Göteborgs Stad

Årsrapport för dataskyddsarbetet 2023

Nämnden för funktionsstöd

2023-12-20

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.	

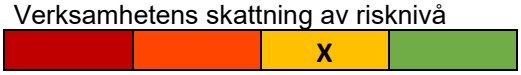
3.2 Resultat från kontrollen 2023

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.

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 bedömer att det finns en väl fungerande intern dataskyddsorganisation. Det finns inom den interna dataskyddsorganisationen en god förståelse för de dataskyddsfrågor som behöver omhändertas inom förvaltningen. Dataskyddskontakterna lyfter många och viktiga frågor med dataskyddsombudet. Det är dessutom positivt att förvaltningen under året bland annat har uppdaterat delegationsordningen för att säkerställa att det är tydligt vem som är behörig att fatta beslut i olika typer av dataskyddsfrågor.

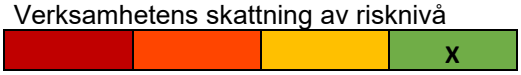
Trots detta finns det ändå områden där förvaltningen behöver genomföra åtgärder.

En förbättringsåtgärd som dataskyddsombudet identifierat behöver vidtas inom ramen för kontrollpunkten är att se över och säkerställa att den interna dataskyddsorganisationen har tillräckliga resurser för att bedriva ett kontinuerligt och systematiskt dataskyddsarbete. Dataskyddsombudet lyfter detta med anledning av att dataskyddslagstiftningen berör samtliga delar av förvaltningens verksamhet där personuppgifter behandlas i någon form. Eftersom förvaltningen bedriver socialtjänst behandlas dessutom en mycket stor mängd extra skyddsvärda och känsliga personuppgifter. De dataskyddsfrågor som behöver hanteras inom förvaltningen kan ibland vara både omfattande och komplicerade. Det medför att den interna dataskyddsorganisationen behöver ha tillräckliga resurser, kompetens och tid att arbeta med frågorna.

Förvaltningen rekommenderas även fortsatt arbeta med att göra dataskydd till en integrerad och naturlig del av det dagliga arbetet så att det finns kunskap och medvetenhet om dataskydd på samtliga nivåer inom förvaltningen. Det kan ske genom exempelvis ett utökat arbete med utbildningsinsatser, vilket dataskyddsombudet återkommer till under kontrollpunkt 6, Utbildning.

3.2.2 Kontrollpunkt 2: Personuppgiftsincidenter

Verksamhetens skattning av risknivå



Dataskyddsombudets bedömning

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

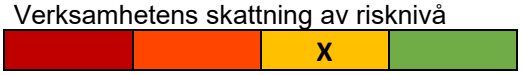
Dataskyddsombudet delar verksamhetens bedömning och anser att verksamheten har ett systematiskt arbete inom kontrollpunkten och inga risker av betydelse föreligger. Dataskyddsombudet bedömer att förvaltningen bedriver ett bra arbete med att upptäcka, utreda och dokumentera personuppgiftsincidenter. Förvaltningen kontaktar även dataskyddsombudet vid inträffade personuppgiftsincidenter.

Även inom verksamheter med låga risker krävs det dock kontinuerliga insatser för att ett systematiskt dataskyddsarbete ska kunna upprätthållas och stärkas ytterligare. En insats som kan vidtas inom ramen för kontrollpunkten är att fortsätta arbeta för att säkerställa att förvaltningens medarbetare, inom samtliga nivåer och verksamhetsområden, har kunskap om vad som är en personuppgiftsincident och hur incidenter ska hanteras. Det kan ske genom exempelvis ett utökat arbete med utbildningsinsatser.

Förvaltningen behöver även säkerställa att det finns dokumenterade arbetssätt för när och hur information till de registrerade ska ges vid personuppgiftsincidenter.

3.2.3 Kontrollpunkt 3: Biträdesavtal och andra överenskommelser

Verksamhetens skattning av risknivå



Dataskyddsombudets bedömning

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

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

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

Att reda ut rollerna inom dataskydd är en av de svårare men också en av de viktigaste utmaningarna i dataskyddsarbetet. En personuppgiftsansvarig behöver bland annat säkerställa att samtliga personuppgiftsbiträden har identifierats och att nödvändiga avtal eller någon annan rättsakt har tecknats. Det finns även krav att mellan gemensamt personuppgiftsansvariga reglera ansvarsförhållanden.

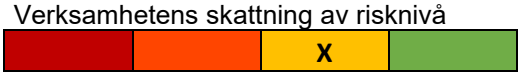
Inom förvaltningen pågår ett arbete med att se över personuppgiftsbiträdesavtalen, med målsättningen att säkerställa att avtal eller annan rättsakt har tecknats med samtliga personuppgiftsbiträden samt att instruktioner har lämnats. Dataskyddsombudet vill uppmuntra förvaltningen att fortsätta det goda arbete som inletts.

Dataskyddsombudet rekommenderar förvaltningen att därutöver säkerställa att det finns både dokumenterade arbetssätt och kompetens för att bedöma hela kedjan av underbiträden vid anlitandet av ett personuppgiftsbiträde. Det behöver även finnas dokumenterade arbetssätt inom förvaltningen för att kunna genomföra efterlevnadskontroller i syfte att säkerställa att biträden följer det som avtalats och de instruktioner som lämnats.

Inom ramen för denna kontrollpunkt behöver det även beaktas de förändringar som skett inom Göteborgs Stad sedan ny styrmodell trädde i kraft den 1 januari 2023. Detta påverkar förvaltningen på så vis att det bland annat numera finns tre tjänsteleverantörer i Göteborgs Stad: förvaltningen för demokrati och medborgarservice, inköps- och upphandlingsförvaltningen och Intraservice. Ansvaret för förvaltning och utveckling av de verksamhetsspecifika tjänsterna kopplade till vård och omsorg flyttades dessutom vid årsskiftet till Tjänsteförvaltning integrerad digitalisering inom socialförvaltning Nordost. Förvaltningen behöver därför inte enbart klarlägga ansvarsförhållanden med externa aktörer utan även med dessa staden-interna aktörer och säkerställa att nödvändiga avtal, överenskommelser och/eller instruktioner finns på plats. I detta ingår att också kartlägga vilka personuppgiftsbehandlingar som ska omfattas av sådana avtal eller överenskommelser.

3.2.4 Kontrollpunkt 4: Register över personuppgiftshandlingar

Verksamhetens skattning av risknivå



Dataskyddsombudets bedömning

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

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

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

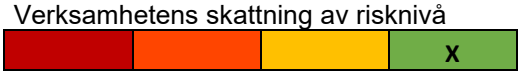
Förvaltningen saknar idag ett fullständigt och uppdaterat behandlingsregister, med all den nödvändiga information som krävs enligt artikel 30 i GDPR. Dataskyddsombudet rekommenderar därför förvaltningen att prioritera det arbetet, då det är en av hörnstenarna i ett fungerande dataskyddsarbete. För att uppnå ett heltäckande behandlingsregister som hålls aktuellt över tid krävs även att

förvaltningen har fungerande och dokumenterat arbetssätt för att kontinuerligt uppdatera registret med behandlingar som tillkommit eller förändras. Förvaltningen bör därför se över hur man ska arbeta med behandlingsregistret på ett systematiskt sätt.

Ett aktuellt och uppdaterat behandlingsregister kan dessutom vara ett användbart hjälpmedel i förvaltningens övriga dataskyddsarbete. Dataskyddsombudet vill uppmuntra förvaltningen att använda behandlingsregistret i arbetet med andra kontrollpunkter, exempelvis i ett arbete med att ta fram en långsiktig plan för det fortsatta arbetet med dataskydd.

3.2.5 Kontrollpunkt 5: Övergripande styrning av dataskyddsarbetet

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.

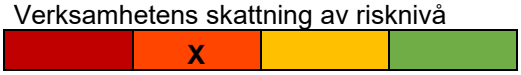
Dataskyddsombudet delar verksamhetens bedömning och anser att verksamheten har ett systematiskt arbete inom kontrollpunkten och inga risker av betydelse föreligger.

Även inom verksamheter med låga risker krävs det kontinuerliga insatser för att ett systematiskt dataskyddsarbete ska kunna upprätthållas och stärkas ytterligare. En viktig del av förvaltningens övergripande styrning av dataskyddsarbetet handlar om att integrera dataskyddsfrågorna i det övriga informationssäkerhetsarbetet. Dataskyddsombudet rekommenderar därför förvaltningen att bedriva ett aktivt och systematiskt arbete med att säkerställa att informationssäkerhetsarbetet sker med stöd av bestämmelserna i GDPR och övrig dataskyddslagstiftning, så att de registrerades fri- och rättigheter kontinuerligt beaktas. Följsamheten mot dataskyddslagstiftningen inom förvaltningen behöver dessutom regelbundet kontrolleras. Ett sätt att kontrollera följsamheten av gällande bestämmelser är genom efterlevnadskontroller inom organisationen.

För att personuppgifterna i den information som förvaltningen hanterar ska kunna hanteras på ett säkert sätt behöver informationen även klassificeras, som ett led i att tillförsäkra rätt nivå av skydd för personuppgifter. För Göteborgs Stad finns sedan i år en ny informationssäkerhetsriktlinje och klassningsmodell. Dataskyddsombudet tycker att det är positivt att ett arbete har inletts för att klassa informationstillgångar enligt Göteborgs Stads nya klassningsmodell.

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.

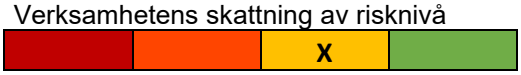
Dataskyddsombudet delar verksamhetens bedömning om att det förekommer risker som är omfattande och kan kräva omgående åtgärder.

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.

Förvaltningens svar indikerar att medarbetare ges möjlighet att få information och utbildning i dataskydd. Den allmänna kunskapsnivån hos medarbetarna är dock fortfarande låg. Dataskyddsombudet rekommenderar därför förvaltningen att fortsätta det arbete som inletts för att åstadkomma en allmän höjning av kunskapsnivån om dataskydd i förvaltningen. För att kunna säkerställa att medarbetarna erbjuds rätt utbildningsinsatser behöver förvaltningen först kartlägga 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 dem som arbetar med specifika dataskyddsfrågor är minst lika viktigt som att alla medarbetare har viss grundläggande kunskap om dataskydd. Dessutom behöver förvaltningen se till så att det finns arbetssätt som säkerställer att kunskapsnivån behålls även efter genomförda utbildningsinsatser.

3.2.7 Kontrollpunkt 7: Informationsplikt

Verksamhetens skattning av risknivå



Dataskyddsombudets bedömning

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

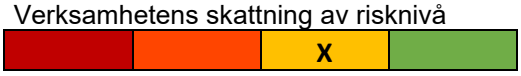
Dataskyddsombudet delar verksamhetens bedömning om att det finns risker som behöver åtgärdas, men gör precis som verksamheten bedömningen att de inte är omfattande, brådskande eller allvarliga.

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.

Dataskyddsenheten höll under våren 2023 en särskild informationsinsats rörande vad som omfattas av informationsplikten enligt GDPR. Dataskyddsombudet rekommenderar förvaltningen, att med utgångspunkt i detta informationsmaterial, se över vilken information de registrerade behöver få och på vilket sätt information ska ges om personuppgiftsbehandlingen. Dataskyddsombudet rekommenderar förvaltningen att därefter göra nödvändiga justeringar för att säkerställa att den information som lämnas till de registrerade uppfyller kraven i artikel 13–14 i GDPR. Dataskyddsombudet vill även understryka att det är lämpligt att mottagaranpassa information. Informationsplikten omfattar både information som lämnas genom en integritetspolicy och information som lämnas på andra sätt till den registrerade. Informationen behöver dessutom vara lättillgänglig oavsett i vilken del av verksamheten som den registrerades personuppgifter behandlas, inbegripet förvaltningens digitala kanaler.

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

Det är av stor vikt att det finns en dokumenthanteringsplan med gallringsbeslut inom en verksamhet för att personuppgiftsbehandlingar ska kunna ske i enlighet med bland annat principen om lagringsminimering i GDPR. En dokumenthanteringsplan behöver omfatta alla verksamhetsdelar och det ska finnas rutiner för när personuppgifter gallras. Förvaltningen har numera en fastställd dokumenthanteringsplan och förvaltningens medarbetare har även fått information om denna genom bland annat informationsfilmer på intranätet. Det som förvaltningen nu behöver säkerställa är att handlingar som innehåller personuppgifter gallras i enlighet med gällande gallringsbeslut.

Mot bakgrund av att det finns det en ny informationssäkerhetsriktlinje och klassningsmodell inom Göteborgs Stad så anser dataskyddsombudet därutöver att det är positivt att ett arbete har inletts för informationsklassificera förvaltningens personuppgiftsbehandlingar i enlighet med stadens riktlinjer.

3.2.9 Kontrollpunkt 9: Konsekvensbedömning/samråd

Verksamhetens skattning av risknivå

Dataskyddsombudets bedömning

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

Dataskyddsombudet delar verksamhetens bedömning om att det finns risker som behöver åtgärdas och bedömer att de utgör relativt omfattande risker för förvaltningen med anledning av att det finns många pågående personuppgiftsbehandlingar inom förvaltningens olika verksamhetsdelar som inte har kontrollerats utifrån höga risker för de registrerades fri- och rättigheter.

Syftet med konsekvensbedömningar är att förebygga risker och på så sätt även minimera riskerna vid sådana behandlingar av personuppgifter som innebär en hög risk för de registrerades fri- och rättigheter. Arbetet med konsekvensbedömningar behöver inledas i ett tidigt skede vid nya eller förändrade behandlingar och vid införanden behöver man ta höjd för att arbetet kräver tid, resurser och korrekt kompetens. Konsekvensbedömningar behöver även genomföras för pågående behandlingar med höga risker för de registrerade om det inte har gjorts tidigare.[2] Konsekvensbedömningsarbetet är till stor del avhängigt den generella medvetenheten om dataskydd inom förvaltningen som helhet och dataskyddsorganisationen i stort. Det behöver finnas kunskap inom verksamheten om bland annat när en konsekvensbedömning behöver göras, hur den ska genomföras, vem som ska involveras och vem som ansvarar för att genomföra åtgärder för att minimera riskerna för de registrerade.

Dataskyddsombudet bedömer att förvaltningen har bra arbetssätt för att genomföra tröskelanalyser och konsekvensbedömningar. Ett flertal tröskelanalyser och konsekvensbedömningar har genomförts under året. Dataskyddsombudet har löpande involverats i detta arbete.

Dataskyddsombudet rekommenderar förvaltningen att fortsätta arbetet med att kartlägga förvaltningens personuppgiftsbehandlingar och identifiera de behandlingar som kan innebära en hög risk för registrerades fri- och rättigheter. 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

[2] 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.

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. Det är i detta sammanhang mycket positivt att socialförvaltningarna gemensamt genomfört ett arbete med kartläggning av personuppgiftsbehandlingar med Treserva som informationsbärare. Det är ett viktigt första steg i det arbete som behöver bedrivas avseende personuppgiftsbehandlingarna som sker i Treserva och kartläggningen kan användas som underlag för arbetet med att ta fram en långsiktig planering för det fortsatta arbetet. Förvaltningen rekommenderas att samråda med dataskyddsombudet kring frågor om bland annat prioriteringar och lämpliga avgränsningar.

3.2.10 Kontrollpunkt 10: IT-projekt och upphandling

Verksamhetens skattning av risknivå

Dataskyddsombudets bedömning

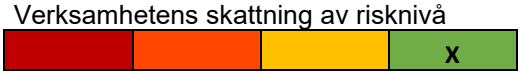
Verksamhetens resultat indikerar att verksamheten bedriver ett systematiskt dataskyddsarbete inom ramen för kontrollpunkten och att inga risker av betydelse föreligger.

Dataskyddsombudet delar verksamhetens 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. Dataskyddsombudet rekommenderar därför förvaltningen att fortlöpande granska hur dataskyddsperspektivet beaktas inom förvaltningen vid utveckling och införandet av nya IT-projekt/system och i samband med upphandling av system och tjänster. Detta för att kunna säkerställa, och vid behov vidareutveckla, ett arbetssätt som medför att skyddet för de registrerades fri- och rättigheter beaktas från början i arbetet med nya systemlösningar. Det är även viktigt att förvaltningens dataskyddskontakter informeras och vid behov involveras i arbetet med upphandling, utveckling och införandet av nya IT-projekt och system.

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. Detta för att förvaltningen ska kunna ta sitt ansvar som personuppgiftsansvarig i arbetet med IT-projekt och upphandling, oavsett om dessa bedrivs internt inom förvaltningen eller i samverkan med andra förvaltningar i staden.

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 verksamhetens 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.

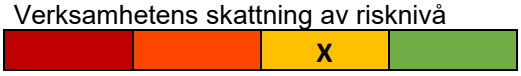
Eftersom IT-system och digitala verktyg är några av de främsta arbetsredskapen inom en verksamhet rekommenderar dataskyddsombudet förvaltningen att regelbundet följa upp och kontrollera så att personuppgiftshanteringen i IT-system och digitala verktyg sker i enlighet med de rutiner och riktlinjer som antagits inom förvaltningen. Förvaltningen behöver även säkerställa dataskyddsperspektivet vid införandet och användandet av kostnadsfria tjänster, så som gratis appar. Dataskyddsombudet har dock fått information om att det pågår ett arbete inom förvaltningen med att införa godkända appar för medarbetarna, vilket är positivt.

Dataskyddsombudet rekommenderar även förvaltningen att säkerställa att det finns dokumenterade arbetssätt för tilldelning av behörigheter och åtkomster till samtliga av förvaltningens IT-system, samt att kontroller görs så att behörigheterna är korrekta och anpassade. Dataskyddsombudet lyfter detta mot bakgrund av 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[3] som förväntas träda i kraft under 2024. Det här behöver förvaltningen beakta i arbetet med tilldelning av behörigheter och åtkomster till de IT-system som omfattas av den här lagstiftningen. Avseende behörigheter och åtkomster till verksamhetssystemet Treserva genomförde dataskyddsombudet en fördjupad kontroll 2022, vilken redogörs för under avsnitt 3.3.1 nedan.

[3] Ny 10 § lag (2001:454) om behandling av personuppgifter inom socialtjänsten.

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.

Förvaltningen har dokumenterade arbetssätt på plats avseende flertalet av de rättigheter som de registrerade kan åberopa. Dataskyddsombudet rekommenderar dock förvaltningen att säkerställa att de har alla rutiner på plats som behövs för att garantera en korrekt och rättssäker hantering av de registrerades rättigheter. Ytterligare en åtgärd som förvaltningen rekommenderas vidta för att säkerställa de registrerades rättigheter är att genom bland annat utbildning och informationsinsatser se till så att förvaltningens medarbetare har kunskap om de registrerades rättigheter och i vilka fall de begränsas.

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.

Kontroll (2022): Behörighetsstyrning

Verksamheten gavs följande rekommendationer:

- Förvaltningen rekommenderas säkerställa att uppföljning av tilldelade behörigheter i Treserva genomförs i enlighet med beslutade rutiner.
- Förvaltningen rekommenderas att arbeta för att minimera risken för felaktiga behörigheter vid personalförändringar och att det sker i direkt anslutning till att en medarbetare exempelvis byter tjänst.
- Förvaltningen rekommenderas att fortsätta arbetet med att ta fram rutiner för åtkomstkontroll/logguppföljning. Berörda medarbetare måste sedan informeras om gällande rutiner.
- Förvaltningen rekommenderas att ge personuppgiftsbiträdet dokumenterade instruktioner.

- Förvaltningen rekommenderas att se över behovet av konsekvensbedömning för behandlingarna i systemet, eftersom det då kan identifieras risker med för vida behörigheter.

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[4] som förväntas träda i kraft under 2024, kommer förvaltningen att behöva arbeta mer aktivt med behörighetstilldelning i IT-system som omfattas av den här lagstiftningen. Dataskyddsombudet kommer därför 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 under året, i dialog med förvaltningen.

[4] Ny 10 § lag (2001:454) om behandling av personuppgifter inom socialtjänsten.

4 Rekommenderade fokusområden 2024

Utifrån höga föreliggande risker för de registrerades fri- och rättigheter har dataskyddsombudet identifierat ett antal områden som förvaltningen 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 förvaltningen.

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 uppgifterna innehåller all obligatorisk information om behandlingarna som krävs enligt artikel 30 i GDPR. Förvaltningen behöver ha ett fungerande arbetssätt för att hålla registret uppdaterat och korrekt.

- Kontrollpunkt 6: Utbildning
  Kartlägg utbildningsbehovet inom dataskydd och ta fram en långsiktig utbildningsplan.

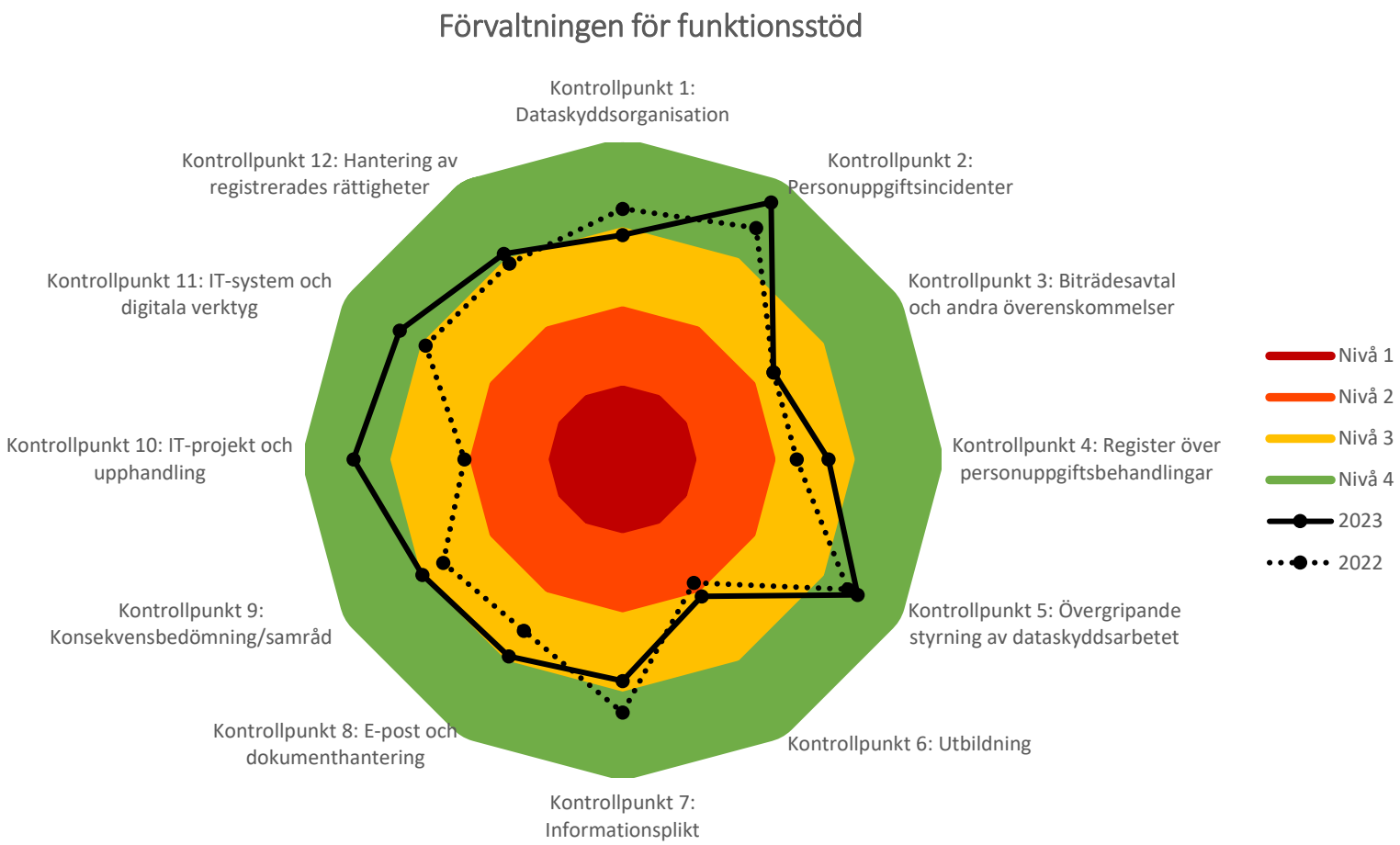
- Kontrollpunkt 9: Konsekvensbedömning/samråd
  Kartlägg samtliga personuppgiftsbehandlingar som innebär en hög risk för de registrerades fri- och rättigheter och ta fram en handlingsplan för att på sikt säkerställa att konsekvensbedömningar genomförs för samtliga behandlingar där detta krävs.

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

Förvaltningen för funktionsstöd

Kontrollplan för dataskyddsarbetet 2023–2024

2023-02-07

Innehåll

1 Bakgrund

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

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

1.1 Ny utformning av kontrollarbetet

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

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

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

2 Kontrollarbetet 2023–2024

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

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

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

2.1 Kontrollarbetets delar

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

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

2.2 Tidplan för kontrollarbetet 2023–2024

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

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

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

3 Kontroller

3.1 Fasta kontrollpunkter

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

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

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

För beskrivning av de fasta kontrollpunkterna, se bilaga 1.

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

3.2 Fördjupad kontroll

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

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

3.3 Uppföljning av genomförda kontroller

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

4 Rapportering

4.1 Årsrapport

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

4.2 Särskilt yttrande

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

5 Kontakt

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

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

Bilaga 1 - Beskrivning av fasta kontrollpunkter

Kontrollpunkt 1: Dataskyddsorganisation

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

Kontrollpunkt 2: Personuppgiftsincidenter

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

Kontrollpunkt 3: Biträdesavtal och andra överenskommelser

Kontrollpunkten avser verksamhetens dokumentation av biträdesavtal och andra överenskommelser gällande dataskydd och förutsätter att verksamheten har identifierat samt registrerat personuppgiftsbiträden i personuppgiftsregistret. Även verksamhetens rutiner för uppdatering och uppföljning av tecknade biträdesavtal innefattas.

Kontrollpunkt 4: Register över personuppgiftsbehandlingar

Kontrollpunkten avser verksamhetens efterlevnad av skyldigheten att systematiskt dokumentera alla personuppgiftsbehandlingar i form av ett register. Även verksamhetens arbete med, och rutin för, att säkerställa ett uppdaterat och heltäckande register innefattas.

Kontrollpunkt 5: Övergripande styrning av dataskyddsarbetet

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

Kontrollpunkt 6: Utbildning

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

Kontrollpunkt 7: Informationsplikt

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

Kontrollpunkt 8: E-post och dokumenthantering

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

Kontrollpunkt 9: Konsekvensbedömning/samråd

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

Kontrollpunkt 10: IT-projekt och upphandling

Kontrollpunkten avser verksamhetens organisation och rutiner för hantering av dataskyddsfrågor inom IT-projekt och upphandling. I detta ingår till exempel hur verksamheten integrerar dataskyddsfrågor i arbetet med upphandling av nya, samt utvecklingen av, befintliga system och tjänster.

Kontrollpunkt 11: IT-system och digitala verktyg

Kontrollpunkten avser verksamhetens rutiner för att säkerställa att verksamhetens personuppgiftshantering inom ramen för IT-system och digitala verktyg är förenlig med dataskyddslagstiftningen. Rutin för att säkerställa och kontrollera att dessa system/tjänster uppfyller kraven på dataskydd ingår även.

Kontrollpunkt 12: Hantering av registrerades rättigheter

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