Göteborgs Stad

Årsrapport för dataskyddsarbetet 2023

Äldre samt vård och omsorgsnämnden

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.	

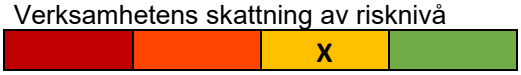
3.2 Resultat från kontrollen 2023

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

Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger risker som behöver åtgärdas, men att dessa inte är brådskande, omfattande eller allvarliga. I det arbetet som har gjorts inom förvaltningen under året, märks bland annat att antalet dataskyddskontakter har utökats och en ny medarbetare introducerats. Ett arbete har också genomförts för att förtydliga mandat, roller och ansvar. Bland annat har flera styrande dokument tagits fram och delegationsordningen har setts över. Tjänstepersoner har uppgett att de arbetar strategiskt med att göra dataskyddsorganisationen och dataskyddskontakternas roll känd inom förvaltningen. Eftersom äldre- samt vård och omsorgsförvaltningen är en stor organisation, innebär detta att arbetet med att sprida kunskap om dataskyddsorganisationen tar tid.

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. Områden där verksamheten behöver genomföra åtgärder är att fortsätta arbeta för att göra dataskydd till en naturlig och integrerad del i det dagliga arbetet i alla delar av verksamheten. Detta kan bland annat göras genom att kartlägga och uppdatera befintliga dokumenterade arbetssätt med relevant information om dataskydd. Det kan också göras genom att exempelvis utbilda fler medarbetare om reglerna kring personuppgiftsincidenter (jmf kontrollpunkt 2 och 6).

3.2.2 Kontrollpunkt 2: Personuppgiftsincidenter

Verksamhetens skattning av risknivå

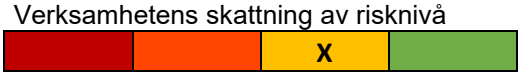
Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att verksamheten bedriver ett systematiskt dataskyddsarbete inom ramen för kontrollpunkten och att inga risker av betydelse föreligger. Föregående år gavs förvaltningen rekommendationer om att se över rutiner för att identifiera personuppgiftsincidenter, hur bedömningar görs för att eventuellt informera registrerade om en incident samt följa upp inträffade incidenter. I samtal med förvaltningens dataskyddskontakter framkommer att de har identifierat att alla personuppgiftsincidenter inte kommer till deras kännedom. Därför ska ett samarbete med de roller som hanterar avvikelser påbörjas inom kort. Det har identifierats att antalet personuppgiftsincidenter som kommer till dataskyddsorganisationens kännedom är få i förhållande till antalet avvikelser som hanteras av exempelvis rollerna socialt ansvarig samordnare och medicinskt ansvarig sjuksköterska.

Dataskyddsombudet delar till stor del verksamhetens bedömning. Dataskyddsombudet gör dock till skillnad från verksamheten bedömningen att det ändå föreligger risker inom kontrollpunkten, även om dessa inte bedöms som omfattande, brådskande eller allvarliga. Dataskyddsombudet konstaterar att det fortfarande finns behov av att dokumentera arbetssätt för när och hur information till de registrerade ska tillhandahållas. Vidare bedömer dataskyddsombudet att det mot bakgrund av att alla personuppgiftsincidenter inte kommer dataskyddsorganisationen till del, sannolikt förekommer att incidenter inte heller anmäls eller anmäls i tid till Integritetsskyddsmyndigheten. Dataskyddsombudet ser positivt på att personuppgiftsincidenter i vart fall dokumenteras och följs upp inom ramen för avvikelsehanteringen, men vill samtidigt påtala att kraven på dokumentation i vissa delar kan skilja sig åt. Dataskyddsombudet ser positivt på kommande initiativ att ta fram en utbildning för medarbetare om personuppgiftsincidenter (jmf kontrollpunkt 6).

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. Precis som föregående år har verksamheten skattat sig lågt vad gäller rutiner för kontinuerlig kontroll av efterlevnad hos personuppgiftsbiträden samt rutiner för att bedöma underbiträden. Tidigare har det funnits utmaningar i arbetet med att identifiera personuppgiftsansvar, så väl mellan förvaltningar inom staden som gentemot exempelvis Västra Götalandsregionen. Dels utifrån att staden från årsskiftet 2022/23 gick in i en ny styrmodell[2] där andra och fler förvaltningar än tidigare blivit tjänsteleverantörer. Men också utifrån att förvaltningen för äldre samt vård- och omsorg har flera samarbeten där rollerna inte är helt klarlagda (leverera mat till skolor bland annat). På fråga till dataskyddskontakt svarar de att det ännu inte har genomförts några utredningar av ansvarsförhållandena utifrån de förändringar som den nya styrmodellen innebär, utan att man fortsatt på samma sätt som tidigare. Exempelvis vad gäller att teckna personuppgiftsbiträdesavtal med socialförvaltning Nordost som efter årsskiftet 2022/23 tagit över viss förvaltning och utveckling av tjänster från förvaltningen för Intraservice.

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. Även om flera personuppgiftsbiträdesavtal har tecknats utifrån de nya förhållandena, är det dataskyddsombudets förståelse att det ännu inte gjorts någon kartläggning av ansvar och roller eller vilka

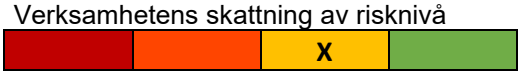
[2] Riktlinjen trädde i kraft den 1 januari 2023 Göteborgs Stads riktlinje för styrning, samordning och finansiering av digital utveckling och förvaltning (goteborg.se)

personuppgiftsbehandlingar som omfattas. Det område där verksamheten behöver genomföra åtgärder är därför framför allt att i samråd med de nya tjänsteleverantörerna klarlägga ansvarsförhållandena. Därefter behöver en kartläggning göras över vilka personuppgiftsbehandlingar som ansvaret behöver regleras för. Först därefter kan förvaltningen säkerställa att nödvändiga överenskommelser och/eller avtal med instruktioner kan tecknas.

Därutöver finns det behov av att ta fram och dokumentera arbetssätt för att bedöma ansvarsförhållanden gentemot nya leverantör eller andra samarbetspartners, samt öka den förvaltningsinterna kompetens som krävs för att genomföra detta arbete. Det är även viktigt att förvaltningens dataskyddskontakter informeras och vid behov involveras i sådant arbetet. Verksamheten behöver därutöver ta fram och dokumentera arbetssätt för att kontinuerligt genomföra efterlevnadskontroller av anlitade personuppgiftsbiträden med syftet att säkerställa att dessa uppfyller villkoren enligt biträdesavtalet. I detta ingår att bedöma hela kedjan av eventuella underbiträden.

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. Enligt verksamhetens skattning ligger arbete med registret kvar på samma nivå som föregående och 2021 års nivåer. Förvaltningens dataskyddskontakt uppger att ett arbete har påbörjats med att se över hur registret relaterar till den nya dokumenthanteringsplanen. Arbetet genomförs av dataskyddskontakt i samarbete med arkivarie och kommer framöver att vara ett prioriterat område för dataskyddsarbetet. Vissa aktiviteter överlappar med arbetet med att informationssäkerhetsklassa och kommer att göras inom ramen för arbetet med informationssäkerhet.

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. Områden där verksamheten behöver genomföra åtgärder är att kartlägga och dokumentera förvaltningens personuppgiftsbehandlingar samt uppdatera den information som finns i registret så att den överensstämmer med kraven i artikel 30 i GDPR. Dataskyddsombudet ser positivt på att en översyn av förvaltningens register över personuppgiftsbehandlingar ska göras. Att ta avstamp i förvaltningens dokumenthanteringsplan i det arbetet, är en bra utgångspunkt eftersom denna ger en god överblick över all verksamhet inom organisationen. Att det saknas behandlingar i förvaltningens register utgör en risk, liksom att det för många

behandlingar saknas tillräcklig information. Till stöd i arbetet rekommenderas förvaltningen att dels använda det informationsmaterial som dataskyddsombudet tagit fram under året, dels samråda med dataskyddsombudet. Vidare behöver förvaltningen ta fram och dokumentera arbetssätt för att kontinuerligt uppdatera registret med behandlingar som tillkommer och/eller förändras.

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. Föregående år angavs att förvaltningen valt att först fokusera på att bygga upp kompetenser i organisationen, innan det att intern kontroll påbörjas. Vidare angavs att ett arbete med att inventera informationstillgångar hade påbörjats. Dataskyddskontakt har uppgett att man i årets enkät har angett att stora delar av verksamhetens informationstillgångar ännu inte har informationsklassats enligt stadens styrande dokument, eftersom denna riktlinje är ny för i år[3]. Arbetet med att inventera informationstillgångar och personuppgiftsbehandlingar pågår. Dataskyddskontakt uppger att man i alla dataskyddsfrågor tydligt arbetar riskbaserat. Vidare finns en plan på att ta fram årshjul för dataskyddsarbetet.

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. Som framgår av flera andra kontrollpunkter finns det ett behov av att ta fram en långsiktig plan för arbetet med dataskydd inom förvaltningen. I stor utsträckning påverkas möjligheten att planera långsiktigt av att delar av organisationen fortfarande är under utarbetande och att vissa grundläggande arbeten behöver komma på plats. Bland dessa exempelvis implementering av ny dokumenthanteringsplan, kartläggning av informationstillgångar, IT-system och digitala verktyg och register över personuppgiftsbehandlingar – inklusive bedömning av för vilka behandlingar som en konsekvensbedömning avseende dataskydd ska genomföras. Dataskyddsombudet rekommenderar därför förvaltningen att prioritera dessa områden, för att därefter kunna gå vidare med att ta fram en långsiktig planering och årshjul för dataskyddsarbetet.

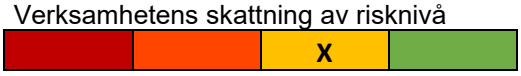
För att personuppgifterna i den information som förvaltningen hanterar ska kunna hanteras på ett säkert sätt behöver informationen bland annat klassificeras, som ett led i att tillförsäkra rätt nivå av skydd för personuppgifter. För Göteborgs Stad finns det en ny informationssäkerhetsriktlinje och klassningsmodell. Dataskyddsombudet är positiv till att socialförvaltningarna har inlett ett gemensamt

[3] Riktlinjen reviderades i maj 2023 Göteborgs Stads riktlinje för informationssäkerhet (goteborg.se)

arbete för att klassa informationstillgångar enligt Göteborgs Stads nya riktlinje för informationssäkerhet.

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. Föregående år uppgavs att man försökt samordna utbildnings- och informationsinsatser med arkivarie och IT. Detta har ännu inte genomförts, enligt uppgift från dataskyddskontakt, men planeras att göras under 2024. På fråga till dataskyddskontakter om vilken kartläggning som har gjorts över behov av utbildning, uppger dataskyddskontakten att någon bred kartläggning inte har gjorts. I stället har dataskyddskontakterna i sitt arbete med personuppgiftsincidenter och konsekvensbedömningar avseende dataskydd identifierat behov av utbildningsinsatser. Bland annat vill man utifrån detta behov ta fram en utbildning om personuppgiftsincidenter. Utöver detta har vissa verksamheter hört av sig till dataskyddskontakterna och efterfrågat utbildningsinsatser i dataskyddsfrågor. Under året har utbildning i dataskydd och informationssäkerhet getts i samband med att nya chefer introducerats. Detta arbete kommer att fortsätta även framöver. I samband med att digitala navet införs kommer också en översyn av vilken information som ska finnas tillgänglig på intranätet att göras.

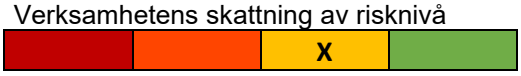
Dataskyddsombudet delar verksamhetens bedömning om att det finns risker som behöver åtgärdas, men gör precis som verksamheten bedömningen att de inte är omfattande, brådskande eller allvarliga. Dataskyddsombudet ser positivt på att dataskyddskontakter i viss utsträckning har analyserat vilken nivå av dataskyddskunskap som olika befattningars arbete kräver och planerar utbildnings- och informationsinsatser utifrån identifierade behov. En god allmän kunskapsnivå om dataskydd hos medarbetarna i förvaltningen skapar goda förutsättningar för dataskyddsarbetet i stort. Det ökar förutsättningarna för att bland annat personuppgiftsincidenter hanteras korrekt, att registrerade får sina rättigheter enligt GDPR tillgodosedda eller att dataskyddsperspektivet beaktas när ett nytt IT-stöd ska införas i verksamheten. Det här är därmed en kontrollpunkt som även får stor påverkan på resultatet av flera av de andra kontrollpunkterna, i och med att medarbetare med mer kunskap har bättre förutsättningar att behandla personuppgifter på ett korrekt sätt i enlighet med gällande lagstiftning.

Dataskyddsombudet rekommenderar därför förvaltningen att i första hand prioritera att genomföra planerade utbildnings- och informationsinsatser. Vidare behöver förvaltningen se till att verksamheten har dokumenterade arbetssätt för att följa upp och bibehålla kunskapsnivån hos medarbetarna efter genomförda utbildningar. Att ta fram en långsiktig plan för att arbeta strategiskt med att utbilda medarbetare inom dataskydd är också en åtgärd som förvaltningen på sikt bör

överväga. För att kunna säkerställa att medarbetarna erbjuds rätt utbildningsinsatser behöver förvaltningen först systematiskt kartlägga och analysera vilka utbildningar och andra kompetenshöjande insatser som behövs för att sedan kunna ta fram en långsiktig utbildningsplan. En kartläggning av behovet av kompetens eller kunskap som behövs kan även omfatta behovet av specialkunskaper i vissa fall. Att förvaltningen analyserar vilka eventuella behov av utbildning som finns hos exempelvis de som arbetar med specifika dataskyddsfrågor eller frågor där dataskyddsfrågor särskilt ska beaktas är minst lika viktigt som att alla medarbetare har viss grundläggande kunskap om dataskydd.

3.2.7 Kontrollpunkt 7: Informationsplikt

Verksamhetens skattning av risknivå



Dataskyddsombudets bedömning

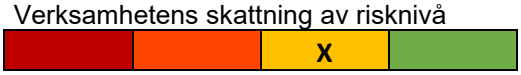
Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger risker som behöver åtgärdas, men att dessa inte är brådskande, omfattande eller allvarliga. Dataskyddskontakt uppger att det ännu inte har gjorts några uppdateringar av den information om behandling av personuppgifter som finns i förvaltningens integritetspolicy. Föregående år fick förvaltningen rekommendationen att se över integritetspolicyn utifrån innehåll, hur innehållet presenteras och vilken specifik information som ges i samband med olika behandlingar. På enkätfrågan om huruvida de registrerade på ett enkelt sätt kan nå verksamhetens integritetsinformation/-policy från samtliga digitala kanaler har svaret ”vet inte/kan inte besvara frågan” angetts.

När personuppgifter behandlas är förvaltningen skyldig enligt bestämmelser i GDPR att ge information till den registrerade om hur dennes personuppgifter behandlas. Dataskyddsombudet bedömer att förvaltningen ännu inte lever upp till den skyldigheten. Detta eftersom det finns brister dels i vilken information som ges, dels på vilket sätt informationen ges till olika kategorier av registrerade. 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.

Utifrån vad som framgår ovan rekommenderar dataskyddsombudet förvaltningen på nytt att se över den information som ges till de registrerade. För närmare vägledning hänvisar dataskyddsombudet till de rekommendationer som gavs i 2022 års årsrapport samt till den informationsinsats som dataskyddsombudet tillhandahåll under 2023. Därutöver rekommenderar dataskyddsombudet förvaltningen att se över i vilka digitala kanaler som information till registrerade behöver lämnas samt hur det kan göras.

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. Det har under året 2023 tagits fram och antagits en ny dokumenthanteringsplan. Även andra styrande dokument har arbetats fram och antagits. Den låga skattningen av arbetet med att informationsklassificera personuppgiftsbehandlingar utifrån stadens riktlinje, beror enligt uppgift från dataskyddskontakt, på att riktlinjen är ny för i år. En planering för arbetet med att implementera dokumenthanteringsplan så väl som klassificera information är under framtagande.

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. Dataskyddsombudet ser positivt på att arbete inom området har prioriterats under 2023 och att förvaltningen numera har en dokumenthanteringsplan på plats. Det är nu viktigt att förvaltningen ser till att det finns dokumenterade arbetssätt för att säkerställa att handlingar som innehåller personuppgifter gallras i enlighet med gällande gallringsbeslut samt att alla medarbetare har kunskap om förvaltningens dokumenthantering och gallringsbestämmelser kopplat till kraven i GDPR.

Mot bakgrund av att det finns det en ny informationssäkerhetsriktlinje och klassningsmodell inom Göteborgs Stad ser dataskyddsombudet positivt på att socialförvaltningarna har inlett ett gemensamt arbete för att informationsklassificera personuppgiftsbehandlingar i enlighet med stadens nya riktlinjer.

3.2.9 Kontrollpunkt 9: Konsekvensbedömning/samråd

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. Av de lämnade svaren framgår att en stor andel av förvaltningens personuppgiftsbehandlingar med höga risker ännu inte har konsekvensbedömts. Dataskyddskontakterna berättar att målet är att arbeta strategiskt med konsekvensbedömningar, för att undvika ett arbetssätt där endast mindre och nya behandlingar bedöms utifrån dataskyddsrisker. Under året har dataskyddsombudet involverats i samband med att konsekvensbedömningar har genomförts.

Dataskyddsombudet delar förvaltningens bedömning av de frågor som ställts under kontrollpunkten men anser att det sammanvägda resultatet inte ger en korrekt bild av risknivån. Det föreligger enligt dataskyddsombudets bedömning omfattande risker för förvaltningen med anledning av att det finns många pågående personuppgiftsbehandlingar som ännu inte har kontrollerats utifrån höga risker för de registrerades fri- och rättigheter. Dataskyddsombudet rekommenderar förvaltningen att kartlägga vilka personuppgiftsbehandlingar som innebär hög risk för registrerades fri- och rättigheter. En sådan kartläggning är ett viktigt verktyg för att sedan kunna ta fram en långsiktig plan för arbetet med att genomföra konsekvensbedömningar avseende dataskydd, i samtliga de fall där detta är ett krav enligt artikel 35 i GDPR. Därefter bör en handlingsplan tas fram för att kunna prioritera och genomföra konsekvensbedömningar av behandlingar med störst risker för de registrerade. För att arbeta riskbaserat är det lämpligt att prioritera personuppgiftsbehandlingar inom förvaltningens kärnverksamhet. I detta arbete bör ingå att ta ställning till vem eller vilka som ska genomföra arbetet, det vill säga vilka roller och vilken kompetens som behövs samt i vilka fall det är lämpligt att samarbeta över förvaltningsgränser. Förvaltningens mål bör vara att på sikt ha genomfört konsekvensbedömningar för samtliga behandlingar där det krävs. Förvaltningen rekommenderas att samråda med dataskyddsombudet kring frågor om bland annat prioriteringar och lämpliga avgränsningar i arbetet.

Dataskyddsombudet vill kommentera behovet av att genomföra konsekvensbedömningar för de personuppgiftsbehandlingar där Treserva utgör en informationsbärare. Att dessa behandlingar var pågående när dataskyddsförordningen infördes, medför inte att kravet på konsekvensbedömning avseende dataskydd kan frångås[4]. Även om det systemstöd där personuppgifter behandlas har stor betydelse för bedömningen av risker för de registrerade, så ska bedömning av risk göras utifrån personuppgiftsbehandlingen och inte utifrån systemet som sådant. Att dessa behandlingar framöver kan komma att flyttas från Treserva till andra verksamhetsstöd innebär inte att en genomförd konsekvensbedömning avseende dataskydd som genomförs innan, har gjorts i onödan. Att behandlingar av personuppgifter bedöms utifrån risker för de registrerade kan därtill utgöra ett värdefullt verktyg för det fall nya verksamhetsstöd ska upphandlas i framtiden.

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

[4] Riktlinjer om konsekvensbedömning avseende dataskydd och fastställande av huruvida behandlingen ”sannolikt leder till en hög risk” i den mening som avses i förordning 2016/679, WP 248, antagna den 4 april 2017, s 15 f.

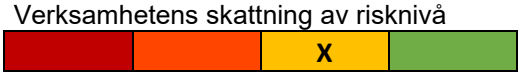
föreligger. Föregående år angavs att dataskyddskontakterna arbetade för att tidigare involveras i olika inköps- och upphandlingsprocesser och under innevarande år har vissa rutiner och checklistor tagits fram för dessa processer för att säkerställa dataskyddsperspektivet. Under året har dataskyddskontakter också deltagit i upphandlingsprojekt. Dataskyddskontakter informerar dataskyddsombudet löpande om de upphandlingar där dessa deltar. Det pågår också upphandlings- och utvecklingsprojekt där annan dataskyddskompetens än förvaltningens egna dataskyddskontakter deltar, till följd av samverkan mellan socialförvaltningarna.

Dataskyddsombudet delar till stor del verksamhetens bedömning. Dataskyddsombudet gör dock till skillnad ifrån verksamheten bedömningen att det ändå föreligger risker inom kontrollpunkten. Bland annat utifrån att äldre samt vård- och omsorgsförvaltningen är en mycket stor organisation, vilket kräver att fler än bara dataskyddskontakterna aktivt och systematiskt arbetar med att bedöma risker för personuppgiftsbehandlingar i samband med upphandlingar av nya, så väl som vid utvecklingen av befintliga, verksamhetsstöd och tjänster. Därtill påverkas förvaltningens arbete till viss del av den omorganisation som genomfördes vid årsskiftet 2022/23 inom ramen för stadens styrmodell för digitalisering. Mot bakgrund av att ansvaret för förvaltning och utveckling av de verksamhetsspecifika tjänsterna kopplade till vård och omsorg numera innehas av Tjänsteförvaltning integrerad digitalisering (TID) inom socialförvaltning Nordost behöver förvaltningen se till så att det fastställas ett arbetssätt som säkerställer att dataskyddsfrågorna införlivas i det förvaltnings- och utvecklingsarbetet som TID bedriver.

Dataskyddsombudet rekommenderar därför förvaltningen att säkerställa att de roller som ansvarar för upphandling och utveckling av såväl nya som befintliga system och tjänster har kunskaper om dataskydd och vilka krav som ställs utifrån dataskyddsförordningen. Detta kan exempelvis innebära utbildningsinsatser, att ta fram arbetssätt som säkerställer att personer med kompetens konsulteras eller ta fram stöd för arbetet så som checklistor eller liknande. Dataskydd ska vara en del vid kravställning, upphandling och implementering.

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. Verksamheten har skattat sig lågt på frågor om tilldelning och uppföljning av behörigheter i IT-system. Av de svar som verksamheten har lämnat i uppföljningen av den fördjupade kontroll som avser behörighetsstyrning i Treserva, framkommer att en av svårigheterna med att anpassa behörigheter är tekniska begränsningar i Treserva (jmf avsnitt 3.3.1). Dataskyddskontakter har uppgett att de fortfarande inväntar en heltäckande och uppdaterad dokumentation över samtliga IT-system

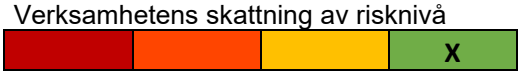
och digitala verktyg som används inom organisationen. En sådan ska tas fram, vilken kommer att utgöra ett bra stöd och ge god överblick över vilket arbete som behöver göras inom kontrollpunkten. Så här långt är ett av de riskområden som identifierats mobila arbetssätt och det pågår ett arbete för att identifiera och vidta åtgärder för att minska risker inom det området. Dataskyddskontakterna uppger också att de är beroende av samverkan med andra roller både inom den egna förvaltningen och externt, vilket fortfarande är ett utvecklingsområde. Bland annat finns nya strategiska nätverk inom digitalisering, där rollerna ännu inte har satt sig.

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. Dataskyddsombudet delar verksamhetens bedömning att det är viktigt att en kartläggning över IT-system och digitala verktyg tas fram. Dataskyddsombud rekommenderar förvaltningen att prioritera arbetet med att ta fram en förteckning över IT-system och digitala verktyg.

Vidare delar dataskyddsombudet verksamhetens bedömning att arbetet med tilldelning och uppföljning av behörigheter är ett område där det föreligger risker. Dataskyddsombudet rekommenderar förvaltningen att säkerställa att de dokumenterade arbetssätt för tilldelning av behörigheter och åtkomster till samtliga av förvaltningens IT-system är korrekta och anpassade. Dataskyddsombudet vill i detta sammanhang göra förvaltningen uppmärksam på den regeländring om tilldelning av behörighet för åtkomst och kontroll av åtkomst som gjorts under året[5] och den som förväntas göras under första delen av år 2024[6]. Det här behöver förvaltningen beakta i arbetet med tilldelning av behörigheter och åtkomster till IT-system som träffas av den aktuella lagstiftningen. Ändringarna motsvarar i stort det som sedan tidigare gäller inom hälso- och sjukvårdsområdet, vilket innebär att även socialtjänstområdet framöver är reglerat på motsvarande sätt.

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. Dataskyddskontakter uppger att de blir kontaktade av andra funktioner inom förvaltningen, i samband med att registrerade utöver sina rättigheter. Bland annat arbetar dataskyddskontakterna nära förvaltningsjurist och registratorer. Det har under året tagits fram och dokumenterats arbetssätt för att säkerställa att registrerades rättigheter hanteras rättssäkert. Dataskyddskontakterna bedömer att de funktioner som vanligen hanterar förfrågningar från registrerade vård- eller

[5] Lag (2022:913) om sammanhållen vård- och omsorgsdokumentation
[6] Ny 10 § lag (2001:454) om behandling av personuppgifter inom socialtjänsten

omsorgstagare har god kännedom om vilka rättigheter dessa har enligt GDPR och vilka rutiner som gäller inom förvaltningen.

Dataskyddsombudet delar verksamhetens bedömning och anser att verksamheten har ett systematiskt arbete inom kontrollpunkten och inga risker av betydelse föreligger. Förvaltningen har under året involverat dataskyddsombudet i frågor som rör de registrerades rättigheter.

Även inom verksamheter med låga risker krävs det kontinuerliga insatser för att ett systematiskt dataskyddsarbete ska kunna upprätthållas och stärkas ytterligare. En förbättringsåtgärd som dataskyddsombudet identifierat skulle kunna vidtas inom ramen för kontrollpunkten är att genom bland annat utbildning och informationsinsatser säkerställa att medarbetarna har kunskap om de registrerades rättigheter och i vilka fall de begränsas. Vidare är en förbättringsåtgärd att säkerställa att även HR-funktionen har god kännedom om vilka regler som gäller för anställda registrerade som vill utöva sina rättigheter enligt GDPR.

3.3 Uppföljning

3.3.1 Uppföljning av rekommendationer lämnade inom ramen för tidigare genomförd kontroll

Dataskyddsombudet har följt upp vilka åtgärder som vidtagits utifrån rekommendationer som lämnats vid den fördjupade kontrollen 2022. Under 2022 genomförde dataskyddsombudet en fördjupad kontroll där delar av verksamhetens arbete med behörighetsstyrning i IT-systemet Treserva granskades. Syftet med kontrollen var att granska om dataskyddsombudet ser risker i verksamhetens arbete med behörighetsstyrning utifrån kraven i artikel 32 i GDPR. Kontrollen avgränsades till att endast omfatta tilldelning och kontroll av behörigheter för chefer och medarbetare vid avdelning Myndighet Hisingen och Sydväst.

Kontroll (2022): Behörighetsstyrning

Verksamheten gavs följande rekommendationer:

• Se över och dokumentera ert arbetssätt för tilldelning av behörigheter.

• Se över ert arbetssätt för uppföljning av tilldelade behörigheter.

• Fortsätt arbetet med att ta fram rutiner för loggranskning och gör dessa rutiner kända bland medarbetarna.

• Ge personuppgiftsbiträdet Intraservice dokumenterade instruktioner.

• Ta arbetet vidare med ny profil för avvikelsehantering och motverka kvarstående risker.

• Se över utformningen av de behörigheter som tilldelats medarbetare i Treserva, med hänsyn till risker för klienters integritet.

• Gör en bedömning av om aktuella personuppgiftsbehandlingar behöver konsekvensbedömas.

Kommentarer och rekommendationer:

Av de svar som förvaltningen har lämnat framgår att styrande dokument har tagits fram. Dataskyddskontakt uppger att dessa nu ska implementeras. Ett systematiskt arbete för uppföljning av behörigheter har påbörjats, där dataskyddskontakter kommer att arbeta tillsammans med rollen lokalt verksamhetsstöd (LVS). För medarbetare som arbetar inom andra förvaltningar, som behöver tillgång till förvaltningens ärenden i Treserva, saknas tillräckliga möjligheter att tekniskt begränsa behörigheterna, vilket har felanmälts till leverantör. Ett samarbete med tjänsteförvaltning integrerad digitalisering (TID) har inletts, där medarbetare hos TID ställer krav på bättre funktionalitet för behörighetsstyrning hos leverantören. Organisatoriska säkerhetsåtgärder finns på plats, som innebär att medarbetare får instruktioner om begränsningar i hur de får använda en tilldelad teknisk behörighet som är vidare än den befogenhet handläggaren har. Vidare framkommer att granskning av loggar inte kan göras på ett ändamålsenligt sätt, på grund av tekniska begräsningar i Treserva. Även detta har felanmälts till leverantör.

Kommentarer och rekommendationer:

Dataskyddsombudets uppföljning visar att förvaltningen har beaktat och vidtagit vissa åtgärder i enlighet med lämnade rekommendationer men att det fortfarande finns förbättringsområden inom denna kontroll. Utifrån den regeländring om tilldelning av behörighet för åtkomst och kontroll av åtkomst som gjorts under året i samband med att lag (2022:913) om sammanhållen vård- och omsorgsdokumentation trädde i kraft, och den nya bestämmelse i lag (2001:454) om behandling av personuppgifter inom socialtjänsten[7] som förväntas träda i kraft under 2024, kommer förvaltningen att behöva arbeta mer aktivt med behörighetstilldelning i IT-system som omfattas av lagstiftningen. Dataskyddsombudet ser därför positivt på det arbete som har påbörjats internt så väl som i samarbete med andra förvaltningar och leverantör. Dataskyddsombudet kommer att följa upp förvaltningens arbete med tilldelning av behörighet för åtkomst och kontroll av åtkomst under 2024, huvudsakligen med utgångspunkt i den nya lagstiftningen. Uppföljningen kommer att ske löpande.

[7] Genom tillägg av en ny paragraf, 10 § i SoLPul.

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 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
  Säkerställ att samtliga personuppgiftsbehandlingar dokumenteras i behandlingsregistret och att registret innehåller all obligatorisk information om behandlingarna enligt artikel 30 i GDPR.

- Kontrollpunkt 6: Utbildning
  Genomför planerade utbildnings- och informationsinsatser. Kartlägg behovet av utbildningar och andra kompetenshöjande insatser för att därefter ta fram en långsiktig utbildningsplan.

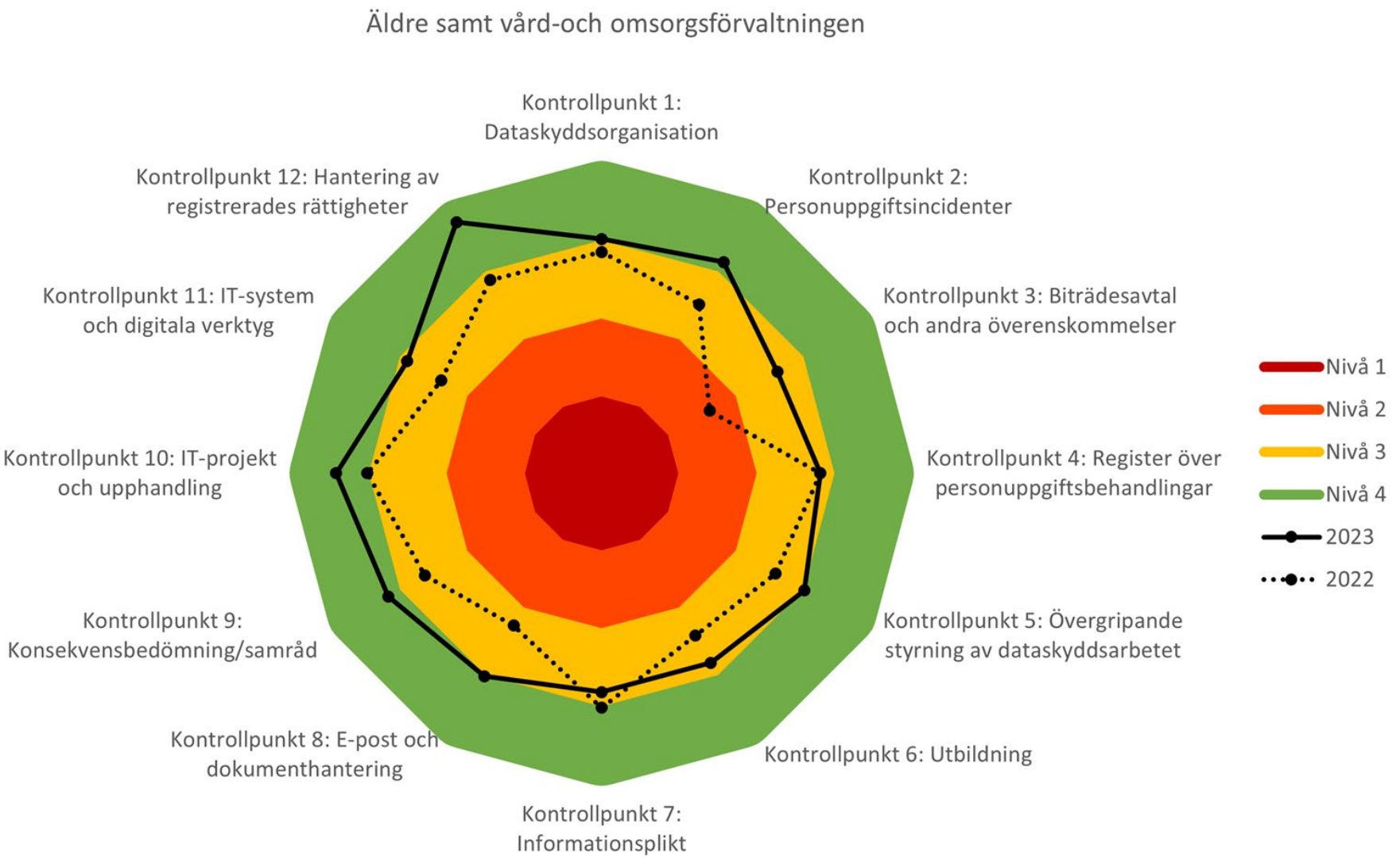
- Kontrollpunkt 9: Konsekvensbedömning/samråd
  Kartlägg personuppgiftsbehandlingar som innebär en hög risk för de registrerades fri- och rättigheter och ta fram en handlingsplan för att på sikt säkerställa att konsekvensbedömningar genomförs för samtliga behandlingar där detta krävs.

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

Äldre samt vård- och omsorgsförvaltningen

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.