Göteborgs Stad

Årsrapport för dataskyddsarbetet 2023

Valnämnden

2023-12-18

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.	

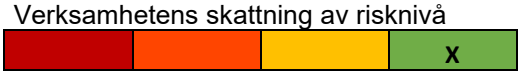
3.2 Resultat från kontrollen 2023

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 verksamheten bedriver ett systematiskt dataskyddsarbete inom ramen för kontrollpunkten och att inga risker av betydelse föreligger. Resultatet innebär en marginell sänkning jämfört med förra årets skattning.

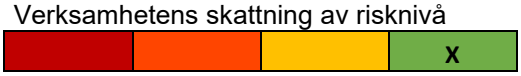
Dataskyddsombudet har inte fått några direkta indikationer som medför en annan bedömning än den som förvaltningen har gjort, men har inte heller kontrollerat dataskyddsorganisationen särskilt. Även inom verksamheter med eventuella låga risker krävs det kontinuerliga insatser för att ett systematiskt dataskyddsarbete ska kunna upprätthållas och stärkas ytterligare.

Vid muntlig avstämning i oktober har dataskyddskontakterna berättat följande. Valkansliet är en liten organisation och därför kan dataskyddsregleringen och kraven i den upplevas som relativt krävande. Det finns dock vilja och engagemang att jobba med frågorna. Även om saker och ting och arbetssätt gällande dataskyddsorganisationen inte finns nedtecknade så upplever man att det finns en tydlighet och en bra kommunikation internt kring dataskyddsarbetet.

Verksamheten har angett en trea på delfrågan om att verksamheten har tillräckliga resurser för att kunna bedriva ett systematiskt dataskyddsarbete. Dataskyddsombudet delar inte helt verksamhetens bedömning vad gäller tillräckliga resurser, men ser att det finns ett systematiskt angreppssätt hos dataskyddskontakterna. Dataskyddsombudet rekommenderar att förvaltningen fortsätter det goda arbetet och tar stöd av dataskyddsombudet när så är behövligt. Vidare rekommenderar dataskyddsombudet att verksamheten fortsätter att vidta åtgärder för att implementera dataskyddsarbetet på bredden så att frågorna och perspektivet blir integrerat i det dagliga arbetet.

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. Resultatet innebär en marginell höjning jämfört med förra årets skattning.

Förutom att dataskyddsombudet har rådfrågats i samband med en incident som gällde en kommungemensam tjänst så har dataskyddsombudet under året inte

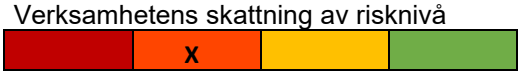
involverats i någon ytterligare konkret fråga kopplad till kontrollpunkten, varför dataskyddsombudet inte kan göra någon självständig bedömning. Även inom verksamheter med eventuella låga risker krävs det kontinuerliga insatser för att ett systematiskt dataskyddsarbete ska kunna upprätthållas och stärkas ytterligare.

Vid genomgång av årsrapporten för dataskyddskontakterna i november har följande framkommit. Det finns en rutin för personuppgiftsincidenter och den har kommunicerats med medarbetare och nämnd.

Som en upprepning av föregående års rekommendation, rekommenderar dataskyddsombudet att verksamheten deltar i och/eller vidtar informations- och utbildningsinsatser för att medarbetare ska kunna identifiera personuppgiftsincidenter och så att de vet vad de behöver göra. Dataskyddsombudet har under året skickat ut ett frågebatteri (i samband med ett nyhetsbrev) som bygger på artikel 29-gruppens/EDPB:s riktlinje om anmälan av personuppgiftsincidenter.[2] Frågorna är tänkta att användas för att bedöma risk i samband med en personuppgiftsincident och innehåller olika faktorer som man bör ta i beaktan för att bedöma incidenten svårighetsgrad och sannolikhet för att de registrerades fri- och rättigheter påverkas negativt. Dataskyddsombudet rekommenderar att förvaltningen införlivar dessa frågor i sin modell för riskbedömning.

3.2.3 Kontrollpunkt 3: Biträdesavtal och andra överenskommelser

Verksamhetens skattning av risknivå



Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger omfattande risker som kräver omgående åtgärder. Resultatet innebär en sänkning jämfört med förra årets skattning.

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

Förutom de kommungemensamma tjänsterna så har verksamheten berättat att det finns två verksamhetsspecifika personuppgiftsbiträdesrelationer. Den en gäller systemet Kaskelot och den andra gäller demokrati och medborgarservices kontaktcenters hantering av utskrift av dubblettröstkort. Vi muntlig avstämning i oktober har dataskyddskontakterna uppgett att det finns PUB-avtal för båda.

Dataskyddsombudet rekommenderar att förvaltningen följer upp och säkerställer att den behandling som utförs av biträdena inom ramen för Kaskelot respektive dublettröstkortshanteringen, är förenlig med GDPR. Vad gäller PUB-avtalet

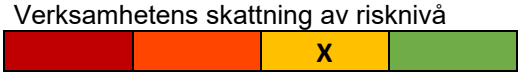
[2] Riktlinjer om anmälan av personuppgiftsincidenter enligt förordning (EU) 2016/679 s. 24-27, Tillgänglig: wp250rev_en (imy.se).

gällande Kaskelot så är detta från ”PUL-tiden”[3] och därför rekommenderar dataskyddsombudet att verksamheten vidtar åtgärder för att uppdatera avtalet samt att man lämnar instruktioner till biträdet. Vad gäller dublettkortshanteringen så rekommenderar dataskyddsombudet att verksamheten reder ut eventuella frågetecken gällande ansvarsfrågan tillsammans med demokrati och medborgarservice.

Utifrån förvaltningens lämnade svar rekommenderar dataskyddsombudet att förvaltningen tar sig till kunskap för att bättre kunna bedöma ansvar och roller (vem som är personuppgiftsansvarig och personuppgiftsbiträde samt om det förekommer gemensamt personuppgiftsansvar). Utifrån förvaltningens skattning i enkäten rekommenderar dataskyddsombudet att förvaltningen även utreder vad som behövs göras för att förvaltningen bättre ska leva upp till ansvarsskyldigheten som personuppgiftsansvarig. Det gäller både frågan om att genomföra efterlevnadskontroller av personuppgiftsbiträden, samt att bedöma hela kedjan av underbiträden. Förvaltningen rekommenderas vidta åtgärder för att åstadkomma en sådan förbättring och att dokumentera arbetssättet.

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. Resultatet innebär en betydande höjning jämfört med förra årets skattning. I årsrapporten för 2022 rekommenderade dataskyddsombudets att förvaltningen skulle prioritera den här kontrollpunkten.

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.

Dataskyddskontakterna har informerat dataskyddsombudet om att man har tagit in en konsult för att ”ta ett helhetsgrepp” om verksamhetens dokument- och ärendehantering och att behandlingsregistret ingår som en del i detta arbete. Dataskyddsombudet har därefter i oktober deltagit i ett möte gällande behandlingsregistret tillsammans med konsulten och en dataskyddskontakt. Under mötet diskuterades bland annat frågan om definition och avgränsning av behandlingar och dataskyddsombudet gav råd kopplat till detta. Ett utkast på behandlingsregister har presenterats för dataskyddsombudet i slutet på november,

[3] Personuppgiftslagen som förkortas PUL är den lag som gällde före GDPR.

men i skrivandets stund har återkoppling ännu inte kunnat ske, varför ingen bedömning heller kan presenteras i den här årsrapporten.

Dataskyddsombudet ser positivt på att arbetet har inletts och rekommenderar förvaltningen att arbeta vidare med frågan och att framgent använda behandlingsregistret som ett verktyg i det löpande dataskyddsarbetet. Behandlingsregistret kan till exempel användas för att identifiera behandlingar som sannolikt innebär hög risk för de registrerades fri- och rättigheter (d.v.s. behandlingar som behöver konsekvensbedömmas). Behandlingsregistret ger också den personuppgiftsansvarige grundläggande förutsättningar att tillgodose de registrerades fri- och rättigheter. Dataskyddombudet rekommenderar att förvaltningen checkar av behandlingsregistret och integritetspolicyn mot varandra så att informationen stämmer överens. Som ett nästa steg rekommenderar dataskyddsombudet att verksamheten antar ett dokumenterat arbetssätt för att hålla registret uppdaterat.

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. Resultatet innebär inga förändringar jämfört med förra årets skattning.

Dataskyddsombudet har inte fått några direkta indikationer som medför en annan bedömning än den som förvaltningen har gjort, men har inte heller kontrollerat den övergripande styrningen särskilt.

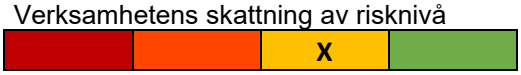
Utifrån verksamhetens skattning i enkäten rekommenderar dataskyddsombudet att verksamheten utvärderar på vilket sätt verksamheten kan göra interna kontroller för att säkerställa följsamhet gentemot GDPR. Kontroller kan vara ett sätt att identifiera utvecklingsområden, öka medvetenhet bland medarbetare, skapa systematik i dataskyddsarbetet och är ett bland många verktyg för att leda och styra en organisation. Dataskyddsombudet rekommenderar därför att verksamheten identifierar områden som är meningsfulla, rimliga och möjliga att kontrollera. Verksamheten rekommenderas att sätta upp en tidsplan och att verkställa kontrollen/kontrollerna. I valet av kontrollområden kan verksamheten förslagsvis hämta vägledning från kontrollpunkterna och rekommendationerna som ges i den här årsrapporten. Det kan vara så väl kontroller som utförs punktvis som löpande kontroller.

Verksamheten har inte kunnat svara på frågan om hur stor andel av verksamhetens informationstillgångar som har identifierats och värderats utifrån K/R/T i enlighet med stadens styrande dokument. Mot bakgrund av detta rekommenderas

verksamheten att framåt ta fram en handlingsplan för arbetet med informationsklassning, som ett led i att tillförsäkra rätt nivå av skydd för personuppgifter.

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. Resultatet innebär en höjning jämfört med förra årets skattning.

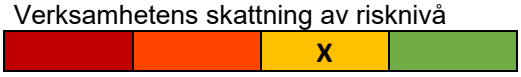
Dataskyddsombudet har inte involverats i några konkreta frågor kopplat till kontrollpunkten, men har ingen anledning att göra en annan bedömning än den som verksamheten har gjort avseende risknivå.

Vid muntlig avstämning med dataskyddskontakterna i oktober har följande framkommit. Det ingår numera i introduktionspaketet för projektanställda att man ska gå dataskyddsenhetens grundkurs i dataskydd. För de personer som är fastanställda efterfrågas möjlighet till kompetenshöjning.

Utifrån förvaltningens skattning i enkäten och som en allmän rekommendation rekommenderar dataskyddsombudet att förvaltningen gör en analys av kunskapsnivån och kunskapsbehovet inom verksamheten utifrån olika roller, ansvar och arbetsuppgifter, samt gör upp en plan för att delta i och/eller vidta informations- och utbildningsinsatser och för att möta dessa behov.

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. Resultatet innebär en sänkning jämfört med förra årets skattning. I årsrapporten för 2022 rekommenderade dataskyddsombudets att förvaltningen skulle prioritera den här kontrollpunkten. Integritetspolicyn var även föremål för fördjupad kontroll under 2022 och har följts upp särskilt i den här årsrapporten (se längre fram vid avsnitt 3.3 om uppföljning).

Dataskyddsombudet delar verksamhetens bedömning om att det finns risker som behöver åtgärdas. Dataskyddskontakterna har under året tagit fram en integritetspolicy och dataskyddsombudet har lämnat rekommendationer kopplat till den. Integritetspolicyn har i skrivandets stund ännu inte publicerats.

Dataskyddsombudet ser positivt på det arbete som har inletts och uppmuntrar verksamheten att fortsätta vidta åtgärder kopplat till informationsplikten. Trots det goda arbetet med den externa integritetspolicyn vill dataskyddsombudet i sammanhanget lyfta att kontrollpunkten i år har ändrats från att fokusera på integritetspolicyn till att avse informationsplikten i stort. Informationsplikten är långtgående och omfattar mer än den externa integritetspolicyn.

Dataskyddsombudet vill påminna om den informationsinsats som dataskyddsenheten höll på temat informationsplikten och det informationsmaterial som togs fram i samband med detta. Förvaltningen rekommenderas att läsa materialet, utvärdera i vilken mån förvaltningen lever upp till kraven och att vidta eventuella förbättringsåtgärder. Informationsplikten handlar som sagt inte bara handlar om att ha en integritetspolicy på hemsidan. Det finns även vissa kvalitativa krav kopplat till hur information förmedlas, när den ska informeras och att den verkligen ska nå fram till den registrerade. Information kan behöva förmedlas på olika sätt i olika sammanhang. Slutmålet är med andra ord inte att ta fram en informationstext, utan snarare att den registrerade verkligen får kunskap om behandlingen så att den registrerade i förlängningen kan utöva sina rättigheter.

Eftersom verksamheten har ett pågående arbete med att identifiera behandlingar för att ta upp i behandlingsregistret så räknar dataskyddsombudet med att verksamheten kommer att behöva ta ett omtag i frågan om informationsplikten vad gäller eventuella nya och omdefinierade behandlingar som identifierats. Dataskyddombudet rekommenderar att förvaltningen checkar av behandlingsregistret och integritetspolicyn mot varandra så att informationen stämmer överens.

3.2.8 Kontrollpunkt 8: E-post och dokumenthantering

Verksamhetens skattning av risknivå

	X		

Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger omfattande risker som kräver omgående åtgärder. Resultatet innebär en marginell höjning jämfört med förra årets skattning. I årsrapporten för 2022 rekommenderade dataskyddsombudets att förvaltningen skulle prioritera den här kontrollpunkten.

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

Denna kontrollpunkt innehåller bland annat delfrågor om dokumenthantering och informationsklassning. Som tidigare nämnts vid kontrollpunkt fyra så har verksamheten tagit in en konsult för att ”ta ett helhetsgrepp” om verksamhetens dokument- och ärendehantering. Utöver detta så har dataskyddsombudet inte fått närmare inblick i verksamhetens arbete med kontrollpunkten.

Dataskyddsombudet uppmuntrar förvaltningen att fortsätta arbetet med att ta fram en uppdaterad dokumenthanteringsplan och att informationsklassa personuppgifter och rekommenderar att förvaltningen drar nytta av detta i dataskyddsarbetet. Även om dokumenthanteringsplanen och informationsklassningen inte är direkta krav utifrån GDPR, utan snarare krav utifrån annan lagstiftning så är dessa verktyg meningsfulla i arbetet med dataskydd. Dokumenthanteringsplanen kan hjälpa verksamheten i arbetet med behandlingsregistret och för att få överblick på vilka personuppgifter som kan förekomma i olika handlingar och sammanhang. Informationsklassningsarbetet kan hjälpa verksamheten att få en enhetlig och säker hantering vad gäller personuppgifter som är av liknande art och känslighet.

Utifrån verksamhetens skattning rekommenderar dataskyddsombudet att verksamheten antar ett dokumenterat arbetssätt för hur personuppgifter får hanteras i e-post.

3.2.9 Kontrollpunkt 9: Konsekvensbedömning/samråd

Verksamhetens skattning av risknivå

X			

Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger höga risker som omgående kräver insatser av ledning och/eller övriga verksamheten. Resultatet innebär en betydande sänkning jämfört med förra årets skattning.

Dataskyddsombudet delar verksamhetens bedömning om att det inom kontrollpunkten föreligger höga risker som omgående kräver insatser ifrån ledningsnivå.

Dataskyddsombudet upprepar rekommendationen från årsrapporten för 2022 om att förvaltningen behöver vidta åtgärder kopplat till kontrollpunkten. Som tidigare nämnts är ett tips att förvaltningen använder sig av behandlingsregistret för att identifiera behandlingar som sannolikt innebär hög risk för de registrerades fri- och rättigheter. Verksamheten rekommenderas ta fram en genomförandeplan för arbetet med tröskelanalyser och konsekvensbedömningar.

Dataskyddskontakterna har vid muntlig avstämning i oktober uppgett att man behöver mer kunskap i frågan för att kunna göra framsteg. Dataskyddsombudet har tipsat om dataskyddsenhetens mall och mallstöd för tröskelanalyser och konsekvensbedömningar.

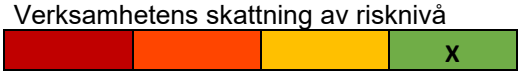
Kravet på att genomföra konsekvensbedömningar infaller när det är sannolikt att en behandling leder till hög risk för de registrerades fri- och rättigheter. I GDPR står det utskrivet omständigheter som typiskt sett leder till hög risk. Den svenska tillsynsmyndigheten har tagit fram en lista med ytterligare omständigheter som typiskt sett leder till hög risk. Baserat på dessa typexempel har dataskyddsenheten tagit fram något som dataskyddsenheten kallar en ”tröskelanalys”. Vid osäkerhet

om en behandling behöver konsekvensbedömmas rekommenderar dataskyddsombudet att förvaltningen genomför en tröskelanalys.

Dataskyddsombudet rekommenderar att relevanta personer i verksamheten läser igenom dataskyddsenhetens mallstöd för tröskelanalyser och konsekvensbedömningar för att få kunskap om när skyldigheten att genomföra en konsekvensbedömning infaller och vilken information som behöver redogöras för i en konsekvensbedömning. Därefter rekommenderar dataskyddsombudet att verksamheten inleder arbetet med att kartlägga personuppgiftsbehandlingar som sannolikt innebär en hög risk och att verksamheten tar fram en handlingsplan för att påbörja arbetet med att genomföra konsekvensbedömningar.

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. Resultatet innebär en betydande höjning jämfört med förra årets skattning.

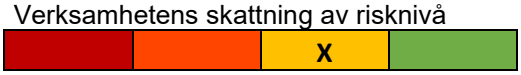
Dataskyddsombudet har under året inte involverats på djupet i några frågor kopplad till kontrollpunkten, varför dataskyddsombudet inte kan göra någon självständig bedömning. Även inom verksamheter med eventuella låga risker krävs det kontinuerliga insatser för att ett systematiskt dataskyddsarbete ska kunna upprätthållas och stärkas ytterligare.

I samband med muntlig avstämning i oktober har dataskyddskontakterna informerat dataskyddsombudet om att verksamheten har skaffat en ny applikation som ska kunna användas av invånare i samband med nästa val. Applikationen innebär att var och en kan skriva in adressuppgifter alternativt använda sig av sin aktuella position för att söka fram information om närmsta lokal för förtidsröstning. Dataskyddskontakterna har berättat att verksamheten tillsammans med Intraservice har genomfört en risk- och sårbarhetsanalys och klassning utifrån ett informationssäkerhetsperspektiv. Behandlingen har dock inte belysts utifrån ett dataskyddsperspektiv. Dataskyddsombudets preliminära analys är att det kan röra sig om personuppgiftsbehandling, i vart fall i den del som handlar om att använda aktuell position för att göra en sökning (användning av positioneringsteknik). Eftersom det verkar röra sig om positioneringsteknik rekommenderar dataskyddsombudet att förvaltningen utreder frågan närmare och genomför en konsekvensbedömning vid behov.

Dataskyddsombudet rekommenderar att verksamheten vidtar behövliga åtgärder för att säkerställa att dataskyddsperspektivet tas i beaktan på ett systematiskt sätt i samband med upphandling av nya system och vid utvecklandet av befintliga system.

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. Resultatet innebär en höjning jämfört med förra årets skattning.

Dataskyddsombudet har under året inte involverats i någon fråga kopplad till kontrollpunkten, varför dataskyddsombudet inte kan göra någon självständig bedömning.

Vid muntlig avstämning i oktober har dataskyddskontakterna uppgett att verksamheten inte använder sig av sociala medier utan använder sig främst av stadens kanaler för kommunikation.

Förvaltningen har inte kunnat svara på frågan om förvaltningens användning av cookies på verksamhetens webbsidor följer kraven enligt GDPR. Dataskyddsombudet rekommenderar därför förvaltningen att ta del av informationsmaterialet om cookies som dataskyddsenheten tog fram i samband med informationsinsatsen om informationsplikten. Vidare rekommenderar dataskyddsombudet att förvaltningen kartlägger användning av cookies, analyserar i vilken mån förvaltningen lever upp till kraven och att förvaltningen vidtar eventuella behövliga åtgärder för att leva upp till kraven.

Utifrån verksamhetens skattning rekommenderar dataskyddsombudet att verksamheten vidtar åtgärder för att få full överblick på samtliga IT-system och digitala verktyg och att verksamheten säkerställer att det finns målgruppsanpassad information för användarna.

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. Resultatet innebär en marginell höjning jämfört med förra årets skattning.

Förutom att dataskyddsombudet har gett marginalkommentarer på förvaltningens rutin och mall för registerutdrag så har dataskyddsombudet under året inte involverats i några ytterligare frågor kopplade till kontrollpunkten, varför dataskyddsombudet inte kan göra någon heltäckande självständig bedömning.

I samband med muntlig avstämning i oktober har dataskyddskontakterna uppgett att förfrågningar från de registrerade inte är så vanligt förekommande.

Mot bakgrund av att förvaltningen arbetar med att ta fram ett behandlingsregister ser dataskyddsombudet att förutsättningarna för att kunna hantera de registrerades fri- och rättigheter kommer att öka. Förutom att fortsätta med detta arbete så rekommenderar dataskyddsombudet att förvaltningen utvärderar och analyserar sitt nuvarande arbetssätt, de verktyg och dokument som finns till hands för att hantera de registrerades rättigheter. Verksamheten rekommenderas vidta konkreta åtgärder för att, ha en god beredskap att tillvarata de registrerades rättigheter i samband med konkreta förfrågningar. Verksamheten rekommenderas även utvärdera och vidta åtgärder för att i de konkreta personuppgiftsbehandlingarna kunna tillvara ta de registrerades fri- och rättigheter.

3.3 Uppföljning

3.3.1 Uppföljning av rekommendationer lämnade inom ramen för tidigare genomförda kontroller

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

Kontroll (2022): Integritetspolicyn

Verksamheten gavs följande rekommendationer:

- Förtydliga och beskriv vilka behandlingar som utförs i verksamheten och vilka personuppgifter som behandlas.
- Förtydliga rättslig grund för behandlingarna.
- Tydliggör lagringstid för respektive behandling.
- Säkerställ att samtliga behandlingar, där personuppgifterna inte samlas in direkt från den registrerade, kompletteras med information om kategorier av personuppgifter och var personuppgifterna kommer ifrån.
- Förtydliga vad som gäller avseende de registrerades rättigheter och specificera för respektive behandling.
- Förtydliga informationen om tredjelandsöverföring.
- Säkerställ att integritetspolicyn och informationen har ett tydligt språk och inte innehåller bestämningsord såsom ”kan” och liknande.
- Säkerställ att de registrerade har tillgång till en aktuell och uppdaterad integritetspolicy och gör policyn tillgänglig på Stadens hemsida.
- Ta fram rutiner som beskriver hur integritetspolicyn hålls uppdaterad.

Kommentarer och rekommendationer:

Uppföljningen visar att verksamheten har vidtagit åtgärder i enlighet med rekommendationerna. Fortsatt uppföljning kommer ske inom ramen för de fasta kontrollpunkterna om ingen särskilt föranleder att det behöver följas upp separat.

Dataskyddsombudet vill här upprepa upplysningen om informationspliktens bredd samt de rekommendationer som getts vid kontrollpunkt sju om informationsplikten. Verksamheten behöver checka av integritetspolicyn mot behandlingsregistret så att de stämmer överens och verksamheten rekommenderas se över hanteringen av informationsplikten i stort.

4 Rekommenderade fokusområden 2024

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

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

- **Kontrollpunkt 3: Biträdesavtal och andra överenskommelser**

Utred vad som behövs göras för att förvaltningen bättre ska leva upp till ansvarsskyldigheten som personuppgiftsansvarig. Det gäller både frågan om att genomföra efterlevnadskontroller av personuppgiftsbiträden samt att bedöma hela kedjan av underbiträden. Vidta åtgärder för att åstadkomma en sådan förbättring och dokumentera arbetssättet. Uppdatera PUB-avtalet gällande Kaskelot. Red ut eventuella frågetecken gällande dublettkortshanteringen och ansvarsfrågan kopplat till detta, tillsammans med demokrati och medborgarservice.

- **Kontrollpunkt 9: Konsekvensbedömning/samråd**

Ta del av dataskyddsenhetens mallstöd för tröskelanalyser och konsekvensbedömningar för att få kunskap om när skyldigheten att genomföra en konsekvensbedömning infaller och vilken information som behöver redogöras för i en konsekvensbedömning. Inled arbetet med att kartlägga personuppgiftsbehandlingar som sannolikt innebär en hög risk. Ta fram en handlingsplan för att påbörja arbetet med att genomföra konsekvensbedömningar.

- **Kontrollpunkt 5: Övergripande styrning av dataskyddsarbetet**

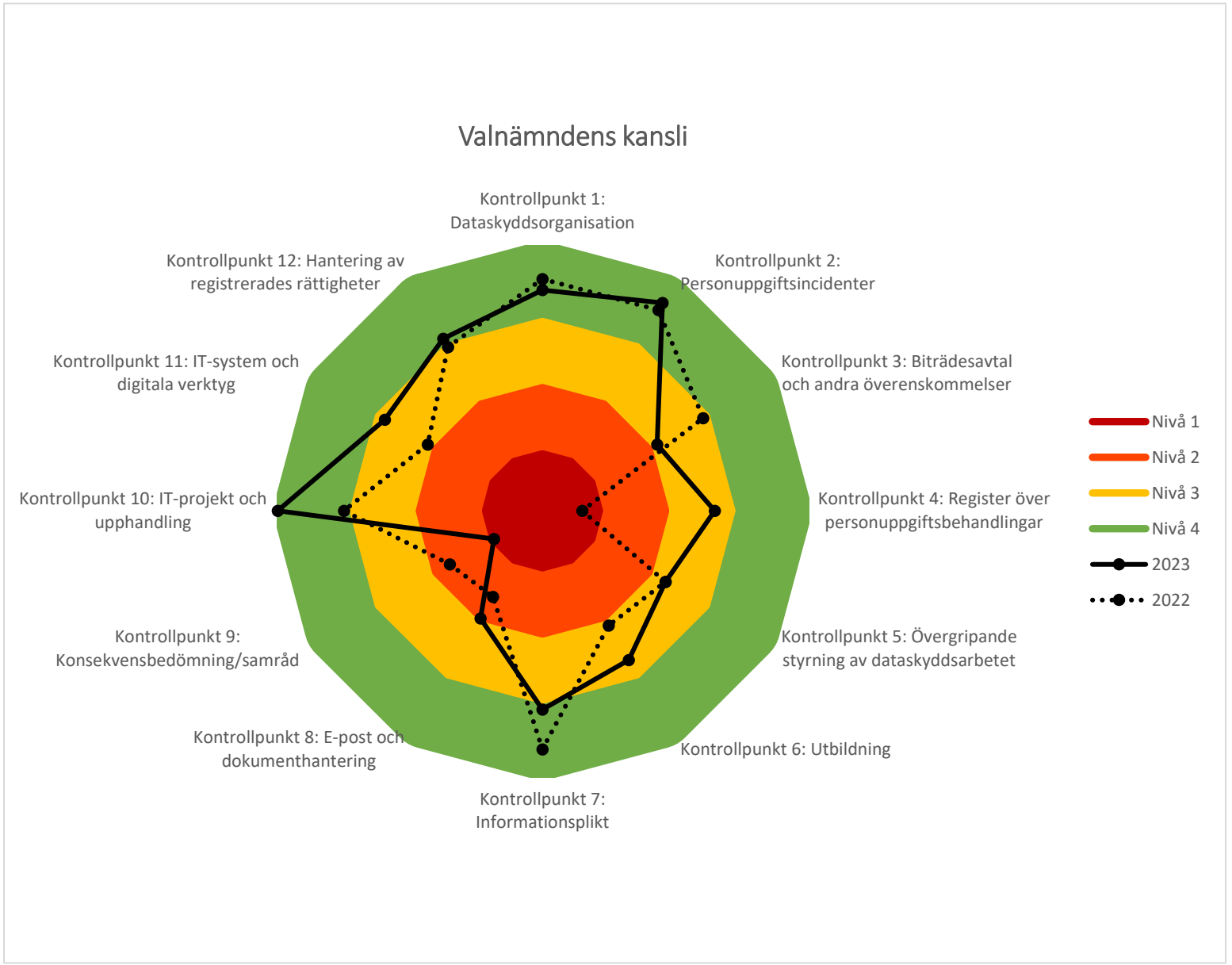
Utvärdera på vilket sätt verksamheten kan göra interna kontroller för att säkerställa följsamhet gentemot GDPR. Identifiera områden som är meningsfulla, rimliga och möjliga att kontrollera. Sätt upp en tidsplan och verkställ kontrollen/kontrollerna.

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

Valnämndens Kansli

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.