Göteborgs Stad

Årsrapport för dataskyddsarbetet 2023

Grundskolenämnden

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.

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.	

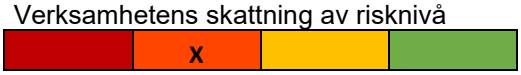
3.2 Resultat från kontrollen 2023

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 omfattande risker som kräver omgående åtgärder. Dataskyddsombudet delar verksamhetens bedömning om att det förekommer risker som är omfattande och kräver omgående åtgärder.

Dataskyddsombudet rekommenderade förvaltningen i årsrapport för 2022 att prioritera frågan. Frågan har även varit föremål för fördjupad granskning under 2021. Årets kontroll samt uppföljning visar att förvaltningen vidtagit vissa åtgärder, men då dessa ännu inte kunnat implementeras bedöms de höga risker som tidigare identifierats kopplat till bristerna i dataskyddsorganisationen kvarstå. Dataskyddsombudet bedömer det allvarligt att ledningen inte prioriterat arbetet med frågan och att det fortfarande inte vidtagits några åtgärder som i praktiken minskar riskerna.

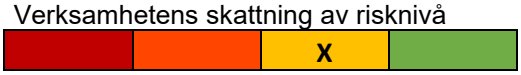
För att kunna bedriva ett systematiskt och effektivt dataskyddsarbete är en välfungerande dataskyddsorganisation en grundläggande förutsättning. En del i detta är att sträva efter att göra dataskydd till en integrerad och naturlig del av det dagliga arbetet och att det på samtliga nivåer inom förvaltningen 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.

Förvaltningen har under året arbetat med att ta fram en anvisning för att bland annat tydliggöra uppdraget för förvaltningens dataskyddsorganisation, vilket dataskyddsombudet ser som positivt. Förvaltningen anger även att en ny delegationsordning kommer att finnas på plats vid årsskiftet. Trots att en ny anvisning och en ny delegationsordning kommer att gälla från och med årsskiftet ser dataskyddsombudet risker med att det kan ta tid innan det nya arbetssättet är på plats. Förvaltningen har även angett att det under kommande år kommer att ske en omorganisation inom förvaltningen. Det är därför viktigt att förvaltningen under kommande år säkerställer att det nya arbetssättet efterlevs. Dataskyddsombudet rekommenderar även att förvaltningen kompletterar anvisningen för dataskyddsorganisationen med de rutiner som krävs för att den i praktiken ska kunna efterlevas samt kontinuerligt utvärderar hur arbetssättet i praktiken fungerar.

Utifrån de höga risker som en icke fungerande dataskyddsorganisation medför rekommenderar dataskyddsombudet att arbetet med att säkerställa en fungerande dataskyddsorganisation prioriteras 2024.

3.2.2 Kontrollpunkt 2: Personuppgiftsincidenter

Verksamhetens skattning av risknivå



Dataskyddsombudets bedömning

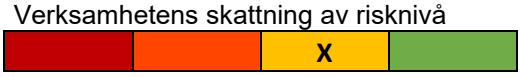
Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger risker som behöver åtgärdas, men att dessa inte är brådskande, omfattande eller allvarliga. Dataskyddsombudet delar till viss del verksamhetens bedömning, men gör till skillnad ifrån verksamheten bedömningen att det inom kontrollpunkten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

Förvaltningen har skattat sig lägre på en fråga inom kontrollpunkten, gällande om förvaltningen har dokumenterade arbetssätt för hur och när den registrerade ska informeras i samband med en personuppgiftsincident. Dataskyddsombudet har läst igenom den rutin som finns tillgänglig på förvaltningens intranät. Avsnittet gällande information är väldigt kortfattat och det framgår inte hur förvaltningen gör sin bedömning. Det framgår inte heller hur information ska lämnas. Dataskyddsombudet rekommenderar därför förvaltningen att komplettera sin rutin med information för hur och när information ska lämnas till de registrerade.

Dataskyddsombudets rekommenderar även (i likhet med föregående år) att förvaltningen kompletterar sin rutin för personuppgiftsincidenter med instruktion/metod för hur en bedömning av risken för de registrerades fri- och rättigheter kan göras. Dataskyddsenheten tillhandahåller en mall som förvaltningen kan använda sig av. Incidenthanteringen måste även göras mindre personberoende genom att tydliggöra och konkretisera rutinen så fler kan följa den. Förvaltningen behöver även se över behovet av rutin/plan för att regelbundet informera medarbetarna vad en personuppgiftsincident är och den interna incidenthanteringen.

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 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.

Förvaltningen har nästan genomgående skattat sig lågt inom kontrollpunkten och är på gränsen till att hamna inom en lägre risknivå. 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 personuppgiftsbiträdesavtalet. Förvaltningen har även angett att det saknas dokumenterade rutiner för att bedöma vem som är personuppgiftsansvarig och personuppgiftsbiträde samt rutiner för att teckna avtal som uppfyller kraven i GDPR innan tjänsten tas i drift. Det saknas även rutiner för att bedöma om andra överenskommelser/avtal behöver upprättas avseende gemensam eller annan delad hantering av personuppgifter. Förvaltningen har slutligen angett att det saknas rutiner för att kontrollera underbiträden.

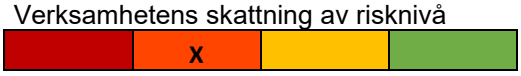
Förvaltningen har vid genomgången av årsrapporten angett att det framåt kommer tas fram en rutin för personuppgiftsbiträdesavtal. Förvaltningen har även angett att det finns rutiner inom förvaltningen för att gå igenom och kontrollera ingångna personuppgiftsbiträdesavtal.

Dataskyddsombudet rekommenderar förvaltningen att utifrån ovanstående säkerställa att kontroll av efterlevnad av personuppgiftsbiträdesavtal sker. Förvaltningen rekommenderas vidare att höja kompentensen när det kommer till bedömningen av personuppgiftsansvar och säkerställa att en rutin tas fram för hur en bedömning ska gå till. Dataskyddsombudet rekommenderar slutligen förvaltningen att ta fram rutiner för att kontrollera underbiträden.

Dataskyddsombudet har även under året identifierat att personuppgiftsbiträdesavtal har ingåtts utan att frågan om personuppgiftsansvaret i alla delar hade utretts. Dataskyddsombudet har därutöver under året uppmärksammat ett personuppgiftsbiträdesavtal där det inte hade lämnats några instruktioner till personuppgiftsbiträdet och där dataskyddsorganisationen inte varit involverade. Dataskyddombudet ser detta som en omfattande brist i organisationen och rekommenderar förvaltningen att omgående vidta åtgärder och säkerställa att dataskyddsperspektivet är inkluderat i hela ledet.

3.2.4 Kontrollpunkt 4: Register över personuppgiftsbehandlingar

Verksamhetens skattning av risknivå



Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger omfattande risker som kräver omgående åtgärder. Dataskyddsombudet delar till stor del verksamhetens bedömning, men gör till skillnad från verksamheten bedömningen att vissa av de identifierade riskerna är så höga att de kräver omgående insatser ifrån ledningsnivå.

Förvaltningen har i sin skattning angett att ca 25% av förvaltningens behandlingar finns dokumenterade i behandlingsregistret. Förvaltningen även angett att registret i stora delar inte innehåller all den information som ska finnas enligt GDPR och att

det saknas rutiner för att hålla det uppdaterat. Vid genomgången av årsrapporten anger förvaltningen att det bedöms behöva vidtas åtgärder på ledningsnivå då det inom förvaltningens olika delar saknas resurser för arbetet. Det anges vidare att förvaltningen även behöver hitta arbetssätt för att nå ut till verksamheterna för att kunna kartlägga förvaltningens behandlingar.

Förvaltningen skattade även föregående år att behandlingsregistret endast innehöll 25% av förvaltningens behandlingar. Skattningen var densamma även under 2021. Dataskyddsombudets tidigare rekommendationer har varit att prioritera arbetet. Av förvaltningens skattning i år kan det konstateras att detta inte har gjorts eller att vidtagna åtgärder inte har haft avsedd effekt. Det föreligger en skyldighet enligt GDPR att upprätta ett behandlingsregister, där samtliga av förvaltningens behandlingar ska ingå. Det är även en förutsättning att ett behandlingsregister finns på plats för att kunna bedriva ett systematiskt och riskbaserat dataskyddsarbete. Avsaknad av ett behandlingsregister innebär även stora risker för de registrerade. Med tanke på grundskoleförvaltningens uppdrag, omfattning och att man hanterar personuppgifter gällande barn är detta extra allvarligt. Dataskyddsombudet delar därför förvaltningens bedömning om att resurser behöver avsättas för att framöver kunna arbeta med behandlingsregistret, då det är ett omfattande arbete. Dataskyddsombudet rekommenderar förvaltningen att omgående vidta åtgärder och prioritera arbetet med behandlingsregistret. Dataskyddsombudet ser även ett behov av att förvaltningsledningen tydliggör att det är en fråga som ska prioriteras. Dataskyddsombudet kommer under våren att avsätta tid för regelbundna avstämningar kopplat till frågan för att säkerställa att arbetet påbörjas och fortlöper.

3.2.5 Kontrollpunkt 5: Övergripande styrning av dataskyddsarbetet

Verksamhetens skattning av risknivå

	X		

Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger omfattande risker som kräver omgående åtgärder.

Dataskyddsombudet delar verksamhetens bedömning om att det förekommer risker som är omfattande och kräver omgående åtgärder.

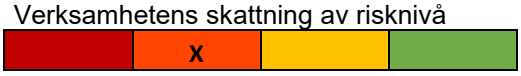
Vid genomgången av årsrapporten angav förvaltningen att det under året har tagits fram nya arbetssätt som kommer att implementeras under 2024. De nya arbetssätten innebär att förvaltningens direktör och ledning kommer att vara mer involverade i förvaltningens dataskyddsarbete. Dataskyddsombudet ser positivt på det nya arbetssättet och ser att förvaltningen vidtar åtgärder för att arbeta mer strategiskt med frågorna. Till dess att de nya arbetsformerna har implementerats ser dock dataskyddsombudet att riskerna kvarstår och att uppföljning därför behöver göras efter 2024 för att säkerställa att de vidtagna åtgärderna har fått önskad effekt.

Förvaltningens skattning inom kontrollpunkten är genomgående av lägre karaktär, vilket indikerar på att det finns omfattande insatser och förändringar som behöver göras. Förvaltningen har bland annat angett att det saknas en övergripande strategi för arbetet med dataskydd. Dataskyddsombudet delar förvaltningens bedömning och ser stora risker kopplat till detta. 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. Det ska även tilläggas att förvaltningen är stor, varför ett decentraliserat ansvar är ett måste för att kunna arbeta effektivt med frågorna. Eftersom förvaltningen inte heller har ett komplett behandlingsregister begränsas ett riskbaserat arbetssätt, vilket innebär att förvaltningen inte har kännedom om vilka behandlingar som innebär höga risker. Detta är särskilt alarmerande eftersom förvaltningen hanterar personuppgifter gällande barn.

Dataskyddsombudet upplever även att det ofta kommer frågor till dataskyddsombudet från medarbetare inom förvaltningen där den interna dataskyddsorganisationen inte har blivit involverade. Detta visar på att det inte finns någon tydlig styrning över hur dataskyddsfrågor ska hanteras i verksamheten eller information om var medarbetare ska vända sig. Dataskyddsombudet rekommenderar därför förvaltningen att genomföra de insatser som krävs för att få en tydlig dataskyddsorganisation på plats och en organisation som ska arbeta riskbaserat med dataskyddsfrågorna.

3.2.6 Kontrollpunkt 6: Utbildning

Verksamhetens skattning av risknivå



Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger omfattande risker som kräver omgående åtgärder. Dataskyddsombudet delar verksamhetens bedömning om att det förekommer risker som är omfattande och kräver åtgärder.

Förvaltningen har nästan genomgående skattat sig lågt inom kontrollpunkten. Resultatet är även en försämring jämfört med föregående år. Förvaltningen har angett att det saknas kunskap inom förvaltningen för att kunna bedriva ett fullgott dataskyddsarbete. Förvaltningen har även angett att det inte finns möjlighet att regelbundet delta i utbildningar inom dataskydd och att verksamheten inte har dokumenterande arbetssätt för att följa upp och bibehålla kunskap hos medarbetare efter genomförda utbildningar. Förvaltningen har inte heller kartlagt vilken kunskapsnivå av dataskydd som olika befattningar kräver och kan därmed inte planera utbildningar och informationsinsatser utifrån behov. Förvaltningen har dock angett att det inom verksamheten regelbundet genomförs informationsinsatser för att utbilda och informera medarbetarna inom dataskydd. Förvaltningen har även angett att man bland annat har riktat utbildningsinsatser inom elevhälsan eftersom

det där förekommer stora risker. Även systemförvaltare har getts information i samband med arbetet med konsekvensbedömningar.

Eftersom förvaltningen har angett att det genomförs utbildningar och informationsinsatser inom förvaltningen, men att kunskapsnivån likväl är låg rekommenderar dataskyddsombudet förvaltningen att kartlägga kunskapsbehovet av dataskydd. I och med förvaltningens storlek behöver förvaltningen arbeta strategiskt med frågan för att nå ut till samtliga verksamhetsgrenar, inklusive skolorna. Det är även viktigt att utbildningarna riktar sig till de medarbetare som har störst behov av detta, till exempel som förvaltningen har identifierat inom elevhälsan. Förvaltningen rekommenderas även att se över hur kunskap i nuläget sprids inom förvaltningen för att kunna vidta åtgärder och effektivisera förfarandet.

3.2.7 Kontrollpunkt 7: Informationsplikt

Verksamhetens skattning av risknivå

Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger omfattande risker som kräver omgående åtgärder. Dataskyddsombudet delar verksamhetens bedömning om att det förekommer risker som är omfattande och kräver omgående åtgärder.

Förvaltningen har skattat varierande värden inom kontrollpunkten. Verksamheten har skattat högre värden på frågorna om verksamhetens integritetspolicy uppfyller kraven enligt GDPR samt att informationen till de registrerade är tydlig och lättillgänglig.

Verksamheten angett lägre värden på frågorna om det finns dokumenterade arbetssätt att informera medarbetarna om hur deras personuppgifter behandlas och om verksamheten kontinuerligt ser över och uppdaterar integritetsinformationen. På frågan om de registrerade enkelt kan nå verksamhetens integritetsinformation från samtliga av verksamhetens digitala kanaler har förvaltningen svarat att de inte vet/inte kan besvara frågan. Vid genomgången av årsrapporten angav förvaltningen att man framåt ska ta kontakt med den interna kommunikationsavdelningen för att få bättre överblick samt identifiera de kanaler som används.

Dataskyddsombudet finner att förvaltningens integritetspolicy som återfinns på goteborg.se inte uppfyller de krav som ställs enligt artikel 13 och 14 GDPR. Integritetspolicyn saknar helt information om vilka personuppgiftsbehandlingar som förvaltningen utför. Detta är speciellt problematiskt eftersom förvaltningen ofta i sina konsekvensbedömningar hänvisar till sin integritetspolicy som ett sätt att uppfylla informationsplikten. Dataskyddsombudet rekommenderar därför förvaltningen att kartlägga vilka behandlingar som ska omfattas av integritetspolicyn och komplettera med dessa. Avseende övriga behandlingar måste förvaltningen säkerställa att informationsplikten uppfylls på annat vis.

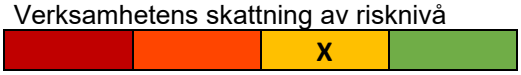
Förvaltningen måste även säkerställa att förvaltningens medarbetare får information om hur deras personuppgifter behandlas.

Dataskyddsombudet rekommenderar även förvaltningen att kartlägga vilka digitala kanaler som förvaltningen använder sig av och säkerställa att förvaltningen uppfyller informationsplikten även i denna del.

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 stora risker inom detta område. Dataskyddsombudet bedömer därför 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 stor del verksamhetens bedömning, men gör till skillnad ifrån verksamheten bedömningen att det inom kontrollpunkten förekommer risker som kräver åtgärder.

Förvaltningen har inom kontrollpunkten skattat varierade värden. Kopplat till frågorna gällande informationsklassificering har förvaltningen angett att ca 25 % av förvaltningens personuppgiftsbehandlingar har informationsklassificerats utifrån Göteborgs stads riktlinje för informationssäkerhet. Förvaltningen har vidare angett att av dessa är ca 50 % av informationen aktuell. Slutligen har förvaltningen i sin skattning angett att det saknas dokumenterade arbetssätt för hur olika informationssäkerhetsklasser ska hanteras och vilka lagringsytor som får användas. Vid genomgången av årsrapporten angavs att detta inte stämde, utan att det fanns framtaget. Dataskyddsombudet har gått igenom de dokument som hänvisats till och då dessa är generella för Göteborgs Stad och inte anpassade utifrån grundskoleförvaltningens verksamhet ser dataskyddsombudet att det kvarstår ett behov av att ta fram förvaltningsspecifika arbetssätt.

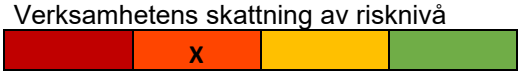
Förvaltningen har även inom kontrollpunkten angett lägre värden på frågorna kopplat till e-posthantering. Förvaltningen har angett att det saknas dokumenterade arbetssätt för hanteringen av personuppgifter i e-post och det saknas enligt förvaltningens skattning även hänvisning till förvaltningens integritetpolicy i samband med direkt kontakt via till exempel e-post.

Utifrån de risker som en oreglerad informationshantering innebär rekommenderas förvaltningen att ta fram dokumenterade arbetssätt/anvisningar för hur information

i olika informationsklasser ska hanteras och vilka lagringsytor som får användas samt rutiner för hur personuppgifter får hanteras i e-post.

3.2.9 Kontrollpunkt 9: Konsekvensbedömning/samråd

Verksamhetens skattning av risknivå



Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger omfattande risker som kräver omgående åtgärder. Förvaltningens skattning är nästan uteslutande låg inom ramen för kontrollpunkten. Jämfört med föregående år indikerar resultatet på en tydlig försämring.

Dataskyddsombudet delar verksamhetens bedömning om att det förekommer risker som är omfattande och kräver omgående åtgärder.

Förvaltningen har angett att det finns framtagna konsekvensbedömningar för ca 25 % av de behandlingar som innebär höga risker för de registrerade eller där det enligt IMY:s riktlinjer krävs. Av de konsekvensbedömningar som inte har gjorts har förvaltningen dokumenterad planering för ca 25 % av dessa. 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 att förvaltningen parallellt med arbetet med personuppgiftsregistret, kontrollerar samtliga av verksamhetens behandlingar utifrån höga risker. Förvaltningen riskerar annars att konsekvensbedömningar inte genomförs för behandlingar där det ska göras. Föregående år rekommenderades förvaltningen 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.

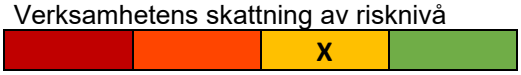
Förvaltningens skattning inom kontrollpunkten tyder på att det saknas rutiner för både riskbedömningar och konsekvensbedömningar, där det inte finns något arbetssätt för att bland annat vidta åtgärder efter lämnade rekommendationer eller att inhämta synpunkter från de registrerade. Dataskyddsombudet rekommenderar därför förvaltningen att i stort se över frågorna inom kontrollpunkten och vidta åtgärder då nuvarande arbetssätt innebär stora risker för de registrerade.

Dataskyddsombudet vill även uppmärksamma förvaltningen på att IMY nyligen avslutade sin granskning av Östersunds kommuns användning av Google Workspace for Education. IMY utdömde i beslutet en sanktionsavgift för att en konsekvensbedömning inte hade gjorts innan dess att man påbörjat behandlingen. Dataskyddsombudet vill påtala att situationen är densamma inom förvaltningen. Förvaltningen använder sig av Google Workspace for Education och har i nuläget ingen färdigställd konsekvensbedömning. Dataskyddsombudet har fått information

om att arbetet har påbörjats. Dataskyddsombudet vill dock poängtera att avsaknaden av en konsekvensbedömning kan vid en granskning innebära en sanktionsavgift för förvaltningen.

3.2.10 Kontrollpunkt 10: IT-projekt och upphandling

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

Utifrån verksamhetens egen skattning bedömer dataskyddsombudet dock att det föreligger risker kopplat till kontrollpunkten.

För att kunna bedriva ett effektivt dataskyddsarbete krävs att dataskyddsperspektivet finns med frågan början. Förvaltningen har angett lägre värden kopplat till om dataskyddsperspektivet är en del vid initierande av nya digitala lösningar samt vid kravställning kopplat till upphandling av nya system. På frågan om det finns dokumenterande arbetssätt för att involvera dataskyddsombudet vid upphandling skattar förvaltningen även ett lägre värde.

Utifrån skattningen kvarstår de rekommendationer som lämnades 2022, vilket innebär att förvaltningen rekommenderas säkerställa 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.

3.2.11 Kontrollpunkt 11: IT-system och digitala verktyg

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

Utifrån skattningen kan det utläsas att det föreligger risker inom kontrollpunkten. Förvaltningen har bland annat skattat lägre värden på frågorna om verksamheten regelbundet följer upp medarbetares behörigheter och åtkomster i IT-system för att

kontrollera att medarbetarens tillgång är nödvändig och om förvaltningen följer upp och kontrollerar att användningen av system och/eller andra digitala verktyg följer antagna styrande dokument. Dataskyddsombudet rekommenderar förvaltningen utifrån ovanstående att ta fram rutiner för uppföljning av behörigheter samt kontroller av system och andra digitala verktyg för att säkerställa efterlevnad av GDPR och andra styrande dokument inom staden.

Förvaltningen har även skattat ett lägre värde gällande huruvida förvaltningens användning av cookies på webbsidor följer kraven enligt GDPR. Förvaltningen rekommenderas därför att säkerställa användningen av cookies på de hemsidor som förvaltningen ansvarar för. 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.

Även vid årets genomgång av förvaltningens kommunikationskanaler noterar dataskyddsombudet att verksamheten 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. Dataskyddsombudet 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.

3.2.12 Kontrollpunkt 12: Hantering av registrerades rättigheter

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.

Dataskyddsombudet ser (liksom föregående år) behov av att lyfta 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 fortfarande 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. För att den registrerade därmed ska kunna utöva sina rättigheter i enlighet med förordningen rekommenderas förvaltningen att arbeta med sitt behandlingsregister.

Förvaltningen har liksom föregående år angett en lägre skattning på frågan om verksamheten har dokumenterade arbetssätt för att hantera ett tillbakadragande av samtycke från en registrerad. Dataskyddsombudet rekommenderar därför i likhet med föregående år att det behöver finnas rutiner för hur återkallande av samtycke ska hanteras för de behandlingar där samtycke används.

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): Kontroll av användningen av samtycke som rättslig grund

Verksamheten gavs följande 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

Kommentarer och rekommendationer:

Uppföljningen visar att verksamheten inte aktivt har arbetat med frågan sedan årsrapporten 2022. Förvaltningen har dock tagit fram en grundmall för samtycke i de fall samtycke som rättslig grund kan komma ifråga samt tillsett att den nya rutinen för hantering av ljud, film och bild i läroplattformen Vklass adresserar frågan om samtycke då det tidigare rådde missförstånd kring frågan på just detta område. Dataskyddsombudet ser därför att ytterligare uppföljning är nödvändigt och rekommenderar förvaltningen att i stort arbeta med rekommendationerna som lämnades under 2022. Uppföljning kommer att ske igen under 2024.

Kontroll (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

Kommentarer och rekommendationer:

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

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 1: Dataskyddsorganisation

Säkerställ att det nya arbetssättet efterlevs, komplettera anvisningen med de rutiner som krävs för att anvisningen i praktiken ska kunna efterlevas samt utvärdera hur arbetssättet i praktiken fungerar. Fokus bör vara på att under året skapa en ändamålsenlig och välfungerande dataskyddsorganisation inom förvaltningen.

- Kontrollpunkt 4: Register över personuppgiftsbehandlingar

Gör en översyn av befintligt register. Gå igenom hur de dokumenterade behandlingarna är definierade och för respektive behandling kontrollera att informationen uppfyller kraven enligt artikel 30 i GDPR.

En förutsättning för att arbetet ska kunna genomföras på ett kvalitativt sätt är att förvaltningen tillsätter tillräckliga resurser för arbetet.

- Kontrollpunkt 9: Konsekvensbedömningar/samråd

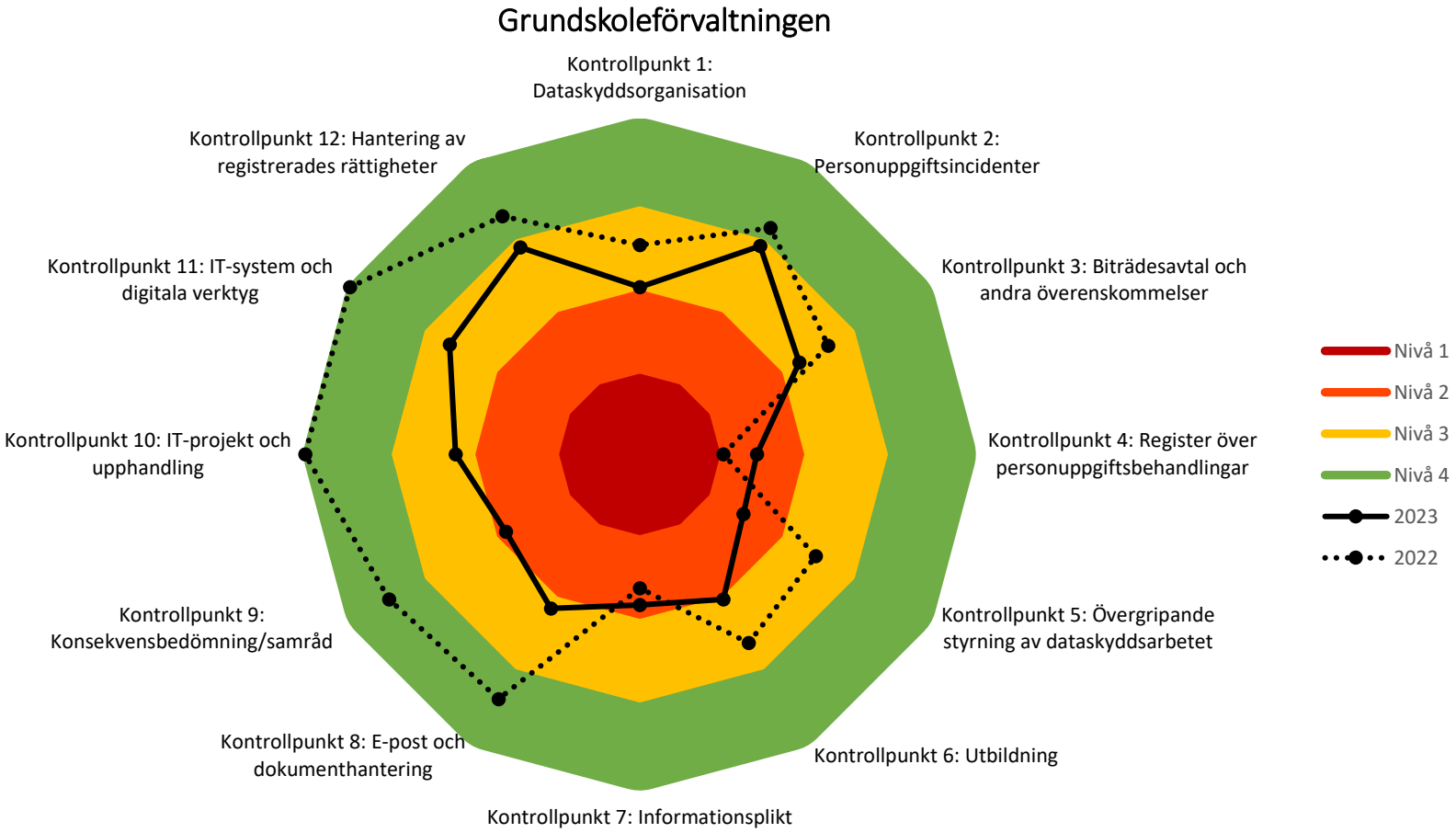
Arbeta parallellt med översynen av behandlingsregistret med att identifiera behandlingar utifrån höga risker och ta fram en handlingsplan för genomförandet av konsekvensbedömningar för dessa behandlingar.

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

Grundskoleförvaltningen

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 personuppgifter 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.