Göteborgs Stad

Årsrapport för dataskyddsarbetet 2023

Arkivnämnden

2023-12-18

Innehåll

1 Inledning 3

1.1 Dataskyddsombud i Göteborgs Stad 3

2 Särskilda iakttagelser 2023 4

2.1 Stadenövergripande 4

2.1.1 Förutsättningar för en hållbar digitalisering 4

3 Granskning av dataskyddsarbetet 2023 5

3.1 Kontroll av fasta kontrollpunkter 5

3.2 Resultat från kontrollen 2023 5

3.2.1 Kontrollpunkt 1: Dataskyddsorganisation 6

3.2.2 Kontrollpunkt 2: Personuppgiftsincidenter 6

3.2.3 Kontrollpunkt 3: Biträdesavtal och andra överenskommelser 8

3.2.4 Kontrollpunkt 4: Register över personuppgiftsbehandlingar 9

3.2.5 Kontrollpunkt 5: Övergripande styrning av dataskyddsarbetet 9

3.2.6 Kontrollpunkt 6: Utbildning 10

3.2.7 Kontrollpunkt 7: Informationsplikt 11

3.2.8 Kontrollpunkt 8: E-post och dokumenthantering 12

3.2.9 Kontrollpunkt 9: Konsekvensbedömning/samråd 13

3.2.10 Kontrollpunkt 10: IT-projekt och upphandling 14

3.2.11 Kontrollpunkt 11: IT-system och digitala verktyg 14

3.2.12 Kontrollpunkt 12: Hantering av registrerades rättigheter 15

3.3 Uppföljning 16

3.3.1 Uppföljning av rekommendationer lämnade inom ramen för tidigare genomförda kontroller 16

4 Rekommenderade fokusområden 2024 20

5 Bilagor 21

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.	

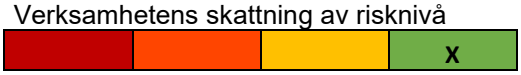
3.2 Resultat från kontrollen 2023

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.

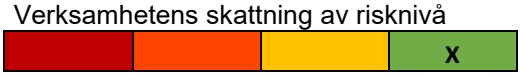
Dataskyddsombudet har inte fått några direkta indikationer som medför en annan bedömning än den som förvaltningen har gjort, men har inte heller kontrollerat dataskyddsorganisationen särskilt. Även inom verksamheter med eventuella låga risker krävs det kontinuerliga insatser för att ett systematiskt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

Dataskyddsombudet har vid muntlig avstämning med dataskyddskontakterna i oktober fått information om följande. I dagsläget är inte alla dataskyddskontakter lika mycket involverade i arbetet, men det finns en ambition och plan för att så ska ske. En delvis förklaring till aktuell situation är att visst grundarbete först behöver göras för att uppgifter sedan ska kunna delegeras vidare. Det finns en plan om att de olika dataskyddskontakterna, med stöd i dataskyddsenhetens grundutbildning, ska hålla utbildningar om dataskydd på sina olika respektive verksamhetsmöten. Dataskyddsombudet ser positivt på att verksamheten har en ambition och plan om ett mer breddat dataskyddsarbete och rekommenderar verksamheten att fullfölja dessa planer och ambitioner.

På delfrågan om huruvida dataskyddsfrågor når rätt nivå/befattning/roll och om det finns definierade rapporteringsvägar har förvaltningen skattat sig lägre jämfört med förra året. Mot bakgrund av detta rekommenderar dataskyddsombudet att förvaltningen analyserar vad det är som eventuellt kan bli bättre och att det vid behov vidtas åtgärder för att förbättra kommunikationen.

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 inga förändringar jämfört med förra årets skattning.

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 dock kontinuerliga

insatser för att ett systematiskt dataskyddsarbete ska kunna upprätthållas och stärkas ytterligare.

Dataskyddskontakterna har vid muntlig avstämning i oktober berättat att i samband med kommungemensamma incidenter så går informationen till förvaltningsbrevlådan och den förmedlas därefter vidare till en huvudansvarig dataskyddskontakt samt till berörd informationsägare. Dataskyddskontakten påbörjar analysen, stämmer av med informationsägaren och vid behov även dataskyddsombudet. Huvudansvarig dataskyddskontakt har en utsedd back-up-person. Dataskyddsombudet ser det som positivt att det verkar finns en fastställd arbetsprocess i frågan.

Dataskyddskontakterna har vid samma muntliga avstämning medgett att verksamheten kan bli bättre på att identifiera interna personuppgiftsincidenter. De incidenter som faktisk uppmärksammas hanteras, vilket är bra, men det kan vara så att fler incidenter faktiskt inträffar men utan att de uppmärksammas. Mot bakgrund av detta rekommenderar dataskyddsombudet att förvaltningen kartlägger och följer upp kunskapsnivån gällande personuppgiftsincidenter och vidtar åtgärder för att höja den allmänna kunskapsnivån.

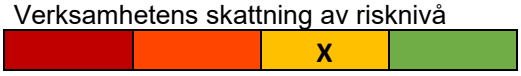
Ytterligare förbättringsåtgärder som dataskyddsombudet har identifierat och som skulle kunna vidtas inom ramen för kontrollpunkten gäller bland annat den modell för riskbedömning som förvaltningen använder sig av. Dataskyddsombudet har under året skickat ut ett frågebatteri som bygger på artikel 29-gruppens/EDPB:s 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 beakta för att bedöma incidenten svårighetsgrad och sannolikhet för att de registrerades fri- och rättigheter ska påverkas negativt. Dataskyddsombudet rekommenderar att förvaltningen införlivar dessa frågor i sin modell för riskbedömning.

Som ett led i det systematiska dataskyddsarbetet behöver förvaltningen regelbundet utvärdera sitt dokumenterade arbetssätt för hantering av personuppgiftsincidenter, samt se över och analysera tidigare inträffade incidenter för att kunna arbeta förebyggande. Dataskyddsombudet upprepar därför denna rekommendation som gällde även föregående år.

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

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. Resultatet innebär inga förändringar 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.

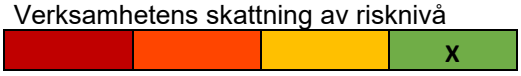
Verksamheten uppskattar att det finns tecknat personuppgiftsbiträdesavtal i 75 % av fallen. Vid muntliga avstämning i oktober har dataskyddskontakterna förklarat följande. Att man har skattat sig lågt på den här kontrollpunkten hänger delvis samman med oklarheterna kring de kommungemensamma tjänsterna och de tjänster som på annat sätt involverar en leverantör i staden. Eftersom ansvarsförhållandena inte är utredda är det svårt att leva upp till kraven enligt GDPR. Vad gäller övriga biträdesförhållanden är dataskyddskontakternas uppfattning att regelefterlevnaden är bättre.

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). Verksamheten rekommenderas att anta ett dokumenterat arbetssätt i frågan.

Utifrån förvaltningens skattning i enkäten rekommenderar dataskyddsombudet att förvaltningen även utreder vad som behöver 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 verksamheten bedriver ett systematiskt dataskyddsarbete inom ramen för kontrollpunkten och att inga risker av betydelse föreligger. Resultatet innebär inga förändringar jämfört med förra årets skattning.

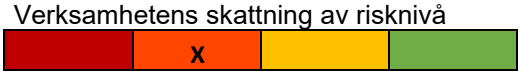
Dataskyddsombudet delar verksamhetens bedömning och anser att verksamheten har ett systematiskt arbete inom kontrollpunkten och inga risker av betydelse föreligger. Även inom verksamheter med låga risker krävs det dock kontinuerliga insatser för att ett systematiskt dataskyddsarbete ska kunna upprätthållas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

Dataskyddsombudet har genom muntlig avstämning med dataskyddskontakterna i oktober fått veta följande. Behandlingsregistret bygger på klassificeringsstrukturen. Eftersom det har skett uppdateringar vad gäller klassificeringsstrukturen så behövs det göras följdändringar i behandlingsregistret. Ett arbete pågår därför med att uppdatera behandlingsregistret. I behandlingsregistret har verksamheten angett flera olika deländamål under ändamålet arkivändamål av allmänt intresse och verksamheten har på så sätt beskrivit ändamålet och uppgifterna mer i detalj. Dataskyddsombudet ser positivt på detta eftersom det klargör ramarna för förvaltningens behandlingar.

Verksamheten har skattat att 75 % av behandlingarna finns upptagna i behandlingsregistret. Dataskyddsombudet rekommenderar att förvaltningen fortsätter arbetet med behandlingsregistret för att få det komplett. Vidare rekommenderar dataskyddsombudet att verksamheten vidtar åtgärder för att säkerställa att registret hålls uppdaterat.

3.2.5 Kontrollpunkt 5: Övergripande styrning av dataskyddsarbetet

Verksamhetens skattning av risknivå



Dataskyddsombudets bedömning

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

Dataskyddsombudet har inte involverats i några 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 dataskyddsombudet fått följande information. Det pågår ett arbete med att införa en ny modell för informationssäkerhetsklassning. Förvaltningen har ”testklassat” information, men eftersom den nya modellen ännu inte har implementerats fullt ut återstår arbete att göra. Mot bakgrund av detta rekommenderas verksamheten framåt ta fram en handlingsplan för arbetet med informationsklassning, som ett led i att tillförsäkra rätt nivå av skydd för personuppgifter.

Utifrån verksamhetens skattning i enkäten rekommenderar dataskyddsombudet att verksamheten antar en övergripande strategi för dataskyddsarbetet samt vidtar åtgärder för att kunna arbeta riskbaserat.

Vidare, 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 sätta upp en tidsplan och att genomföra 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.

Utifrån verksamhetens skattning i enkäten rekommenderar dataskyddsombudet även att förvaltningen antar ett internt styrande dokument för behandling av personuppgifter som på en övergripande nivå anger principer för hur man inom organisationen ska hantera personuppgifter vad gäller skydd av bland annat IT-system, datorer och mobila enheter. Verksamheten bör ha dokumenterat hur medarbetare ska hantera IT-system, datorer och mobila enheter och hur dessa får användas i det dagliga arbetet. Det kan exempelvis handla om lösenordrutiner och appanvändning.

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 inga förändringar jämfört med förra årets skattning.

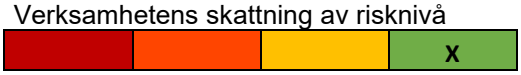
Dataskyddsombudet har inte involverats i några konkreta frågor kopplat till kontrollpunkten, men har ingen anledning att göra en annan bedömning än den som verksamheten har gjort avseende risknivå.

Vid muntlig avstämning med dataskyddskontakterna i oktober har dataskyddskontakterna berättat om planerade interna utbildningar (se beskrivning vid kontrollpunkt ett). Som tidigare nämnts så rekommenderar dataskyddsombudet att verksamheten fullföljer dessa intentioner. Dataskyddskontakterna har även identifierat personuppgiftsincidenter som ett möjligt tema för informations-/utbildningsinsats.

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 utbildnings- och informationsinsatser för att möta dessa behov.

3.2.7 Kontrollpunkt 7: Informationsplikt

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 under året inte involverats i någon fråga kopplad till kontrollpunkten, varför dataskyddsombudet inte kan göra någon självständig bedömning. Dataskyddsombudet vill dock 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 ta del av materialet samt utvärdera i vilken mån verksamheten lever upp till dessa krav och vidta eventuella förbättringsåtgärder. Informationsplikten handlar som sagt inte bara om att ha en integritetspolicy på hemsidan. Det finns även vissa kvalitativa krav kopplat till hur informationen förmedlas, när den ska förmedlas 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.

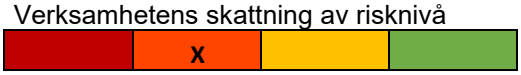
I samband med muntlig avstämning i oktober har dataskyddskontakterna uppgett att man inte har uppdaterat integritetspolicyn under året. Detta behöver förstås mot

bakgrund av att man fortfarande arbetar med behandlingsregistret. Informationen i integritetspolicyn behöver stämmas av mot informationen som framgår ur det nya behandlingsregistret. Dataskyddsombudet rekommenderar att verksamheten fortskrider i arbetet med behandlingsregistret och efter hand uppdaterar integritetspolicyn utifrån det uppdaterade registret.

I årsrapporten för 2022 kommenterade dataskyddsombudet informationsplikten kopplat till användningen av sociala medier. Eftersom frågan om sociala medier också tas upp inom ramen för uppföljningen av fördjupad kontroll finns kommentarerna kring detta samlade vid avsnittet 3.3 om uppföljning.

3.2.8 Kontrollpunkt 8: E-post och dokumenthantering

Verksamhetens skattning av risknivå



Dataskyddsombudets bedömning

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

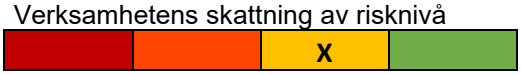
Dataskyddsombudet har inte involverats i några konkreta frågor kopplat till kontrollpunkten, men har ingen anledning att göra en annan bedömning än den som verksamheten har gjort avseende risknivå.

Verksamheten har inte kunnat svara på frågan om hur stor andel av verksamhetens personuppgiftsbehandlingar som har informationsklassificerats utifrån Göteborgs Stads riktlinje för informationssäkerhet. Som tidigare nämnts vid kontrollpunkt fem har verksamheten dock påbörjat ett arbete med att införa en ny modell för informationssäkerhetsklassning. Dataskyddsombudet upprepar rekommendationen om att ta fram en handlingsplan för arbetet med informationsklassning som ett led i att tillförsäkra rätt nivå av skydd för personuppgifter. Dataskyddsombudet rekommenderar verksamheten att dra nytta av informationssäkerhetsarbetet i arbetet med dataskydd. Även om informationsklassningen inte är direkta krav utifrån GDPR, utan snarare krav utifrån annan reglering så är dessa verktyg meningsfulla i arbetet med dataskydd. Informationsklassningsarbetet kan till exempel hjälpa verksamheten att få en enhetlig och säker hantering vad gäller personuppgifter som är av liknande art och känslighet.

Utifrån verksamhetens skattning i enkäten rekommenderar dataskyddsombudet att verksamheten antar ett dokumenterat arbetssätt för att kontrollera att handlingar som innehåller personuppgifter gallras enligt gällande gallringsbeslut.

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. Resultatet innebär en höjning jämfört med förra årets skattning.

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

Den som är personuppgiftsansvarig är skyldig att genomföra konsekvensbedömningar för behandlingar som sannolikt leder till hög risk för fysiska personers fri- och rättigheter. Detta ska göras innan behandlingar påbörjas. Den som är personuppgiftsansvarig ska även rådfråga dataskyddsombudet vid genomförandet av dessa konsekvensbedömningar.

Mot bakgrund av förvaltningens hantering i det konkreta fallet med tröskelanalysen ”Stöd för hantering av objekt och samlingar” (avseende KulturIT:s tjänster Primus och Digitalt Museum), rekommenderar dataskyddsombudet att förvaltningen utvärderar sitt arbetssätt vad gäller tröskelanalyser och konsekvensbedömningar. Dataskyddsombudet uppmuntrar verksamheten att ha en öppen dialog med dataskyddsombudet och att inte vara rädda för frågor som ställs. En bidragande orsak till rekommendationen om att verksamheten skulle genomföra en konsekvensbedömning var att behandlingen inte hade beskrivits tillräckligt utförligt för att dataskyddsombudet eller någon annan utomstående skulle kunna förstå behandlingens utformning. Att genomföra en konsekvensbedömning är alldeles oavsett riskernas nivå ett sätt att förebygga risker och att få överblick på verksamhetens personuppgiftsbehandlingar. Mycket av den information som redogjordes för i förvaltningens tjänsteutlåtande[3] hade sannolikt ingått i en konsekvensbedömning. Dataskyddsombudet rekommenderar förvaltningen att framgent fortsätta gå på djupet i frågor som rör förvaltningens behandlingar.

Även utifrån förvaltningens hantering i det konkreta fallet med tröskelanalysen avseende ”Digitala navet”, rekommenderar dataskyddsombudet att förvaltningen utvärderar sitt arbetssätt och vidtar åtgärder för att säkerställa att dataskyddsombudets synpunkter inhämtas i god tid och att utredningar om behandlingar görs innan avgörande beslut fattas och behandlingar påbörjas.

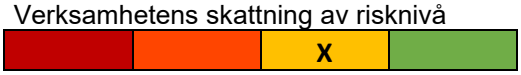
Vid genomgång av årsrapporten i december har dataskyddskontakterna berättat följande. I arbetet med behandlingsregistret så kommer verksamheten att fastställa ansvariga informationsägare kopplat till de olika behandlingarna. Det kommer att tydliggöras vad informationsägaren behöver göra bland annat kopplat till arbetet

[3] Se tjänsteutlåtande ”Behandling av personuppgifter i Primus och DigitaltMuseum”, Dnr. AN-07382/22.

med konsekvensbedömningar och tröskelanalyser. Dataskyddsombudet ser positivt på detta och uppmuntrar förvaltningen i detta.

3.2.10 Kontrollpunkt 10: IT-projekt och upphandling

Verksamhetens skattning av risknivå



Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger risker som behöver åtgärdas, men att dessa inte är brådskande, omfattande eller allvarliga. Resultatet innebär inga förändringar jämfört med förra årets skattning.

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

Vid avstämning med dataskyddskontakterna i oktober har dataskyddskontakterna medgett att förvaltningen rent allmänt kan bli bättre på att ha med GDPR-perspektivet i samband med utvecklandet av tjänster och att verksamheten kan bli mer systematisk detta arbete.

Mot bakgrund av det som dataskyddskontakterna själva uppgett, de indikationer som dataskyddsombudet har fått under året och som en delvis upprepning av rekommendationen som gavs vid föregående kontrollpunkt (kontrollpunkt nio om konsekvensbedömningar) rekommenderar dataskyddsombudet följande. Verksamheten rekommenderas utvärdera sitt arbetssätt vad gäller hantering av dataskyddsfrågor inom IT-projekt och upphandling. Vidare rekommenderas verksamheten vidta åtgärder för att säkerställa att dataskyddsperspektivet omhändertas på ett systematiskt sätt, att det finns med redan innan verksamheten ingår avtal och innan personuppgiftsbehandlingar inleds. Dataskyddsombudet rekommenderar också att förvaltningen vidtar åtgärder för att säkerställa att dataskyddsombudets involveras i god tid.

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. I årsrapporten för 2022 rekommenderade dataskyddsombudets att förvaltningen skulle prioritera den här kontrollpunkten.

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

Förvaltningen har skattat sig lågt på delfrågan om verksamheten har dokumenterade arbetssätt för att säkerställa dataskyddsperspektivet vid införandet och användandet av kostnadsfria tjänster såsom gratisappar och sociala medier. Mot bakgrund av detta rekommenderar dataskyddsombudet att verksamheten antar ett dokumenterat arbetssätt i frågan. Frågan om sociala medier diskuteras närmare vid avsnitt 3.3 om uppföljning.

Utifrån verksamhetens skattning i enkäten rekommenderar dataskyddsombudet att verksamheten utvärderar sitt arbetssätt gällande behörighetsstyrning och att verksamheten dokumenterar detta för att säkerställa en enhetlig hantering.

Förvaltningen har även skattat sig lågt på delfrågan om målgruppsanpassad information gällande hur digitala verktyg får användas och på delfrågan om uppföljning av följsamhet gentemot styrande dokument i samband med användningen av system och andra digitala verktyg. Mot bakgrund av dessa lämnade svar rekommenderar dataskyddsombudet att verksamheten utvärderar hanteringen och vidtar behövliga åtgärder för att säkerställa att användare får tillräcklig kunskap om hur system och andra digitala verktyg får användas och att verksamheten antar ett dokumenterat arbetssätt för att systematiskt följa upp efterlevnaden.

3.2.12 Kontrollpunkt 12: Hantering av registrerades rättigheter

Verksamhetens skattning av risknivå

			X

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 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. Även inom verksamheter med eventuella låga risker krävs det kontinuerliga insatser för att ett systematiskt dataskyddsarbete ska kunna upprätthållas och stärkas ytterligare.

Förvaltningen har informerat om följande vid muntlig avstämning i oktober. Det finns undantag från de registrerades rättigheter vad gäller behandling som sker för arkivändamål av allmänt intresse. Det är ganska ovanligt att förvaltningen tar emot begäran från registrerade. Förvaltningen har en mall för svar när begäran inte kan tillmötesgås med hänvisning till undantagen från de registrerades rättigheter.

Dataskyddsombudet rekommenderar att verksamheten fortsätter att tillvarata de registrerades rättigheter både genom hantering i konkreta förfrågningar från de registrerade och genom faktiska personuppgiftsbehandlingar. Vad gäller de dokument som finns framtagna för hantering av förfrågningar från de registrerade så rekommenderar dataskyddsombudet att verksamheten utvärderar dokumentens ändamålsenlighet samt den praktiska hanteringen och vidtar eventuella behövliga förbättringsåtgärder.

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): Samtycke som rättslig grund

Verksamheten gavs följande rekommendationer:

- Genomför en konsekvensbedömning för behandling av personuppgifter i sociala medier. Förvaltningen avråds från att fortsätta behandla personuppgifter i sociala medier i det fall denna konsekvensbedömning visar att följsamhet mot GDPR inte kan säkerställas.
- Utred och bedöm lämpligheten i att använda samtycke som rättslig grund vid behandling i sociala medier mot bakgrund av bland annat profilering, bristande transparens etc.
- Ta fram en rutin eller instruktion som anställda kan använda som stöd i bedömningen av när och hur samtycke kan eller inte kan användas.

Kommentarer och rekommendationer:

Uppföljningen visar att verksamheten fortfarande har förbättringsområden inom denna kontroll. Även om den aktuella fördjupade kontrollen hade särskilt fokus på den rättsliga grunden samtycke så kommer dataskyddsombudet i denna uppföljning även kommentera användningen av sociala medier ur ett bredare perspektiv.

Rekommendationen om att genomföra en konsekvensbedömning

Verksamheten har uppgett att man inte har genomfört en konsekvensbedömning för användningen av sociala medier och detta med motiveringen att behandlingen endast uppfyller ett kriterium för när en konsekvensbedömning behöver göras och att det numera finns ett adekvansbeslut varför tredjelandsöverföringen inte längre är problematisk.

Vad som är viktigt att förstå vad gäller användning av sociala medier är att det inte bara är publiceringen av bilder på och ljudupptagningar av personer som utgör

personuppgiftsbehandling, utan det sker även personuppgiftsbehandlingar gällande de personer som besöker och interagerar med de sidor och inlägg som verksamheten har. I verksamhetens lämnade svar i uppföljningen ligger fokus på personuppgiftsbehandlingar genom publicering av bilder och ljudupptagningar, men det saknas helt en redogörelse för personuppgiftsbehandlingar som gäller de personer som interagerar med det sociala mediet. Detta är förklarligt utifrån den fördjupade kontrollens rubrik, men dataskyddsombudet vill här understryka att arkivnämnden som personuppgiftsansvarig behöver analyseras frågan om sociala medier ur ett heltäckande perspektiv. Om man utgår från tidigare praxis så är det inte osannolikt att arkivnämnden kommer att bedömas som gemensamt personuppgiftsansvarig tillsammans med Meta i någon eller flera behandlingsaktiviteter som gäller de personer som interagerar med det sociala mediet.[4] Verksamheten behöver kartlägga samtliga personuppgiftsbehandlingar som användningen av sociala medier innebär och bringa klarhet i ansvar och roller vad gäller dessa behandlingar. Det är först när verksamheten har fått klarhet i detta som verksamheten kan utesluta eller bekräfta behovet av att genomföra en konsekvensbedömning.

Rekommendationen om att utreda och bedöma lämpligheten i att använda samtycke som rättslig grund vid behandling i sociala medier

Dataskyddsombudet uppfattar det som att verksamheten har gjort vissa ansträngningar för att utreda och bedöma användningen av samtycke som rättslig grund och att verksamheten har gjort vissa anpassningar i hanteringen framöver så att det inte enbart är samtycke som används som rättslig grund utan att även uppgift av allmänt intresse. Verksamheten har bland annat uppgett följande som framgår ur tabellen nedan gällande publicering av bilder och ljudupptagningar.

Kategorier av registrerade	Personuppgifter	Rättslig grund	Ändamål
Privatpersoner/allmänhet	Äldre bilder/ljuduppgifter från arkiv	Uppgift av allmänt intresse	Arkivändamål av allmänt intresse (att tillgängliggöra arkivhandlingar och främja användning av arkiven)
Anställda och konsulter på regionarkivet	Aktuella genrebilder[5]/ljuduppgifter	Samtycke	Informera om förvaltningens verksamhet och främja användandet av arkiv
Anställda och konsulter på regionarkivet	Aktuella dokumentära bilder/ljuduppgifter	Uppgift av allmänt intresse	Informera om förvaltningens verksamhet och främja användandet av arkiv
Privatpersoner/allmänhet	Aktuella genrebilder/ljuduppgifter	Samtycke	Informera om förvaltningens verksamhet och främja användandet av arkiv
Privatpersoner/allmänhet	Aktuella dokumentära bilder/ljuduppgifter	Uppgift av allmänt intresse	Informera om förvaltningens verksamhet och främja användandet av arkiv

Vad gäller användningen av samtycke som rättslig grund så har verksamheten själva bedömt att man anser sig säkerställa frivillighet och transparens. Dataskyddsombudet instämmer i att flera av de saker som nämns, i sig bidrar till att understödja frivillighet och transparens, men dataskyddsombudets uppfattning är att det inte räcker att bara informera om *att* personuppgifter kommer läggas upp på

[4] EU-domstolens dom i mål C-210/16, ”Wirtschaftsakademie”. Tillgänglig: CURIA - Documents (europa.eu).
[5] Med genrebilder avses här bilder där personerna på bilderna är utbytbara.

sociala medier. Som med all annan personuppgiftsbehandling så har den registrerade rätt att få information om *hur* personuppgifterna kommer att behandlas och ytterligare detaljer kring behandlingen (se mer artikel 13-14 i GDPR). Verksamheten behöver därför kunna förklara för den registrerade på ett mer ingående sätt vad publiceringar och interaktion med verksamhetens konto och inlägg på sociala medier innebär och vilka olika behandlingsaktiviteter som aktualiseras i samband med detta. Verksamheten behöver därför sätta sig in i vad som händer med publiceringar på de plattformar som används och hur exempelvis Meta behandlar denna information. Vidare behöver verksamheten också sätta sig in i de behandlingar som sker vad gäller de personer som interagerar med det sociala mediet och kunna redogöra för detta. Vad gäller möjligheten att dra tillbaka sitt samtycke till publiceringar så behöver verksamheten utreda och kunna svara på mer i detalj vad som gäller vid borttagande av innehåll på de plattformar som används och om eventuella kopior sparas av plattformsleverantören.

Uppgift av allmänt intresse och arkivändamål av allmänt intresse

Eftersom fokus för den här fördjupade kontrollen och uppföljningen har varit samtycke som rättslig grund, så kommer dataskyddsombudet inte här gå helt på djupet i att kommentera den för övrigt valda rättsliga grunden och ändamålet med behandlingarna, men vill ändå kort nämna följande.

Vad gäller uppgift av allmänt intresse så behöver kravet på nödvändighet säkerställas. Verksamheten behöver kunna motivera nödvändigheten i att använda just sociala medier som ett medel för att uppnå de angivna ändamålen. IMY har gjort allmänna uttalanden om publicering av bilder på internet.[6] Eftersom uttalandena gäller internetpubliceringar generellt och inte sociala medier specifikt så är det svårt att med säkerhet dra generella slutsatser om de aktuella resonemangen kring möjliga rättsliga grunder också är applicerbara på sociala medier. Men det kan i vart fall med stöd i uttalandet ifrågasättas om uppgift av allmänt intresse kan användas som rättslig grund för publicering av bilder på vem som helst.

Dataskyddsombudet ställer sig också frågande till verksamhetens bedömning att publicering av bilder och ljudupptagningar från arkivbestånd som görs på sociala medier, kan betraktas som ett led i arkivändamål av allmänt intresse. I detta sammanhang vill därför dataskyddsombudet påminna om de skrivelser som dataskyddsombudet har gjort tidigare på temat.[7] Dataskyddsombudet anser till skillnad från verksamheten att publiceringar i sociala medier som gäller bilder och ljudupptagningar från arkivbestånd snarare verkar sammanfalla med det andra ändamålet som är att informera om förvaltningens verksamhet. Distinktionen mellan vilket ändamål som gäller är viktigt eftersom det finns vissa specialregler kopplat till arkivändamål av allmänt intresse och att dessa regler inte gäller om det inte är fråga om arkivändamål av allmänt intresse. Om de aktuella bild- och ljudpubliceringarna på sociala medier inte räknas som en personuppgiftsbehandling

[6] IMY. Publicera bilder, filmer och ljud på internet. Vi guidar dig. Tillgänglig: Publicera bilder, filmer och ljud på internet | IMY. (Hämtad 2023-12-15).
[7] Se t.ex. dataskyddsombudets skrivelse ”Regionarkivets möjligheter för vidarebehandling av bilder från arkivbeståndet med syftet att informera om regionarkivets verksamhet” (2021-11-15).

som sker för arkivändamål av allmänt intresse, så behöver det rättsliga stödet för behandlingen styrkas och frågan om ändamålsbegränsning undersökas närmare.

Rekommendationen om att ta fram en rutin eller instruktion

Förvaltningen har uppgett att man har uppdaterat ”Kanalguide för Regionarkivet – ett stödjande dokument för Regionarkivets anvisning för kommunikation” och dataskyddsombudet kan därmed konstatera att den aktuella rekommendationen delvis är omhändertagen, men mot bakgrund av tidigare nämnda frågetecken kan ytterligare åtgärder behöva vidtas och justeringar i dokumentet behöva göras.

Övriga reflektioner kring användning av sociala medier

Som tidigare nämnts så behöver verksamheten kartlägga samtliga personuppgiftsbehandlingar som användningen av sociala medier innebär och bringa klarhet i vilka ansvar och roller som gäller för dessa. Verksamheten behöver också säkerställa att rättslig grund finns för samtliga behandlingar. Frågan om rättslig grund är bara en av flera parametrar som är av betydelse för en personuppgiftsbehandlings laglighet och därför behöver frågan om användning av sociala medier ses ur ett bredare perspektiv.

Verksamheten har uppgett att man själva inte profilerar och att man bedömer att det är en väldigt liten risk att externa aktörer ska kunna använda personuppgifter i form av bilder för att profilera. Mot bakgrund av ett aktuellt beslut mot Meta[8] och utifrån vad som framgår ur Metas integritetspolicy,[9] så är det tydligt att Meta ägnar sig åt profilering. Även om det inte skulle förekomma profilering av de personer som förekommer på regionarkivets publicerade bilder, så kan dataskyddsombudet i dagsläget inte utesluta att det kan förekomma profilering av de personer som interagerar med verksamhetens sidor och inlägg på sociala medier. Verksamheten behöver därför utreda frågan närmare.

Uppföljning kommer att ske igen under 2024.

[8] EDPB. EDPB Urgent Binding Decision on processing of personal data for behavioural advertising by Meta | European Data Protection Board (europa.eu).
[9] Meta. Privacy Center. Metas integritetspolicy – Så samlar Meta in och använder användardata | Integritetscenter | Hantera din integritet på Facebook, Instagram och Messenger | Integritet på Facebook.

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 5: Övergripande styrning av dataskyddsarbetet**

Anta en övergripande strategi för dataskyddsarbetet, samt vidta åtgärder för att kunna arbeta riskbaserat.

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 genomför kontrollen/kontrollerna.

- **Kontrollpunkt 9 och 10: Konsekvensbedömning/samråd och IT-projekt och upphandling**

Utvärdera verksamhetens arbetssätt vad gäller hantering av dataskyddsfrågor inom IT-projekt och upphandling, samt tröskelanalyser och konsekvensbedömningar. Fortsätt gå på djupet i frågor som rör verksamhetens behandlingar. Vidta åtgärder för att säkerställa att dataskyddsperspektivet tas i beaktan på ett systematiskt sätt och i ett tidigt skede. Vidta åtgärder för att säkerställa att behandlingar utreds innan beslut fattas, avtal tecknas och personuppgiftsbehandlingar inleds. Vidta åtgärder för att säkerställa att dataskyddsombudets synpunkter inhämtas i god tid.

- **Kontrollpunkt 11: IT-system och digitala verktyg**

Utvärderar verksamhetens arbetssätt gällande behörighetsstyrning och dokumentera arbetssättet för att säkerställa en enhetlig hantering.

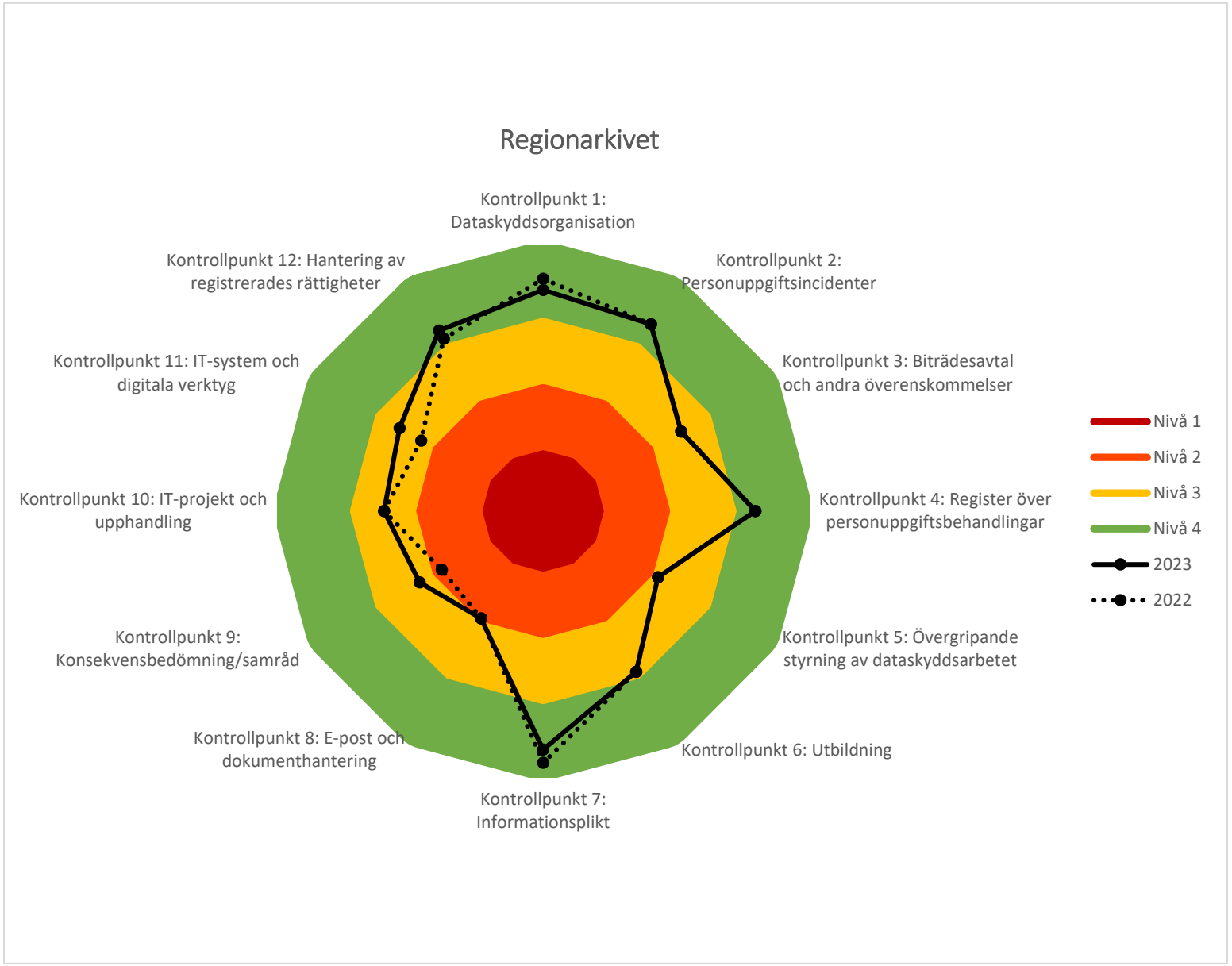
Utvärdera hanteringen gällande målgruppsanpassad information om hur digitala verktyg får användas. Vidta behövliga åtgärder för att säkerställa användare får tillräcklig kunskap om hur system och andra digitala verktyg får användas. Anta ett dokumenterat arbetssätt för att systematiskt följa upp efterlevnaden.

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

Regionarkivet

Kontrollplan för dataskyddsarbetet 2023–2024

2023-02-06

Innehåll

1 Bakgrund ... 3
1.1 Ny utformning av kontrollarbetet ... 3
2 Kontrollarbetet 2023–2024 ... 4
2.1 Kontrollarbetets delar ... 4
2.2 Tidplan för kontrollarbetet 2023–2024 ... 5
3 Kontroller ... 5
3.1 Fasta kontrollpunkter ... 5
3.2 Fördjupad kontroll ... 6
3.3 Uppföljning av genomförda kontroller ... 6
4 Rapportering ... 7
4.1 Årsrapport ... 7
4.2 Särskilt yttrande ... 7
5 Kontakt ... 7

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.