med år 2023. För att också underlätta verksamheternas egen planering kommer en ny kontrollplan att skickas ut varje år, som omfattar både innevarande och nästkommande kalenderår.

Kontrollarbetet kommer även fortsättningsvis bestå av tre delar, men frekvensen för den fasta respektive fördjupade kontrollen ändras. Framåt kommer dessa kontroller att ske vartannat år och under 2023 kommer en kontroll av de fasta kontrollpunkterna att genomföras. Genom att alternera den fasta respektive fördjupade kontrollen mellan åren får verksamheterna mer tid till att omhänderta resultaten från kontrollerna, vilket bedöms kunna bidra till ökad kvalitet på vidtagna åtgärder såväl som lagefterlevnad. Detta ligger också i linje med önskemål från flera verksamheter som har signalerat att tätt liggande kontroller gör det svårt att hinna med att arbeta med de lämnade rekommendationerna.

Den nya utformningen innebär även att tid frigörs för dataskyddsombudet, vilken kommer att läggas på att ytterligare stärka arbetet med informations- och utbildningsinsatser för stadens förvaltningar och bolag.

2 Kontrollarbetet 2023–2024

Dataskyddsombudets uppgift att övervaka den personuppgiftsansvariges efterlevnad av dataskyddslagstiftningen görs i Göteborgs stad genom ett antal kontroller. Dessa kontroller specificeras genom denna kontrollplan, som syftar till att informera personuppgiftsansvariga om upplägg och tidplan för kontrollarbetet åren 2023 och 2024. Enligt GDPR ska dataskyddsombudet arbeta utifrån en riskbaserad metod. Riskbedömningen utgår från riskerna för de registrerades fri- och rättigheter. Kontrollplanen utgår från dataskyddsombudets bedömning avseende risker kopplat till personuppgiftsbehandlingar i verksamheten.

Syftet med att arbeta utefter en på förhand fastställd kontrollplan är att det ska bidra till att sätta fokus på verksamhetens dataskyddsarbete och därmed:

1. Säkerställa ett kontinuerligt dataskyddsarbete som skapar förutsättningar för efterlevnad av förordningen.
2. Uppmuntra ett riskbaserat arbetssätt och därigenom minimera risken för lagbrott.
3. Göra dataskyddsarbetet till en integrerad del i verksamhetens informationssäkerhetsarbete.

2.1 Kontrollarbetets delar

Kontrollarbetet består av tre delar som tillsammans syftar till att ge, såväl dataskyddsombud som personuppgiftsansvariga, en överblick över verksamhetens dataskyddsarbete och dess följsamhet gentemot GDPR.

Del	Beskrivning	Frekvens
Fasta kontrollpunkter	En övergripande kontroll av verksamhetens dataskyddsarbete. Verksamheten skattar det interna arbetet i en enkät uppdelad i tolv fasta kontrollpunkter.	Vartannat år fr.o.m. 2023
Fördjupad kontroll	En fördjupad kontroll av en eller flera utvalda verksamhetsspecifika kontrollpunkter.	Vartannat år fr.o.m. 2024
Uppföljning	Uppföljning och bedömning av hur verksamheten omhändertagit lämnande rekommendationer.	Årligen

2.2 Tidplan för kontrollarbetet 2023–2024

I tabellerna nedan anges huvuddragen i kontrollarbetet för åren 2023–2024 för stadens förvaltningar och bolag.

2023	Aktivitet
Januari - april	Årsrapport 2022 presenteras för nämnd/styrelse.
Januari - februari	Kontrollplan för 2023–2024 lämnas till nämnd/bolag.
September	Utskick av enkät för fasta kontrollpunkter.
November - december	Genomgång av innehåll i årsrapport med förvaltning/bolag.
December	Fastställd årsrapport översänds till förvaltning/bolag.

2024	Aktivitet
Januari - april	Årsrapport 2023 presenteras för nämnd/styrelse.
Januari - februari	Kontrollplan för 2024–2025 lämnas till nämnd/bolag.
Augusti - november	Fördjupad kontroll.
November - december	Genomgång av innehåll i årsrapport med förvaltning/bolag.
December	Fastställd årsrapport översänds till förvaltning/bolag.

3 Kontroller

3.1 Fasta kontrollpunkter

De fasta kontrollpunkterna utgår från principerna om inbyggt dataskydd och dataskydd som standard (enligt artikel 25 i GDPR). Verksamhetens följsamhet mot förordningen beror till stor del på hur väl dessa principer har integrerats i ordinarie arbetsprocesser. Att principerna har en central roll i arbetet med dataskydd blir särskilt tydligt i beaktandesats (skäl) 78 i GDPR, som anger att ”skyddet av fysiska personers rättigheter och friheter i samband med behandling av personuppgifter förutsätter att lämpliga tekniska och organisatoriska åtgärder vidtas”, och därtill att den personuppgiftsansvarige, för att kunna visa att förordningen efterlevs, bör anta interna strategier och vidta åtgärder särskilt för att uppfylla principerna om inbyggt dataskydd och dataskydd som standard. Med principerna som utgångspunkt har tolv kontrollpunkter identifierats. Dessa är av både teknisk och organisatorisk karaktär och är gemensamma för alla verksamheter inom Göteborgs Stad.

De fasta kontrollpunkterna kontrolleras genom en enkät som framöver kommer att vara återkommande vartannat år. Enkäten utgår från de tolv kontrollpunkterna där varje punkt innehåller ett antal delfrågor i form av

påståenden och/eller skattningsfrågor. Det är verksamheten som ansvarar för att enkäten fylls i. För att uppskattningarna ska bli så korrekta som möjligt kan det krävas att olika personer från olika delar i verksamheten deltar i arbetet med att fylla i enkäten. Resultaten från enkäten ger en generell ögonblicksbild för respektive kontrollpunkt och kan användas som vägledning för verksamheten i sitt dataskyddsarbete. Syftet är att få till ett långsiktigt och systematiskt arbetssätt som även åskådliggör de förändringar som vidtas över tid.

För beskrivning av de fasta kontrollpunkterna, se bilaga 1.

Fasta kontrollpunkter
1. Dataskyddsorganisation
2. Personuppgiftsincidenter
3. Biträdesavtal och andra överenskommelser
4. Register över personuppgiftsbehandlingar
5. Övergripande styrning av dataskyddsarbetet
6. Utbildning
7. Informationsplikt
8. E-post och dokumenthantering
9. Konsekvensbedömning/samråd
10. IT-projekt och upphandling
11. IT-system och digitala verktyg
12. Hantering av registrerades rättigheter

3.2 Fördjupad kontroll

Den fördjupade kontrollen ska utgå från verksamhetens specifika risker och kommer framöver att genomföras vartannat år. Dataskyddsombudet kommer att fastställa fokusområde för den fördjupade kontrollen i dialog med verksamheten.

Information om fokusområde för 2024 kommer att tillhandahållas nämnd/bolag i kontrollplanen för 2024–2025.

3.3 Uppföljning av genomförda kontroller

Uppföljning av genomförda kontroller görs årligen för att se hur verksamheten har hanterat tidigare lämnade rekommendationer och utvecklat sitt dataskyddsarbete inom varje kontrollpunkt.

4 Rapportering

4.1 Årsrapport

Det är nämnd/bolag som har det yttersta ansvaret för att verksamheten följer dataskyddslagstiftningen och dataskyddsombudet ska enligt lag rapportera om detta till högsta förvaltningsnivå. Därför sammanställer dataskyddsombudet årligen en rapport om verksamhetens dataskyddsarbete. I rapporten redogörs för eventuella risker och brister som dataskyddsombudet har identifierat. I rapporten redogörs också för de råd och rekommendationer som dataskyddsombudet har lämnat. För att möjliggöra en direkt kommunikation mellan dataskyddsombud och personuppgiftsansvarig presenteras årsrapporten för nämnd/styrelse vid sammanträde/möte.

4.2 Särskilt yttrande

Dataskyddsombudet kan i vissa situationer komma att rikta ett särskilt yttrande till högsta ansvarsnivå. En sådan situation kan vara om dataskyddsombudet har identifierat höga risker för de registrerade som kräver omgående åtgärder från ansvarig nämnd/bolag. Det kan också vara om dataskyddsombudet uppmärksammar att det inom verksamheten fattats beslut som är oförenliga med dataskyddslagstiftningen och dataskyddsombudets råd.

5 Kontakt

Eventuella frågor och synpunkter hänvisas i första hand till verksamhetens huvudansvariga kontaktperson inom dataskyddsenheten.

Frågor kan också alltid ställas till dso@intraservice.goteborg.se.

Bilaga 1 - Beskrivning av fasta kontrollpunkter

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.

Kontrollpunkt 2: Personuppgiftsincidenter

Kontrollpunkten avser verksamhetens förutsättningar för att identifiera och hantera personuppgiftincidenter. För att uppfylla ansvarsskyldigheten bör verksamhetens rutin för hanteringen vara dokumenterad. I de fall verksamheten är både personuppgiftsansvarig och personuppgiftsbiträde bör rutinen omfatta båda scenarier. I kontrollpunkten ingår även översyn av verksamhetens rutin för att bedöma incidenter, hantering av eventuell anmälan till tillsynsmyndigheten, samt hur rutinerna tillgängliggörs och kommuniceras inom verksamheten. Även efterlevnad av verksamhetens dokumentationsskyldighet, att alla inträffade personuppgiftsincidenter registreras, innefattas.

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.

Kontrollpunkt 4: Register över personuppgiftsbehandlingar

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 register innefattas.

Kontrollpunkt 5: Övergripande styrning av dataskyddsarbetet

Kontrollpunkten avser verksamhetens övergripande styrning för att arbeta med dataskydd. Tydlig styrning sätter ramarna för arbetet med dataskydd och främjar ett riskbaserat arbetssätt. Kontrollpunkten innefattar även verksamhetens arbete för att integrera dataskyddsfrågorna i det övriga informationssäkerhetsarbetet, samt hur verksamheten arbetar med egna interna kontroller för att säkerställa att dataskyddslagstiftningen efterlevs.

Kontrollpunkt 6: Utbildning

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

Kontrollpunkt 7: Informationsplikt

Kontrollpunkten avser hur väl verksamheten uppfyller principen om öppenhet och kravet på att lämna information till de registrerade om hur deras person-uppgifter behandlas. Punkten omfattar även hur verksamheten säkerställer att informationen är uppdaterad.

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

Kontrollpunkt 9: Konsekvensbedömning/samråd

Kontrollpunkten avser verksamhetens förutsättningar för att kunna identifiera när en konsekvensbedömning ska göras samt genomföra denna. Även verksamhetens rutiner för arbetet med konsekvensbedömningar samt hur dataskyddsombudet involveras i arbetet ingår. Därtill tillkommer verksamhetens rutin för att hantera de risker som identifieras i konsekvensbedömningen, samt hur genomförda konsekvensbedömningar följs upp och hålls aktuella.

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.

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

Kontrollpunkt 12: Hantering av registrerades rättigheter

Kontrollpunkten avser verksamhetens förutsättningar för att hantera de registrerades rättigheter. En förutsättning för att verksamheten ska kunna hantera de registrerades rättigheter är att man har en process och rutiner för arbetet, så att den registrerades personuppgifter enkelt kan lokaliseras vid efterfrågan. Även verksamhetens rutin för att hantera ett tillbakadragande av samtycke ingår i kontrollpunkten.