Göteborgs Stad

Årsrapport för dataskyddsarbetet 2023

Stadsbyggnadsnämnden

2023-12-19

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

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

Dataskyddsombudet delar förvaltningens bedömning och anser att verksamheten har ett systematiskt arbete inom kontrollpunkten och inga risker av betydelse föreligger. Även inom verksamheter med låga risker krävs det kontinuerliga insatser för att ett systematiskt dataskyddsarbete ska kunna upprätthållas och stärkas ytterligare.

Förbättringsåtgärder som dataskyddsombudet identifierat och som skulle kunna vidtas inom ramen för kontrollpunkten gäller bland annat att tillse att dataskyddsorganisationen har tillräckligt med resurser för att ha tid för att bedriva ett fullgott dataskyddsarbete. Dataskyddsombudets bedömning är att de kompetensmässiga och organisatoriska förutsättningarna finns, men att tiden för att arbeta med frågorna ibland inte är tillräcklig och att personberoendet är stort.

Dataskyddsombudet rekommenderar stadsbyggnadsförvaltningen att:

- Tillse en adekvat resursfördelning så att det tidsmässiga utrymmet finns inom organisationen för att arbeta fullt ut med dataskyddsfrågorna.

3.2.2 Kontrollpunkt 2: Personuppgiftsincidenter

Verksamhetens skattning av risknivå

Dataskyddsombudets bedömning

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

Dataskyddsombudet delar förvaltningens bedömning och anser att verksamheten har ett systematiskt arbete inom kontrollpunkten och inga risker av betydelse föreligger, men vill i sammanhanget påminna om att även inom verksamheter med låga risker krävs det kontinuerliga insatser för att ett systematiskt dataskyddsarbete ska kunna upprätthållas och stärkas ytterligare.

3.2.3 Kontrollpunkt 3: Biträdesavtal och andra överenskommelser

Verksamhetens skattning av risknivå

Dataskyddsombudets bedömning

Förvaltningens resultat indikerar att verksamheten bedriver ett systematiskt dataskyddsarbete inom ramen för kontrollpunkten och att inga risker av betydelse föreligger. Dataskyddsombudet delar bedömningen och anser att verksamheten har ett systematiskt arbete inom kontrollpunkten och inga risker av betydelse föreligger.

Verksamhetens svar indikerar att det finns förbättringspotential avseende förmågan att bedöma och reglera frågan om gemensamt personuppgiftsansvar, vilket skulle kunna vara ett förbättringsområde för förvaltningen att titta närmare på.

Dataskyddsombudet rekommenderar därför att förvaltningen:

- Tar fram arbetssätt för att bedöma om det föreligger ett gemensamt personuppgiftsansvar vid anlitande av leverantör/inledande av samarbeten, gärna i samarbete med övriga NOS-förvaltningar.

3.2.4 Kontrollpunkt 4: Register över personuppgiftsbehandlingar

Verksamhetens skattning av risknivå

Dataskyddsombudets bedömning

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

Dataskyddsombudet delar bedömningen och anser att verksamheten har ett systematiskt arbete inom kontrollpunkten och inga risker av betydelse föreligger. Men vill framhålla vikten av kontinuerliga insatser för att ett systematiskt dataskyddsarbete ska kunna upprätthållas och stärkas ytterligare och att det är viktigt att förvaltningen kontinuerlig arbetar med att hålla sitt behandlingsregister uppdaterat och aktuellt för att bibehålla den höga nivån inom kontrollpunkten.

3.2.5 Kontrollpunkt 5: Övergripande styrning av dataskyddsarbetet

Verksamhetens skattning av risknivå

Dataskyddsombudets bedömning

Förvaltningens resultat indikerar att verksamheten bedriver ett systematiskt dataskyddsarbete inom ramen för kontrollpunkten och att inga risker av betydelse föreligger. Dataskyddsombudet delar bedömningen och anser att verksamheten har ett systematiskt arbete inom kontrollpunkten och inga risker av betydelse föreligger.

Dataskyddsombudets sammanfattande bedömning är att verksamheten har en god övergripande styrning, men precis som för kontrollpunkt 1 är det viktigt att de som arbetar med frågorna inom organisationen har tillräckliga resurser för att kunna utföra det arbete som krävs.

3.2.6 Kontrollpunkt 6: Utbildning

Verksamhetens skattning av risknivå

Dataskyddsombudets bedömning

Förvaltningens resultat indikerar att verksamheten bedriver ett systematiskt dataskyddsarbete inom ramen för kontrollpunkten och att inga risker av betydelse föreligger. Dataskyddsombudet delar bedömningen och anser att verksamheten har ett systematiskt arbete inom kontrollpunkten och inga risker av betydelse föreligger.

Stadsbyggnadsförvaltningen arbetar kontinuerligt med utbildningar, vilket är mycket positivt, samtidigt har förvaltningen identifierat ett behov av att hitta dokumenterade arbetssätt för att arbeta med uppföljning av kunskapsnivån hos medarbetarna.

Dataskyddsombudets rekommendation till förvaltningen är därför att:

- Hitta en modell för att arbeta med uppföljning av utbildningsinsatser.

3.2.7 Kontrollpunkt 7: Informationsplikt

Verksamhetens skattning av risknivå

Dataskyddsombudets bedömning

Förvaltningens resultat indikerar att verksamheten bedriver ett systematiskt dataskyddsarbete inom ramen för kontrollpunkten och att inga risker av betydelse föreligger. Dataskyddsombudet delar inte förvaltningens bedömning, och gör till skillnad ifrån verksamheten bedömningen att det förekommer risker som är omfattande och kräver omgående åtgärder.

Dataskyddsenheten höll under våren 2023 en särskild informationsinsats rörande informationsplikten enligt GDPR. Dataskyddsombudets bedömning är rent generellt att det finn stora brister i den information som lämnas till de registrerade, detta gäller inte enbart för stadsbyggnadsförvaltningen utan är en genomgående brist hos i princip samtliga verksamheter i Göteborgs Stad.

Efter att ha tittat närmare på den information som lämnas i anslutning till förvaltningens e-tjänster, till exempel rörande ansökan om bygglov eller andra åtgärder, är dataskyddsombudets bedömning att den information som lämnas inte uppfyller kraven i artikel 12-14 i GDPR. Bristerna består både i vilken information som lämnas och hur den lämnas. Bristerna är allvarliga. Dataskyddsombudet är medveten om att frågan spänner över flera förvaltningar i Göteborgs Stad då stadsbyggnadsförvaltningen inte helt har rådighet över utformningen av e-tjänsterna på goteborg.se. Inte desto mindre har förvaltningen ett ansvar som personuppgiftsansvarig att upprätthålla sin informationsplikt gentemot de registrerade.

Förvaltningen rekommenderas därför att:

- Se över samtliga delar i den information som lämnas till de registrerade och de arbetssätt som tillämpas för att säkerställa att informationsplikten gentemot de registrerade uppfylls, särskilt avseende den information som lämnas i anslutning till de e-tjänster som kommuninvånare kan nyttja via goteborg.se.

- Om så är nödvändigt, lyfta frågan om utformningen av den information som lämnas i anslutning till e-tjänsterna på goteborg.se till central nivå i Göteborgs Stad.

3.2.8 Kontrollpunkt 8: E-post och dokumenthantering

Verksamhetens skattning av risknivå

Dataskyddsombudets bedömning

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

Dataskyddsombudet delar verksamhetens bedömning och anser att förvaltningen har ett systematiskt arbete inom kontrollpunkten och inga risker av betydelse föreligger. Även inom verksamheter med låga risker krävs det kontinuerliga insatser för att ett systematiskt dataskyddsarbete ska kunna upprätthållas och stärkas ytterligare.

3.2.9 Kontrollpunkt 9: Konsekvensbedömning/samråd

Verksamhetens skattning av risknivå

Dataskyddsombudets bedömning

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

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

Dataskyddsombudet anser att verksamheten har en god kompetens för att genomföra konsekvensbedömningar med hög kvalitet och att man har de dokumenterade arbetssätt på plats som krävs för att kunna bedriva ett fullgott arbete med konsekvensbedömningar.

Trots detta finns det områden där förvaltningen behöver genomföra åtgärder. Dataskyddsombudet vill här särskilt peka på bristen på resurser, i form av tid, för att genomföra bedömningar för samtliga högriskbehandlingar. Dataskyddsombudet bedömer att förvaltningen har en korrekt bild av vad som behöver göras framöver och hur det ska göras, men efter dialog med verksamheten framkommer att tidsbrist innebär att nödvändiga bedömningar inte blivit av. Dataskyddsombudet vill därför särskilt påminna om att för personuppgiftsbehandlingar där höga risker förekommer så är det ett krav enligt GDPR att en konsekvensbedömning ska genomföras innan behandlingen får påbörjas.

Förvaltningen rekommenderas därför att:

- Snarast genomföra konsekvensbedömningar för de personuppgiftsbehandlingar som innebär en hög risk för de registrerades fri- och rättigheter.

3.2.10 Kontrollpunkt 10: IT-projekt och upphandling

Verksamhetens skattning av risknivå

Dataskyddsombudets bedömning

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

Dataskyddsombudet delar bedömningen och anser att verksamheten har ett systematiskt arbete inom kontrollpunkten och inga risker av betydelse föreligger. Förvaltningen har arbetat aktivt med frågan, något som dataskyddsombudet ser mycket positivt på, och ligger långt framme. Dataskyddsombudet har inga särskilda rekommendationer att lämna avseende kontrollpunkten mer än den generella observationen att det även inom verksamheter med låga risker krävs kontinuerliga insatser för att ett systematiskt dataskyddsarbete ska kunna upprätthållas och stärkas ytterligare.

3.2.11 Kontrollpunkt 11: IT-system och digitala verktyg

Verksamhetens skattning av risknivå

Dataskyddsombudets bedömning

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

Dataskyddsombudet delar bedömningen och anser att verksamheten har ett systematiskt arbete inom kontrollpunkten och inga risker av betydelse föreligger. Förvaltningen har arbetat aktivt med frågan och ligger långt framme, något som dataskyddsombudet ser mycket positivt på. Dataskyddsombudet har inga särskilda rekommendationer att lämna avseende kontrollpunkten mer än den generella observationen att det även inom verksamheter med låga risker krävs kontinuerliga insatser för att ett systematiskt dataskyddsarbete ska kunna upprätthållas och stärkas ytterligare.

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 bedömningen om att det finns risker som behöver åtgärdas, men gör precis som förvaltningen bedömningen att de inte är omfattande, brådskande eller allvarliga.

Förvaltningens svar på dataskyddsombudets kontrollfrågor indikerar dock att det finns mindre förbättringsområden där verksamheten behöver genomföra åtgärder.

Förvaltningen rekommenderas därför att:

- Verka för att sprida en medvetenhet inom organisationen för när de registrerades rättigheter begränsas, samt ta fram dokumenterade arbetssätt för hur dessa situationer ska hanteras.

- Ta fram dokumenterade arbetssätt för att bedöma om en invändning från en registrerad är uppenbart ogrundad eller orimlig.

3.3 Uppföljning

3.3.1 Uppföljning av rekommendationer lämnade inom ramen för tidigare genomförda kontroller

Stadsbyggnadsnämnden inrättades den förste januari 2023 som ett led i den nya organiseringen av de stadsutvecklande nämnderna. Eftersom nämnden utgör en ny förvaltningsmyndighet sker ingen uppföljning av tidigare utförda kontroller.

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 7: Informationsplikt
  Förvaltningen rekommenderas att se över samtliga delar i den information som lämnas till de registrerade och de arbetssätt som tillämpas för att säkerställa att informationsplikten gentemot de registrerade uppfylls, särskilt avseende den information som lämnas i anslutning till de e-tjänster som kommuninvånare kan nyttja via goteborg.se.

  Om så är nödvändigt, lyfta frågan om utformningen av den information som lämnas i anslutning till e-tjänsterna på goteborg.se till central nivå i Göteborgs Stad.

- Kontrollpunkt 9: Konsekvensbedömningar/samråd
  Förvaltningen rekommenderas att snarast genomföra konsekvensbedömningar för de personuppgiftsbehandlingar som innebär en hög risk för de registrerades fri- och rättigheter

5 Bilagor

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

Bilaga 2: Kontrollplan för dataskyddsarbetet 2023–2024