Göteborgs Stad

Årsrapport för dataskyddsarbetet 2023

Kretslopp- och vattennämnden

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.	

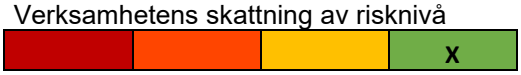
3.2 Resultat från kontrollen 2023

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

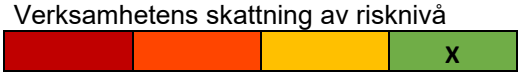
Dataskyddsombudet delar till stor del verksamhetens bedömning. Dataskyddsombudet gör dock till skillnad ifrån verksamheten bedömningen att det ändå föreligger risker inom kontrollpunkten, även om dessa inte bedöms som omfattande, brådskande eller allvarliga. Dataskyddsombudets uppfattning är dock att dataskyddsorganisationen gör ett gott arbete, men att verksamheten i stort behöver höja sig för att bidra till det systematiska dataskyddsarbetet.

Vid muntlig avstämning i oktober har dataskyddskontakten berättat följande. I och med införandet av det verksamhetsövergripande systemet BFUS har dataskyddsfrågorna blivit uppmärksammade mer brett och dataskyddskontakten har blivit mer synlig och känd med anledning av detta. I början på nästa år kommer man tillsätta en ny informationssäkerhetschef som kommer att ta ett helhetsgrepp kring frågorna om informationssäkerhet och dataskydd. Detta blir en ny tjänst och förhoppningen är att verksamheten ska integrera dataskyddsarbetet mer med informationssäkerhetsarbetet i stort och att verksamheten ska få synergier av detta.

Utifrån verksamhetens skattning i enkäten rekommenderar dataskyddsombudet att verksamheten utvärderar och analyserar sitt nuvarande arbetssätt för att ta reda på vad som krävs för att dataskydd ska bli en naturlig och integrerade del i det dagliga arbetet, samt att verksamheten vidtar åtgärder för att åstadkomma sådana förbättringar.

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.

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

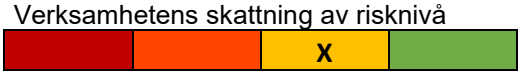
föreligger. Även inom verksamheter med låga risker krävs det dock kontinuerliga insatser för att ett systematiskt dataskyddsarbete ska kunna upprätthållas och stärkas ytterligare.

Vid muntlig avstämning i oktober har dataskyddskontakten berättat att man har en instruktion för hantering av personuppgiftsincidenter. Alla incidenter dokumenteras och verksamheten har en excell-lista i vilken man sammanställer alla årets inträffade incidenter. Listan diarieförs. Listan gör det möjligt att titta tillbaka på tidigare inträffade incidenter.

Utifrån förvaltningens skattning i enkäten och som en allmän rekommendation, rekommenderar dataskyddsombudet att förvaltningen utvärderar sitt arbetssätt för att upptäcka och utreda personuppgiftsincidenter och vidtar behövliga åtgärder för att säkra att arbetssättet är ändamålsenligt och effektivt. Vidare rekommenderar dataskyddsombudet att förvaltningen vidtar utbildnings- och/eller informationsinsatser för att säkerställa en tillräcklig kunskapsnivå inom organisationen.

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.

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.

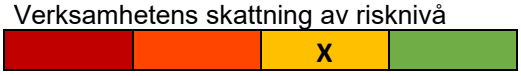
Vid muntlig avstämning med dataskyddskontakten i oktober har följande framkommit. Det finns en instruktion för att bedöma personuppgiftsansvar och biträdesförhållanden. Denna instruktion riktar sig till alla anställda.

Verksamheten uppskattar att personuppgiftsbiträdesavtal har tecknats till 75 %. Dataskyddsombudet rekommenderar att verksamheten fortsätter arbetet med att kartlägga biträdesförhållanden och att teckna avtal.

Utifrån förvaltningens skattning i enkäten rekommenderar dataskyddsombudet att förvaltningen utreder vad som behöver göras för att förvaltningen bättre ska leva upp till ansvarsskyldigheten som personuppgiftsansvarig. Det gäller både frågan om efterlevnadskontroller av personuppgiftsbiträden och 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 inga förändringar jämfört med förra årets skattning.

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.

Dataskyddskontakten har vid muntlig avstämning med dataskyddsombudet i oktober berättat att det finns en instruktion gällande behandlingsregistret.

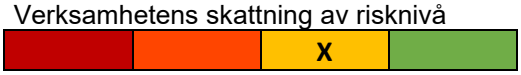
Verksamheten uppskattar att behandlingar finns upptagna till 75 %. Dataskyddsombudet rekommenderar att verksamheten fortsätter att kartlägga och dokumentera behandlingar i registret enligt de krav som finns.

Utifrån förvaltningens skattning i enkäten rekommenderar dataskyddsombudet att förvaltningen tydliggör roller och ansvar vad gäller behandlingsregistret och tar fram en plan för hur verksamheten kan säkerställa att registret hålls uppdaterat.

Vidare rekommenderar dataskyddsombudet att verksamheten undersöker hur registret kan användas i det löpande dataskyddsarbetet och vidtar åtgärder för att detta ska bli verklighet. Behandlingsregistret kan t.ex. användas för att identifiera behandlingar som sannolikt innebär hög risk för de registrerades fri- och rättigheter (d.v.s. behandlingar som behöver konsekvensbedömmas). Det behöver finnas en koppling och samstämmighet mellan de behandlingar som beskrivs i tröskelanalyser och konsekvensbedömningar och de behandlingar som beskrivs i behandlingsregistret. Behandlingsregistret är också användbart på så sätt att det ger den personuppgiftsansvarige grundläggande förutsättningar att tillgodose de registrerades fri- och rättigheter.

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 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.

I årsrapporten för 2022 rekommenderade dataskyddsombudet bland annat att förvaltningen skulle tydliggöra och strukturera styrningen av det systematiska dataskyddsarbetet. Som tidigare nämnts vid kontrollpunkt fem planerar förvaltningen att tillsätta en ny tjänst som informationssäkerhetchef i början på nästa år. Denna person kommer att leda och samordna arbetet med informationssäkerhetsfrågor och dataskydd. Dataskyddsombudet ser positivt på denna planerade åtgärd.

Utifrån verksamhetens skattning i enkäten rekommenderar dataskyddsombudet att verksamheten antar en 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 behöver därefter sätta upp en tidsplan och 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.

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 marginell sänkning jämfört med förra årets skattning.

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.

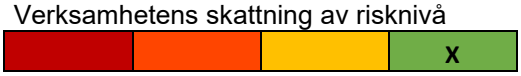
I samband med avstämning i oktober har dataskyddskontakten uppgett följande. Kunskapsnivån inom organisationen är varierande. Några har mycket kunskap och andra behöver bygga grundläggande kunskap. Det finns en plan för att fler ska få

grundläggande kunskaper. Utbildningen dataskydd på jobbet används och tidigare ordinarie dataskyddskontakt har varit ute på APT och pratat om dataskydd.

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

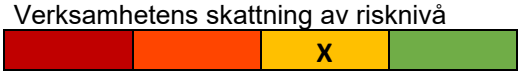
Verksamhetens resultat indikerar att verksamheten bedriver ett systematiskt dataskyddsarbete inom ramen för kontrollpunkten och att inga risker av betydelse föreligger. Resultatet innebär inga förändringar jämfört med förra årets skattning.

Dataskyddsombudet delar till stor del verksamhetens bedömning. Dataskyddsombudet gör dock till skillnad ifrån verksamheten bedömningen att det ändå föreligger risker inom kontrollpunkten, även om dessa inte bedöms som omfattande, brådskande eller allvarliga. Dataskyddsombudet vill 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. Dataskyddsombudets mer försiktiga hållning vad gäller skattningen av den här kontrollpunkten grundar sig även i vad som framkommit gällande den information som ges i e-tjänsterna.

Dataskyddsombudet vill påminna om den informationsinsats som dataskyddsenheten höll på temat informationsplikten och det informationsmaterial som togs fram i samband med detta. Förvaltningen rekommenderas utvärdera i vilken mån verksamheten lever upp till dessa krav och att vidta eventuella förbättringsåtgärder. Informationsplikten handlar 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.

3.2.8 Kontrollpunkt 8: E-post och dokumenthantering

Verksamhetens skattning av risknivå



Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger risker som behöver åtgärdas, men att dessa inte är brådskande, omfattande eller allvarliga. Resultatet innebär en marginell höjning jämfört med förra årets skattning. I årsrapporten för 2022 rekommenderade dataskyddsombudets att förvaltningen skulle prioritera den här kontrollpunkten.

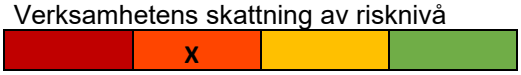
Dataskyddsombudet delar till viss del verksamhetens bedömning, men gör till skillnad ifrån verksamheten bedömningen att det inom kontrollpunkten förekommer risker som är omfattande och kräver omgående åtgärder. Dataskyddsombudets avvikande bedömning ska förstås mot bakgrund av att det finns rekommendationer från föregående år som ännu inte har omhändertagits och mot bakgrund av vissa frågetecken kring gallring (se avsnitt 3.3 om uppföljning).

I årsrapporten för 2022 rekommenderade dataskyddsombudet bland annat att förvaltningen skulle ta fram en anvisning för hur personuppgifter i e-post får hanteras samt att informera de registrerade om hur deras personuppgifter hanteras direkt vid första kontakt. Vid muntlig avstämning har dataskyddskontakten berättat följande. Verksamheten har tagit fram en mall för mejlsignatur som innehåller länk till integritetspolicyn. Verksamheten har ännu inte tagit fram en anvisning för hantering av personuppgifter i e-post, men planerar att göra det för nästa år. Utifrån vad verksamheten berättat rekommenderar dataskyddsombudet att verksamheten fullföljer planerna om att ta fram en anvisning för hantering av personuppgifter i e-post.

Dataskyddsombudet rekommenderar förvaltningen att fortsätta arbetet med dokumenthanteringsplanen 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 till exempel hjälpa förvaltningen i arbetet med behandlingsregistret och för att få en överblick på vilka personuppgifter som kan förekomma i olika handlingar och sammanhang. Informationsklassningsarbetet kan till exempel hjälpa organisationen att få en enhetlig och säker hantering vad gäller personuppgifter som är av liknande art och känslighet. Utifrån att det uppstått vissa frågetecken kring gallring rekommenderar dataskyddsombudet att verksamheten gör en genomlysning av dokumenthanteringsplanen utifrån frågan om gallring. Det behöver vara tydligt vad gallringsbesluten omfattar och gallringstiden behöver vara motiverad. Vidare behöver gallring säkerställas i praktiken.

3.2.9 Kontrollpunkt 9: Konsekvensbedömning/samråd

Verksamhetens skattning av risknivå



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.

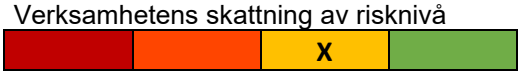
Dataskyddsombudet delar verksamhetens bedömning om att det förekommer risker som är omfattande och kräver omgående åtgärder.

Vid muntlig avstämning i oktober har dataskyddskontakten berättat att det finns en anvisning för konsekvensbedömningar.

Verksamheten har bland annat skattat sig lågt på delfrågan om dokumenterade arbetssätt för att säkerställa att konsekvensbedömningar genomförs innan riskfyllda behandlingar påbörjas. Mot bakgrund av detta rekommenderar dataskyddsombudet att verksamheten utvärderar sitt nuvarande arbetssätt, analyserar hur man kan arbeta mer systematiskt med tröskelanalyser och konsekvensbedömningar samt att åtgärder vidtas för att uppnå en sådan förbättring. Vidare rekommenderar dataskyddsombudet att verksamheten antar ett dokumenterat arbetssätt för att uppdatera konsekvensbedömningar vid förändringar, samt antar ett dokumenterat arbetssätt för att följa upp åtgärder som beslutats för att hantera risker inom ramen för konsekvensbedömningar som gjorts. Vidare, mot bakgrund av att dataskyddsombudet tidigare år observerat en viss ovilja i verksamheten att ta hänsyn till analysresultatet i de bedömningar som gjorts, vill dataskyddsombudet påminna om vikten av att inte ducka för identifierade risker och brister vad gäller dataskydd och att ta ansvar fullt ut även om detta innebär att behandlingar inte kan genomföras överhuvudtaget eller på så sätt som planerats.

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 en marginell höjning jämfört med förra årets skattning.

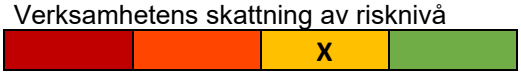
Dataskyddsombudet delar verksamhetens bedömning om att det finns risker som behöver åtgärdas, men gör precis som verksamheten bedömningen att de inte är omfattande, brådskande eller allvarliga. Trots detta finns det ändå områden där verksamheten behöver genomföra åtgärder.

Vid muntlig avstämning med dataskyddsombudet i oktober har dataskyddskontakten uppgett att det finns god kompetens i gruppen som jobbar med IT och informationssäkerhet. Behovs- och riskanalyser genomförs exempelvis i samband med förändringar eller att något nytt system eller digitalt verktyg ska införas.

Utifrån förvaltningens skattning i enkäten rekommenderar dataskyddsombudet att förvaltningen utvärderar sitt arbetssätt vad gäller hantering av dataskyddsfrågor inom IT-projekt och upphandling och vidtar åtgärder för att säkerställa att dataskyddsombudet involveras från start vid uppstart av nya IT-projekt och/eller vid införandet av nya tjänster där personuppgifter kommer att hanteras.

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 marginell höjning jämfört med förra årets skattning.

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.

Under hösten har dataskyddsombudet involverats i konsekvensbedömningen av digitala vattenmätare som är en pilot. Dataskyddsombudet ser det som positivt att verksamheten har involverat dataskyddombudet i ett så pass tidigt skede och uppmuntrar verksamheten att fortsätta på liknande sätt i andra projekt.

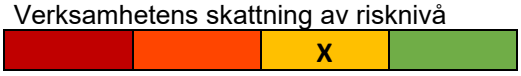
Vid muntlig avstämning i oktober har dataskyddskontakten berättat att det sker en årlig revision av behörigheter och att man har kopplat behörigheterna till roll. Behörigheterna kontrolleras även vid onboarding och offboarding. Vid onbarding så ger man information om hur system ska användas. Hanteringen grundar sig i ett delvis dokumenterat arbetssätt.

Utifrån verksamhetens skattning i enkäten rekommenderar dataskyddsombudet att verksamheten antar ett dokumenterat arbetssätt för att systematiskt kunna följa upp och kontrollera att användningen av system och/eller andra digitala verktyg ligger i linje med antagna styrande dokument.

Vidare, utifrån skattningen i enkäten, rekommenderar dataskyddsombudet att verksamheten antar dokumenterade arbetssätt för att säkerställa dataskyddsperspektivet vid införandet och användandet av kostnadsfria tjänster såsom gratisappar och sociala medier.

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 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 omgående åtgärder. Denna bedömning görs mot bakgrund av förvaltningens hantering i det konkreta fallet med talsvar i natten.[2] Exemplet visar vikten av att ha koll på de praktiska och legala förutsättningarna kring behandlingarna och att som personuppgiftsansvarig ta fullt ansvar för detta och att kunna förmedla information. Dataskyddsombudet rekommenderar att förvaltningen analyserar den egna hanteringen och vidtar åtgärder för att i framtiden ha en bättre beredskap att hantera förfrågningar från de registrerade.

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): Kamerabevakning

Verksamheten gavs följande rekommendationer:

- Säkerställ att förvaltningen uppfyller informationsplikten genom att kontrollera så att korrekt och komplett information om kamerabevakningen tillhandahålls vid samtliga anläggningar.

- Säkerställ att förvaltningen uppfyller informationsplikten genom att ta fram och tillhandahålla korrekt och komplett information om den kamerabevakning som sker internt inom anläggningarna av bland annat förvaltningens anställda.

- Redogör för den dokumentation som finns gällande bedömning av risker kopplat till behandling av personuppgifter genom kamerabevakningen.

[2] Se avvikelserapport ”Problem vid SMS-utskick inför planerade arbeten för inkoppling av stomledning vid Bifrost”.

- Förtydliga vilka ställningstaganden som gjorts kopplat till gallringsfristen av det inspelade filmmaterialet i kamerorna. I dagsläget finns detta material tillgängligt i sex månader, vilket i förhållande till kamerabevakning får anses utgöra en lång gallringsfrist.

Kommentarer och rekommendationer:

Uppföljningen visar att verksamheten har vidtagit åtgärder i enlighet med samtliga rekommendationer. Dataskyddsombudet har dock två anmärkningar. Den ena gäller informationsplikten och den andra gäller motiveringen gällande gallringsfristen.

Verksamheten har bland annat uppgett följande gällande informationsplikten. Verksamheten vill inte ”skylta alltför tydligt med information på kameraskylten om varför kamerabevakning sker, samt personliga kontaktuppgifter på skylten utifrån den mall som Integritetsskyddsmyndigheten föreslår i sina råd”. Dataskyddsombudet ställer sig frågande till detta resonemang. Dataskyddsombudet rekommenderar att verksamheten följer de rekommendationer som integritetsskyddsmyndigheten har lämnat gällande informationsplikten.

Dataskyddsombudets uppfattning är att verksamheten inte har motiverat gallringsfristen på ett tillfredsställande sätt och att gallringsfristen därför kan ifrågasättas. Verksamheten har uppgett att följande framgår ur rutin. ”Information gallras automatiskt senast sex månader efter inspelning eller tidigare om lagringsutrymmet är begränsat. Vid misstanke om brott ska inspelat material kunna sparas med hänsyn till brottsutredning.”.

Dataskyddsombudet förstår att polisens utredning, eventuellt efterföljande åtal och rättegång kan ta mer än sex månader och att det därför är nödvändigt att spara materialet under en länge tid i dessa specifika fall. Dataskyddsombudet ställer sig samtidigt frågande till om det är motiverat att spara allt videomaterial i så lång tid som sex månader. Dataskyddsombudet rekommenderar att verksamheten ser över verksamhetens hantering och säkerställer att den inte innebär att personuppgifter sparas längre än vad som är nödvändigt. Verksamheten behöver skilja på behandling som är nödvändig för hantering av misstanke och utredning av brott och behandling som eventuellt sker för andra ändamål. Det behöver vara tydligt definierat och avgränsat vilken behandling som sker för hantering av misstanke och utredning av brott.

Fortsatt uppföljning kommer ske inom ramen för de fasta kontrollpunkterna om ingen särskilt föranleder att det behöver följas upp separat.

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/förvaltningen att under 2024 prioritera följande delar av dataskyddsarbetet:

- **Kontrollpunkt 8: E-post och dokumenthantering**

Fullfölj planerna om att ta fram en anvisning för hantering av personuppgifter i e-post.

Gör en genomlysning av dokumenthanteringsplanen utifrån frågan om gallring. Säkerställ att det är tydligt vad gallringsbesluten omfattar och att gallringstiden är motiverad samt att gallringsbesluten följs.

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

Utvärdera verksamhetens nuvarande arbetssätt vad gäller IT-projekt och upphandling samt konsekvensbedömningar.

Vidta åtgärder för att säkerställa att dataskyddsombudet involveras från start vid uppstart av nya IT-projekt och/eller vid införandet av nya tjänster där personuppgifter kommer att hanteras.

Analysera hur verksamheten kan arbeta mer systematiskt med tröskelanalyser och konsekvensbedömningar. Vidta åtgärder för att uppnå en förbättring.

Anta ett dokumenterat arbetssätt för att uppdatera konsekvensbedömningar vid förändringar.

Anta ett dokumenterat arbetssätt för att följa upp åtgärder som beslutats för att hantera risker inom ramen för konsekvensbedömningar som gjorts.

- **Kontrollpunkt 12: Hantering av registrerades rättigheter**

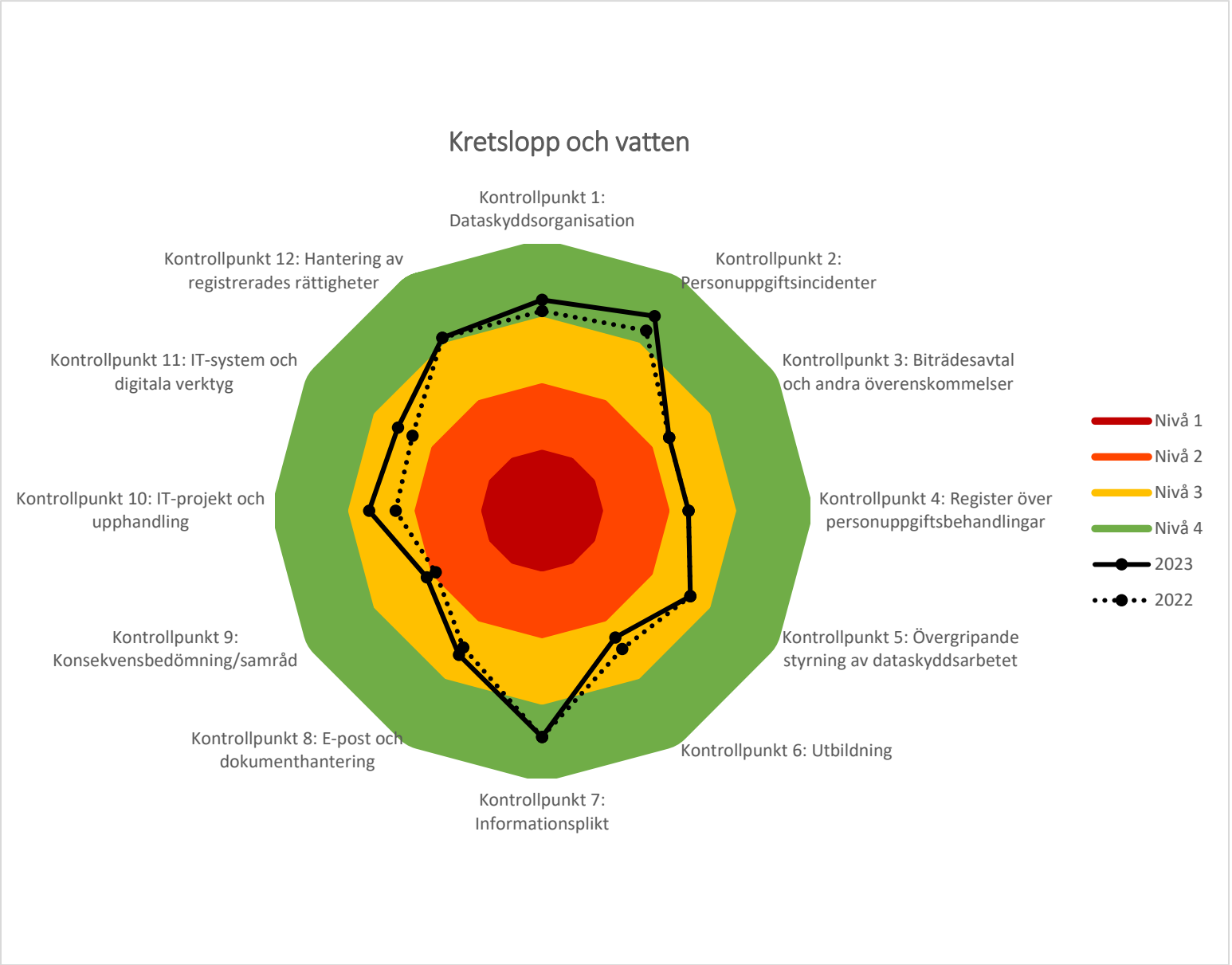
Analyserar den egna hanteringen och vidta åtgärder för att i framtiden ha en bättre beredskap att hantera förfrågningar från de registrerade.

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

Kretslopp- och vatten

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 person-uppgifter behandlas. Punkten omfattar även hur verksamheten säkerställer att informationen är uppdaterad.

Kontrollpunkt 8: E-post och dokumenthantering

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

Kontrollpunkt 9: Konsekvensbedömning/samråd

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

Kontrollpunkt 10: IT-projekt och upphandling

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

Kontrollpunkt 11: IT-system och digitala verktyg

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

Kontrollpunkt 12: Hantering av registrerades rättigheter

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