Göteborgs Stad

Årsrapport för dataskyddsarbetet 2022

Kretslopp- och vatten

2022-12-20

Innehåll

1 Dataskydd i kommunal verksamhet

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 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. 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 uppgifterna.

Arbetet med att säkerställa att personuppgifter behandlas enligt reglerna i GDPR 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 på förvaltningar och bolag inom Göteborgs Stad. I det framåtsyftande arbetet är GDPR ett viktigt redskap för att kunna säkerställa en digitalisering som håller över tid.

1.1 Göteborgs Stads dataskyddsombud

Dataskyddsenheten på Intraservice är Göteborgs Stads dataskyddsombud. Vad som är dataskyddsombudets uppgifter framgår direkt av lagstiftningen i GDPR.[1] Dataskyddsombudets viktigaste uppgift är att övervaka att stadens förvaltningar och bolag följer dataskyddslagstiftningen. Detta sker bland annat genom att samla in information om hur personuppgifter behandlas och genom att kontrollera hur bestämmelser och interna styrdokument som styr dataskyddsarbetet efterlevs.

Dataskyddsombudet har också till uppgift att ge råd och information till förvaltningar och bolag i dataskyddsfrågor. Detta sker genom att dataskyddsombudet är behjälplig när frågor rörande behandlingen av personuppgifter uppkommer hos verksamheterna. Dataskyddsombudet erbjuder också regelbundet utbildningar för stadens medarbetare. Rådgivning ges även till förvaltningar och bolag när dessa genomför konsekvensbedömningar, vilket är en skyldighet som följer av GDPR. Efter att ha identifierat ett särskilt behov av stöd i arbetet med konsekvensbedömningar, har dataskyddsenheten under 2022 tagit fram mallar och mallstöd för det arbetet.

Det är nämnd/styrelse som har det yttersta ansvaret för att verksamheterna följer dataskyddslagstiftningen och dataskyddsombudet ska enligt lag rapportera om detta till högsta förvaltningsnivå.[2] Dataskyddsombudet har inte mandat att fatta beslut åt verksamheterna. Det är i stället genom råd och rekommendationer som

[1] Artikel 39 i GDPR
[2] Artikel 38.3 i GDPR

dataskyddsombudet bistår verksamheterna med underlag för att dessa själva ska kunna fatta väl underbyggda beslut.

2 Granskning av dataskyddsarbetet 2022

2.1 Dataskyddsombudets kontrollfunktion

Dataskyddsombudets uppgift att övervaka den personuppgiftsansvariges efterlevnad av förordningen regleras i artikel 39 i GDPR. I Göteborgs Stad innebär en del av denna övervakning att dataskyddsombudet genomför kontroller av dataskyddsarbetet inom den personuppgiftsansvariges organisation.

Enligt dataskyddsregelverket ska dataskyddsombudet arbeta utifrån en riskbaserad metod som utgår från risker för de registrerades fri- och rättigheter. Genom att utgå från en sådan metod minskas risken för negativa konsekvenser även för verksamheten själv. Sådana konsekvenser kan omfatta bland annat skadestånd, sanktionsavgifter, försämrat varumärke eller minskad tillit för verksamheten.

För dataskyddsombudet är kontrollarbetet ett sätt att få en bild av vilka risker och/eller brister som eventuellt föreligger inom en verksamhet. Genom kontroller kan dataskyddsombudet kartlägga verksamhetens dataskyddsarbete, och därigenom hjälpa verksamheten att få en nulägesbild av hur de faktiskt ligger till i sitt dataskyddsarbete. Denna kartläggning kan sedan användas som ett stöd för verksamheten i sitt fortsatta arbete med dataskydd. Kontrollarbetets syfte är inte främst att peka ut brister utan ska ses som en vägledning för verksamheten och ett verktyg för att identifiera relevanta prioriteringar. Det är sedan 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. I det arbetet är dataskyddsombudet behjälplig med rådgivning utifrån verksamhetens behov och de risker som identifierats.

2.2 Fördjupad kontroll

2.2.1 Kontroll av kamerabevakning 2022

Den fördjupade kontrollen har bestått av kamerabevakning (kontrollpunkt 11). Resultatet av kontrollen presenteras i sin helhet i bilaga 2.

Dataskyddsombudet har i rapporten avseende den fördjupade kontrollen haft vissa synpunkter och har därför lämnat ett antal rekommendationer till verksamheten för åtgärd.

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

- Säkerställa 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.

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

- 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.

2.3 Årlig kontroll av dataskyddsarbetet

Verksamhetens interna dataskyddsarbete följs årligen upp 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.

2.3.1 Metod och risknivåer

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.[3]

[3] I arbetet med enkäten har dataskyddsenheten utgått från Myndigheten för samhällsskydd och beredskaps (MSB) uppföljningsstruktur för den offentliga förvaltningens systematiska informationssäkerhetsarbete.

Beskrivning av risknivåer

Risknivåer	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 har ett systematiskt dataskyddsarbete.	

2.4 Kretslopp- och vattens dataskyddsarbete 2022

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.

2.4.1 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.

Dataskyddsombudets kommentarer:

Dataskyddsombudet har under det gångna året inte fått någon indikation som innebär en avvikande bedömning avseende skattningen. Utifrån enkätsvaren anser sig verksamheten ha en intern organisation där roller och ansvar är tydligt utpekat. Dataskyddsombudet anser att förvaltningen har en god kompetens i att arbeta med dataskyddsfrågor och att det finns definierade former för dataskyddsarbetet.

Frågorna är enligt dataskyddsombudet inte tillräckligt integrerade i den dagliga verksamheten vilket under året till exempel tagit sig uttryck i arbetet med konsekvensbedömningar av behandlingar som verksamheten utför eller planerar att utföra. Dessa ses ofta som ett nödvändigt ont och något som verksamheten bara behöver ”riva av”, utan att ha en djupare förståelse för att slutsatserna av dessa bedömningar är något som förvaltningen behöver ta höjd för i sitt dagliga arbete.

Dataskyddsombudet har också fått indikationer på att delar av förvaltningen i vissa frågor väljer att inte hörsamma de råd som lämnas av förvaltningens dataskyddskontakt eller dataskyddsombudet utan i stället gör egna tolkningar av hur dataskyddsarbetet ska bedrivas och hur GDPR ska tillämpas. Naturligtvis ska alla frågor kunna diskuteras, även dataskyddsfrågor. Med det sagt så är dataskyddsombudets uppfattning att det i en mogen dataskyddsorganisation är tydligt definierat vem som har tolkningsföreträde kring hur dataskyddslagstiftningen ska tillämpas i praktiken. Förvaltningen rekommenderas därför att tydliggöra roller och ansvar i den interna dataskyddsorganisationen.

2.4.2 Kontrollpunkt 2: Personuppgiftsincidenter

Kontrollpunkten avser verksamhetens förutsättningar och rutiner för att identifiera och hantera personuppgiftincidenter.

Dataskyddsombudets kommentarer:

Förvaltningen har angett en varierande skattning som över lag placerar verksamheten inom riskområde fyra. Förvaltningens svar indikerar att verksamheten i stort har rutiner, arbetssätt och utbildningsinsatser som är tillräckliga och fungerande. Samtidigt uppger sig Kretslopp- och vatten på ett övergripande plan, sakna dokumenterade rutiner som ger goda förutsättningar att upptäcka och utreda personuppgiftsincidenter. Verksamheten anser sig inte heller ha rutiner för att regelbundet följa upp inträffade incidenter som en naturlig del av dataskyddsarbetet. Frånvaron av dokumenterade rutiner behöver inte i sig betyda att det saknas ett fungerande arbetssätt. Med hänsyn till ansvarsskyldigheten i artikel 5 i GDPR är det dock önskvärt att rutiner och arbetssätt dokumenteras så att förvaltningen kan visa att och hur verksamheten följer GDPR.

Dataskyddsombudet rekommenderar därför att förvaltningen ser över sina rutiner och utreder var och varför det upplevs finnas brister. Det bör också säkerställas att förvaltningens rutiner med jämna mellanrum utvärderas, för att kontrollera om dessa är ändamålsenliga och effektiva. Verksamheten behöver också fortsätta arbeta med att informera medarbetare om vad som är personuppgiftsincidenter och vad man som anställd ska göra om en sådan incident upptäcks eller inträffar. Efter avstämning med förvaltningens dataskyddskontakt är dataskyddsombudets uppfattning att förvaltningen också behöver tydliggöra för medarbetarna när, hur och varför incidenter ska anmälas till tillsynsmyndigheten IMY.

2.4.3 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.

Dataskyddsombudets kommentarer:

Verksamhetens svar indikerar att det under kontrollpunkten finns brister som behöver åtgärdas framför allt när det gäller avsaknaden av rutiner för att vid anlitandet av ny leverantör avgöra huruvida en biträdessituation uppstår, för att genomföra kontinuerliga efterlevnadskontroller samt för att bedöma om överenskommelser/avtal om gemensamt/delat personuppgiftsansvar behöver tecknas. Verksamheten rekommenderas att ta fram sådana rutiner.

2.4.4 Kontrollpunkt 4: Personuppgiftsregister

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 personuppgiftsregister innefattas.

Dataskyddsombudets kommentarer:

Förvaltningen har på denna punkt angett värden som sammanlagt placerar verksamheten inom risknivå tre. Dataskyddsombudet bedömer att förvaltningens skattning är tvetydig, eftersom man uppger att samtliga behandlingar finns upptagna i registret, men att det samtidigt saknas rutiner för att hålla registret uppdaterat. Dataskyddsombudet ställer sig då frågande till hur förvaltningen kan bedöma att alla behandlingar finns dokumenterade.

Enligt förvaltningens svar så används inte heller registret som en del i det löpande dataskyddsarbetet. Dataskyddsombudets rekommendation är att verksamheten tar fram en rutin för att tillse att nya behandlingar upptas i registret, samt att förvaltningen så långt det är möjligt integrera registret i det dagliga arbetet.

2.4.5 Kontrollpunkt 5: Övergripande strategi för dataskydd

Kontrollpunkten avser verksamhetens övergripande strategi för att arbeta med dataskydd.

Dataskyddsombudets kommentarer:

Verksamheten har i sina svar angett att man har dokumenterade rutiner för att säkerställa att styrande dokument som reglerar personuppgiftsbehandlingar hålls uppdaterade. Det är också positivt att verksamheten har värderat sina informationstillgångar. Med ledning av förvaltningens svar verkar det dock finnas förbättringspotential i det övergripande strategiska arbetet med dataskyddsfrågor. Verksamheten rekommenderas därför att tydliggöra och strukturera styrningen av det systematiska dataskyddsarbetet, ta fram och implementera en informationssäkerhetspolicy för behandling av personuppgifter och anta ett riskbaserat arbetssätt i dataskyddsfrågor.

2.4.6 Kontrollpunkt 6: Utbildning

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

Dataskyddsombudets kommentarer:

Utifrån den angivna skattningen utgör kontrollpunkten ett område med potential till förbättring för verksamheten. Dataskyddsombudet rekommenderar därför att det inledningsvis sker en kartläggning av var i verksamheten det kan behövas större behov av kunskaper i dataskydd och att det därefter genomförs riktade utbildningsinsatser. Mot bakgrund av att det också anges att den allmänna kunskapsnivån inte är helt tillfredsställande rekommenderas insatser genomförs för att åtgärda detta.

Eftersom kunskap är en färskvara rekommenderas även förvaltningen att ta fram en plan/rutin för att regelbundet genomföra informationsinsatser med syftet att bibehålla och/eller höja den allmänna kunskapsnivån.

2.4.7 Kontrollpunkt 7: Integritetspolicy

Kontrollpunkten avser verksamhetens utformning samt tillhandahållande av dess integritetspolicy till registrerade (både internt och externt). Även verksamhetens rutin för att upprätthålla en aktuell integritetspolicy omfattas.

Dataskyddsombudets kommentarer:

Dataskyddsombudet delar inte fullt ut förvaltningens bedömning om att integritetspolicyn, som finns tillgänglig via kretslopp- och vattens hemsida uppfyller kraven enligt GDPR. Informationen behöver bland annat ses över vad

gäller tredjelandsöverföringar och cookiehantering. Förvaltningen rekommenderas därför att göra en översyn i dessa delar. Förvaltningen rekommenderas även att vidta åtgärder för att göra informationen lättillgänglig, oavsett i vilken digital kanal som den registrerades personuppgifter behandlas.

2.4.8 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 dataskyddsförordningen. Även verksamhetens rutin för att säkerställa att gallringsrutiner för personuppgifter följs innefattas.

Dataskyddsombudets kommentarer:

Kretslopp- och vatten har skattat kontrollpunkten med varierande värden. Förvaltningen uppger sig ha en aktuell och fastställd dokumenthanteringsplan med angivna gallringsfrister. Verksamheten har informationsklassificerat merparten av sina tillgångar, men uppger att informationen inte har uppdaterats senaste året. Förvaltningen uppger sig också sakna vissa rutiner och arbetssätt inom kontrollpunkten. Bland annat saknas dokumenterade rutiner för hantering av personuppgifter i E-post och anvisningar för hur information i olika informationsklasser ska hanteras och vilka lagringsytor som ska användas.

Utifrån skattningen rekommenderar dataskyddsombudet att Kretslopp- och vatten utför kontroller i system och lagringsytor som innehåller personuppgifter och kontrollera att dessa gallras i enlighet med vad som anges i dokumenthanterings-planen. Förvaltningen rekommenderas också ta fram en anvisning för hur personuppgifter i e-post får hanteras, informera de registrerade om hur deras personuppgifter hanteras direkt vid första kontakt, ta fram anvisningar för hanteringen av information i olika informationsklasser samt att kontinuerligt inventera de personuppgiftsbehandlingar som informationsklassificerats, för att tillse att informationen hålls uppdaterad.

2.4.9 Kontrollpunkt 9: Konsekvensbedömning/samråd

Kontrollpunkten avser verksamhetens förutsättningar för att kunna identifiera när en konsekvensbedömning ska göras, samt rutiner kopplat till detta.

Dataskyddsombudets kommentarer:

Förvaltningen har under det gångna året involverat dataskyddsombudet i flera konsekvensbedömningar med anledning av system och tjänster som har inneburit nya eller förändrade personuppgiftsbehandlingar. Dataskyddsombudets uppfattning är att förvaltningen har en god kompetens i egenskap av förvaltningens dataskyddskontakt, men att verksamheten i stort saknar förutsättningar för att arbeta med konsekvensbedömningar på ett systematiskt sätt.

Detta framkommer också av verksamhetens egna skattningar. Skattningen indikerar att verksamheten saknar rutiner och arbetssätt i organisationen för ett heltäckande arbete med konsekvensbedömningar. Dataskyddsombudets bedömning är att förvaltningen inte har ett riskbaserat arbetssätt. Positiva delar i förvaltningens skattning rör bland annat rutiner för att involvera dataskyddsombudet och för att inhämta råd ifrån och dokumentera dataskyddsombudets rekommendationer. Dataskyddsombudet delar förvaltningens bedömning i dessa delar. Samtidigt är dataskyddsombudets uppfattning att detta i mångt och mycket blir en pappersprodukt då resultatet av de bedömningar som görs och de synpunkter som framförs från dataskyddsombudet många gånger inte kommer till uttryck i förvaltningens faktiska arbete med sina personuppgiftsbehandlingar.

Råd och rekommendationer från dataskyddsombudet och slutsatser från konsekvensbedömningar förefaller ibland betraktas av verksamheten som något nödvändigt ont som verksamheten bara behöver ”riva av” och sedan inte ta hänsyn till i det faktiska arbetet. Dataskyddsombudet har också fått uppfattningen att verksamheten många gånger lämnar förvaltningens dataskyddskontakt ”vind för våg” med ansvaret för konsekvensbedömningarna, trots att arbetet med dessa bedömningar är någonting som måste involvera olika delar av en verksamhet och olika kompetenser. För att säkerställa att konsekvensbedömningar genomförs innan riskfyllda behandlingar påbörjas, samt att slutsatserna i dessa bedömningar beaktas krävs det att förvaltningen har ett strukturerat och tillräckligt resurssatt arbete i hela organisationen. Dataskyddsombudets bedömning är att detta är något som idag saknas.

Sammantaget indikerar skattningen att förvaltningen behöver vidta flertalet åtgärder för att säkerställa följsamhet mot GDPR vad gäller konsekvensbedömningar. Det är positivt att detta har identifierats som ett förbättringsområde och indikerar god insikt i att detta är något som behöver prioriteras. Dataskyddsombudets rekommendation är att förvaltningen tar ett helhetsgrepp i frågan och påbörjar ett arbete med att genomföra konsekvensbedömningar för samtliga behandlingar med höga risker, samt tar fram rutiner för samtliga delar av kontrollpunktens omfång där sådana saknas.

2.4.10 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.

Dataskyddsombudets kommentarer:

Förvaltningen har på denna punkt skattat sin organisation och sina rutiner med varierande värden. Enkätsvaren indikerar att förvaltningen säkerställer principerna om inbyggt dataskydd och dataskydd som standard vid upphandlingar, men att det i övrigt finns förbättringspotential.

Dataskyddsombudet har under det gångna året inte involverats från start i någon upphandling som förvaltningen själv har hanterat. Däremot har dataskyddsombudet involverats i en konsekvensbedömning avseende behandlingar i verksamhetssystemet IFS, detta skedde dock när systemet redan var upphandlat. Detta enstaka fall tydliggör verksamhetens behov av att ta fram rutiner för att säkerställa att nya lösningar uppfyller grundläggande principer i GDPR. Påståendet om att involvera dataskyddsombudet har också skattats lågt vilket innebär att verksamheten identifierat att detta är ett förbättringsområde.

Dataskyddsombudet rekommenderar att förvaltningen tar fram rutiner för att säkerställa att nya digitaliseringslösningar uppfyller kraven enligt GDPR och att verksamheten vidtar åtgärder som säkerställer att förvaltningen på ett mer systematiskt sätt arbetar med att bedöma risker för personuppgiftsbehandlingar vid upphandlingar och utvecklingsprojekt. Verksamheten rekommenderas också ta fram rutiner för att involvera dataskyddsombudet vid uppstart av nya IT-projekt där personuppgifter kommer hanteras.

2.4.11 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 dataskyddsförordningen. Rutin för att säkerställa och kontrollera att dessa system/tjänster uppfyller kraven på dataskydd ingår även.

Dataskyddsombudets kommentarer:

Förvaltningen har även på denna punkt skattat sin organisation och sina rutiner med varierande värden. Verksamhetens svar visar att förvaltningen i stort har koll på sina system och verktyg, med god dokumentation. Verksamheten har rutiner för tilldelning av behörigheter och åtkomst till IT-system och det finns målgruppsanpassad information för de verktyg som används. På minuskontot

framgår det att rutiner saknas för att systematiskt kunna följa upp och kontrollera att användningen av olika system följer antagna rutiner och riktlinjer. Förvaltningen saknar också rutiner för att säkerställa dataskyddsperspektivet vid införande av kostnadsfria tjänster som gratisappar och sociala medier.

Dataskyddsombudet ser ingen anledning att ifrågasätta förvaltningens skattning. En förutsättning för ett bra dataskyddsarbete är att bra rutiner finns på plats. Rutiner tjänar dock bara sitt syfte om de faktiskt följs. Dataskyddsombudet rekommenderar därför förvaltningen att ta fram rutiner för systematisk uppföljning samt för säkerställandet av dataskyddsperspektivet vid införande av kostnadsfria tjänster. Verksamheten behöver också aktivt följa upp medarbetares behörigheter och åtkomst till personuppgifter för att kontrollera att dessa är anpassade till endast det som den anställde behöver för att utföra sina arbetsuppgifter.

2.4.12 Kontrollpunkt 12: Hantering av registrerades rättigheter

Kontrollpunkten avser verksamhetens förutsättningar och rutiner för att hantera de registrerades rättigheter, till exempel registerutdrag eller radering.

Dataskyddsombudets kommentarer:

Dataskyddsombudet har inte fått några indikationer som tyder på att skattningen skulle vara missvisande eller felaktig. Utifrån svaren från verksamheten behöver förvaltningen säkerställa att det finns en tillräcklig medvetenhet om de registrerades rättigheter och hur dessa begränsas.

Dataskyddsombudet rekommenderar därför att förvaltningen inkluderar information om detta i den utbildning som ges till medarbetare om dataskydd, för att säkerställa att medarbetarna har kunskap om hur de registrerades rättigheter tillvaratas på det sätt som krävs enligt GDPR.

2.5 Sammanfattande rekommendationer

För att på ett praktiskt plan kunna identifiera vad verksamheten behöver arbeta med inom ramen för respektive kontrollpunkt behövs en noggrann genomgång av enkätresultaten. I detta rekommenderas verksamheten att samråda med dataskyddsombudet för att se hur arbetet framåt bör utformas och vilka delar som bör prioriteras utifrån verksamhetens risker. Även för verksamheter med låga risker krävs kontinuerliga insatser för att denna risknivå ska bibehållas.

Utifrån identifierade risker rekommenderar dataskyddsombudet att förvaltningen/bolaget under 2023 prioriterar följande delar av dataskyddsarbetet:

- Kontrollpunkt 1: Dataskyddsorganisation

  Förvaltningen rekommenderas att tydliggöra roller och ansvar i den interna dataskyddsorganisationen.

- Kontrollpunkt 8: E-post och dokumenthantering

  Förvaltningen rekommenderas ta fram en anvisning för hur personuppgifter i e-post får hanteras.

- Kontrollpunkt 9: Konsekvensbedömning/samråd

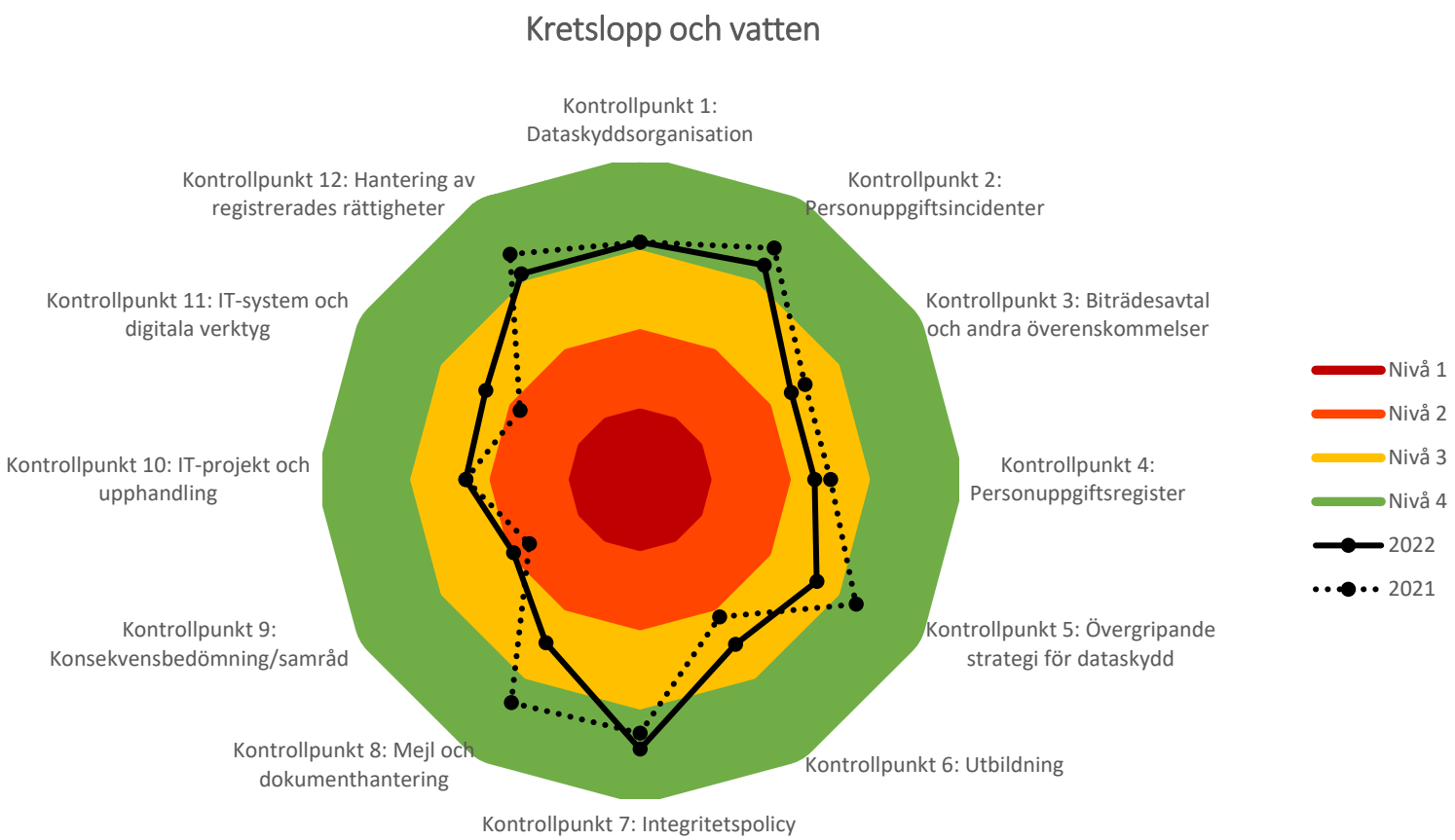
  Dataskyddsombudets rekommendation är att förvaltningen tar ett helhetsgrepp i frågan och påbörjar ett arbete med att genomföra konsekvensbedömningar för samtliga behandlingar med höga risker, samt tar fram rutiner för samtliga delar av kontrollpunktens omfång där sådana saknas

3 Bilagor

Bilaga 1: Diagram över resultat av fasta kontrollpunkter, jämfört med 2021.

Bilaga 2: Fördjupad kontroll 2022

Bilaga 1: Diagram över resultat av fasta kontrollpunkter, jämfört med 2021.



Fördjupad kontroll Kretslopp- och vatten

Kontrollpunkt 11: Kamerabevakning

Bakgrund

Den fördjupade kontrollen avseende kamerabevakning har haft till syfte att kartlägga verksamhetens kamerabevakning som innebär personuppgiftsbehandling och undersöka om hanteringen uppfyller kraven i dataskyddsförordningen (GDPR) och kamerabevakningslagen. Fokus har legat på ifall det finns dokumenterade bedömningar, om tillräcklig information lämnas till de registrerade och i förekommande fall om tillstånd finns. Kontrollen har genomförts genom att verksamheten har fått svara på ett antal frågor och bifoga underlag. I vissa fall har även uppföljande/kompletterande frågor och avstämningar varit nödvändiga.

Iakttagelser från kontrollen

Personuppgiftsansvariga ska i sin användning av kamerabevakning, i de fall det innebär en personuppgiftsbehandling, följa reglerna i dataskyddsförordningen och kamerabevakningslagen. Även i de fall då kamerabevakningen inte medför att tillstånd behöver sökas hos Integritetsskyddsmyndigheten (IMY) behöver reglerna i GDPR följas.

Kontrollen har varit svårarbetad då mycket av den kamerabevakning som Kretslopp- och vatten utför omfattas av i säkerhetsskyddslagen och därför är undantaget från reglerna i dataskyddsförordningen.

Rättslig reglering och vägledning

En verksamhet som planerar en kamerabevakning måste noga tänka igenom bevakningen och dokumentera sina bedömningar. En del i detta är att säkerställa att bevakningen uppfyller kraven enligt dataskyddsförordningen. Det innebär att bevakningen bl.a. behöver ha ett tydligt avgränsat ändamål, rättslig grund och att förordningens principer beaktas. För att uppfylla principen om uppgiftsminimering behöver platsen/platserna som bevakas vara begränsade och endast omfatta det som syftet med bevakningen kräver. Det får också enbart ske bevakning på de tider då bevakningen, med hänsyn till syftet, är nödvändig. Om kamerabevakningen sker med bildinspelning behöver det även säkerställas att lagring inte sker under längre tid än vad som är nödvändigt. Enligt vägledning från IMY är huvudregeln att materialet inte bör sparas längre än 72 timmar. Verksamheten behöver också säkerställa att konsekvensbedömningar görs i de fall då kraven för detta är uppfyllda. Det ska också lämnas information om kamerabevakningen till de registrerade. Informationen ska vara lättillgänglig och begriplig.

Offentliga aktörer och andra som utför en uppgift av allmänt intresse är tillståndspliktiga vid bevakning på platser dit allmänheten har tillträde, men bara om bevakningen innebär varaktig eller regelbundet upprepad personbevakning. Även om kamerabevakningen inte är tillståndspliktig innebär det inte automatiskt att den är tillåten.

Kretslopp och vattens användning av kamerabevakning

Kretslopp- och vatten har angett att majoriteten av förvaltningens civila skyddsobjekt kamerabevakas, samt delar av huvudanläggningen (vilken omfattar lager, förråd och garage). Förvaltningen vill inte uppge vilka specifika delar av anläggningarna som kamerabevakas då det anses utgöra en säkerhetsrisk.

Enligt förvaltningen kan inte all dokumentation som begärts in för kontrollen lämnas ut med hänvisning till att delar av den är sekretessbelagd (OSL 18:8). De dokument som bifogats kontrollen är ett nämndbeslut för tillstånd på vattenverket i Lackarebäck, en fil innehållandes mailväxling med dåvarande Datainspektionen (nuvarande Integritetsskyddsmyndigheten) och en rutin/anvisning för hantering av kamerabevakning.

Kretslopp och vatten har ett antal tillstånd för förvaltningens kamerabevakning, bland annat gjordes en ansökan till Länsstyrelsen 2013. Samtidigt anger förvaltningen att det skedde en uppdatering utav Kamerabevakningslagen 2018 vilken innebar att förvaltningen inte längre behöver Länsstyrelsens tillstånd när det gäller kamerabevakning vid skyddsobjekt. Förvaltningen uppger att det däremot alltid blir ett nämndärende när ett nytt objekt ska kamerabevakas. Exempel på hur ett sådant beslut ser ut tillhandahölls (PU KoV 2020-09-23 §173), och förvaltningen har även tillhandahållit ett beslut för hur ett tillstånd från Länsstyrelsen ser ut, där uppgifter som rör den specifika anläggningen har maskerats.

Förvaltningen har emellertid angett ett fall gällande en plats där kameran filmar mot en allmän plats. På denna plats finns ett stängslat skyddsobjekt där kameran sitter på stängslet och filmar mot en gång- och cykelbana. Syftet med bevakningen är att filma porten till skyddsobjektet för att förhindra intrång och/eller skadegörelse. Kameran filmar i realtid, men inspelningen aktiveras endast vid larm. Längs med hela stängslet finns tydliga skyltar om att det är kamerabevakat område. I övrigt ges ingen upplysning gentemot de registrerade som tillhör allmänheten.

Förvaltningen uppger att andra platser där allmänheten riskerar att filmas är vid infartsgrindar till anläggningar, där filmning sker i realtid. I ett av dessa fall syns en gångbana bredvid, om än diffust.

När det gäller skyltning för kamerabevakning anger förvaltningen att det finns skyltning vid vissa anläggningar, men inte vid alla. Att komplettera vid alla platser där kamerabevakning sker är ett arbete som kommer utföras under hösten. Förvaltningen uppger även att man ska se över så att ingen kamera filmar bortanför de tre metrar utanför skyddsobjekt som Länsstyrelsen vid diskussion godtagit som acceptabel gräns.

Dataskyddsombudets rekommendationer

Dataskyddsombudets generella reflektion efter arbetet med denna kontroll är att förvaltningen varit motvilligt i att dela med sig av information om användningen av kamerabevakning. Förvaltningen har hänvisat till att det utgör en säkerhetsrisk att tillhandahålla denna information till dataskyddsombudet, med referenser till OSL och säkerhetsskyddslagen. Mer konkret uppgavs att kamerabevakningen utgör en del av säkerhetshöjande åtgärder enligt en antagen säkerhetsskyddsplan, som grundar sig på en säkerhetsskyddsanalys. Genom att röja kamerornas placering menar förvaltningen att nyttan med den säkerhetshöjande åtgärden faller. Vidare skulle ett röjande av kamerornas placering få till följd att förvaltningen röjer information om sina mest känsliga och högst säkerhetsklassade objekt. Detta menar förvaltningen skulle innebära ett brott mot Säkerhetsskyddslagen (2018:585) i enlighet med 2 kap § 2 punkt 2, samt 2 kap § 3. Utöver detta uppgavs även att man enligt Säkerhetsskyddslagen (2018:585) 2 kap § 4 ska förhindra att personer som inte är säkerhetsprövade ges tillgång till säkerhetsskyddsklassificerad information. Att information om bland annat vilka anläggningar som kamerabevakas inte kan tillhandahållas (inte heller muntligt) motiverades med att dataskyddsombudet utgörs av hela dataskyddsenheten, och att samtliga inom enheten då skulle behöva säkerhetsklassas.

Dataskyddsombudet delar förvaltningens bedömning gällande att dessa regelverk ska följas, men vill i sammanhanget poängtera att andra verksamheter inom Göteborgs Stad med skyddsobjekt kunnat samarbeta med och besvara dataskyddsombudets frågor utan att riskera ett röjande av säkerhetsskyddsklassificerad information. Rimligen borde därför även kretslopp och vatten ha kunnat samarbeta med dataskyddsombudet i kontrollen.

Utifrån den knapphändiga information som tillhandahållits har dataskyddsombudet kunnat identifiera ett antal brister, men någon heltäckande rekommendation kan inte ges utifrån det begränsade underlaget. Dock är dataskyddsombudets bedömning att det faktum att brister trots detta kunnat konstateras i sig är en indikation på att en mer genomgående kontroll av förvaltningens kamerabevakning är nödvändig.

Ändamål och rättslig grund

Förvaltningen har uppgett att ändamålet med behandlingen är att förebygga och upptäcka brott riktad mot säkerhetsklassad verksamhet. I enlighet med detta anger förvaltningen rättslig förpliktelse enligt Säkerhetsskyddslagen (2 kap § 3) som rättslig grund för behandlingen. All kamerabevakning sker kopplad till anläggningar dit allmänheten inte har tillträde.

För att få en bättre bild av användningen ombads kretslopp- och vatten att specificera hur kamerabevakningen går till på de olika anläggningarna. Förvaltningen angav då att man inte kan tillhandahålla en djupare beskrivning, utan hänvisar istället till den rutin för kamerabevakning som finns inom förvaltningen.

Konsekvensbedömningar och dokumenterade bedömningar/analyser

En konsekvensbedömning är i vissa fall ett krav enligt dataskyddsförordningen. IMY anger till exempel att systematisk övervakning av en allmän plats i stor omfattning, genom till exempel kameraövervakning, innebär att en konsekvensbedömning ska göras. Även en behandling som sannolikt leder till hög risk för de registrerades fri- och rättigheter kräver att en konsekvensbedömning görs. Syftet med en konsekvensbedömning är att identifiera risker och åtgärder samt bedöma om behandlingen är nödvändig och proportionerlig i förhållande till syftet.

Kretslopp- och vatten hävdar att det finns dokumentation där behovet av kamerabevakning har bedömts utifrån en säkerhetsskyddsanalys. Denna är dock sekretessbelagd enligt OSL kap 15 § 2, och tillhandahålls således inte dataskyddsombudet. De som deltagit i att ta fram analysen är personer med kunskap om och som har ansvar för den säkerhetskänsliga verksamheten. En grundläggande förutsättning för att delta i analysen är att man är säkerhetsprövad. Dataskyddsombudet noterar att den information som behövs för att göra en bedömning om risker specifikt kopplat till behandling av personuppgifter genom kamerabevakningen inte finns tillgänglig, vilket bedöms vara information som förvaltningen ska kunna tillhandahålla dataskyddsombudet inom ramen för kontrollen.

Säkerhet för bevakningen

Förvaltningen uppger att en leverantör är upphandlad som tillhandahåller säkerhetstekniska system. I dessa system ingår den senaste tekniken som är integrerbar med förvaltningens befintliga tekniska system, däribland Petzkameror och klotkameror. Förvaltningen har uppgett att det inte har upprättats några personuppgiftsbiträdesavtal då personuppgiftsbiträdet inte får åtkomst till några personuppgifter.

Förvaltningen uppger att det finns cirka 20 personer som har möjlighet att se kamerabilderna i realtid men att det endast är cirka fem personer som har möjlighet att gå in och titta på äldre inspelat material. Enligt Regionarkivets generella gallringsbeslut AN-04528/18 ska material från kameraövervakning ”gallras när materialet inte längre är nödvändigt för ändamålet”. Kretslopp- och vatten har bedömt att de har behov av att spara materialet i sex månader då allmänheten inte har tillträde till skyddsobjekten som filmas och att eventuella brott bör ha upptäckts inom den tidsperioden. Dataskyddsombudet noterar att detta för kamerabevakningsändamål är att anse som en lång gallringsfrist och att förvaltningen behöver motivera den långa lagringstiden ytterligare. Noteras bör även att förvaltningens bedömning av nödvändig lagringstid ligger långt ifrån tillsynsmyndighetens vägledning om att materialet, som huvudregel, inte bör sparas längre än 72 timmar.

Förvaltningen uppgavs lämna mer information om de leverantörer som används samt vilken teknik som brukas för kamerabevakningen. Ytterligare information om detta vill förvaltningen inte lämna ut med motiveringen att det skulle innebära ett röjande av säkerhetskänslig information. Förvaltningen uppger också att utlämnande av sådan information skulle innebära en ökad risk för sabotage mot systemen. Dataskyddsombudet ställer sig frågande till denna motivering och önskar att förvaltningen tydligare beskriver

hur bedömningen att tillhandahålla av information till dataskyddsombudet skulle öka risken för sabotage.

Information till de registrerade

Om kamerabevakning sker måste information lämnas på ett begripligt och lättillgängligt sätt. IMY rekommenderar att information sker via två så kallade informationslager. Det första ska ges på en varningsskylt med den viktigaste informationen om bevakningen. Ett andra informationslager med all information kan ges på annat sätt.

När det kommer till att upplysa om kamerabevakningen externt har förvaltningen uppgett att det finns skyltar utanpå de större skyddsobjekten, men att det saknas skyltning vid vissa anläggningar. Bristen på komplett information är enligt dataskyddsombudet allvarlig och är något som förvaltningen skyndsamt behöver åtgärda. Då förvaltningen angett att detta ska åtgärdas under hösten önskar dataskyddsombudet en återkoppling på när så skett samt hur informationen på dessa skyltar utformats. Dataskyddsombudet rekommenderar att förvaltningen utgår ifrån den exempelskylt samt övrig information om informationsplikten som finns att tillgå i IMY:s ”Vägledning vid kamerabevakning, Tillstånd till kamerabevakning 2018–2020 – en praxissammanställning, IMY rapport 2021:2”.

I de fall kamerabevakning sker internt på anläggningarna saknas skyltning. Förvaltningen anger att behörig personal informeras genom Intranätet och att det finns interna rutiner för att upplysa mer i detalj om hur kamerabevakningen går till. Gällande samtliga kameror där förvaltningens egen personal filmas finns det för personalen tillgänglig information i rutin *Säkerhetssystem KV Alelyckan*, samt rutinen för kamerabevakning.

Utifrån tillhandahållen information kan inte dataskyddsombudet se att förvaltningen uppfyller kraven enligt GDPR för den personuppgiftsbehandling som kamerabevakningen innebär. En förutsättning för att kunna kamerabevaka är att registrerade informeras om det på ett begripligt och lättillgängligt sätt, vilket inte bedöms vara fallet utifrån avsaknad av skyltning. Även för denna kamerabevakning är bristen på korrekt och komplett information allvarlig och är något som skyndsamt behöver åtgärdas.

Sammanfattande rekommendationer

- Säkerställa att förvaltningen uppfyller informationsplikten genom att kontrollera så att korrekt och komplett information om kamerabevakningen tillhandahålls vid samtliga anläggningar.
- Säkerställa 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.
- Redogöra för den dokumentation som finns gällande bedömning av risker kopplat till behandling av personuppgifter genom kamerabevakningen.
- Förtydliga vilka ställningstaganden som gjorts kopplat till gallringsfristen av det inspelade filmmaterialet i kamerorna. I dagsläget finns detta material tillgängligt i

sex månader, avseende kamerabevakning får detta anses utgöra en lång gallringsfrist.

Bilagor

1. Information om fördjupad kontroll 2022
2. Fördjupad kontroll 2022 Kamerabevakning (del 1)
3. Fördjupad kontroll 2022 Kamerabevakning (del 2)

Bilaga 1

Fördjupad kontroll Kretslopp- och vatten

Kontrollpunkt 11: Kamerabevakning

Personuppgiftsbehandlingar som sker i samband med kamerabevakning behöver uppfylla kraven i dataskyddsförordningen. Därtill finns reglering i form av kamerabevakningslagen (2018:1200), vars syfte bl.a. är att säkerställa att fysiska personer skyddas mot otillbörligt intrång i den personliga integriteten. Sedan lagens införande 2018 har det skett vissa förändringar inom kamerabevakningsområdet och flera aktörer undantas nu från det tidigare kravet på att ansöka om tillstånd.

Även om en verksamhet inte behöver ansöka om tillstånd för att få kamerabevaka är det viktigt att den som bedriver bevakning beaktar reglerna i dataskyddsförordningen och säkerställer att nödvändiga bedömningar görs och dokumenteras. Den som använder kamerabevakning behöver också säkerställa att tillräcklig information lämnas om den aktuella bevakningen, för vilket det finns specifika krav.

Granskningen avser att kontrollera huruvida verksamhetens användning av kamerabevakning uppfyller dataskyddsförordningen och kamerabevakningslagen, med fokus på dokumenterade bedömningar, om tillräcklig information lämnas till de registrerade och i förekommande fall om tillstånd finns.

Tillvägagångssätt

Den fördjupade kontrollen kommer att genomföras i två delar. I del ett ombeds ni att skicka in dokumenterade instruktioner/rutiner samt besvara ett antal frågor. I del två kommer uppföljande frågor att ställas.

Dataskyddsombudet kommer sedan att sammanställa underlaget i en delårsrapport som lämnas till er i juni.

Bilaga 2

Fördjupad kontroll 2022 - Kamerabevakning

Del 1

Ni ombeds besvara följande frågor samt skicka in dokumenterade rutiner, instruktioner, styrande dokument eller liknande avseende er användning av kamerabevakning.

1. Vilka platser kamerabevakar ni? Detta ska beskrivas även utifrån vilka områden/ytor på platsen som kamerabevakas tex. entrén utvändigt, entrén invändigt, trapphus, specifika rum. a. Ange ändamålet och rättslig grund för behandlingen/behandlingarna. b. Har ni sökt tillstånd för den kamerabevakning som ni utför? Om inte ange varför.

2. Har ni utfört konsekvensbedömningar eller andra typer av dokumenterade bedömningar/analyser för er kamerabevakning? Om ja, skicka även in denna dokumentation.

3. Vilken teknik använder ni och vilka leverantörer använder ni? a. Finns personuppgiftsbiträdesavtal upprättade med de leverantörer som ni använder? Bifoga dessa avtal.

4. Hur informerar ni de registrerade om kamerabevakningen som utförs? Bifoga den information som ni tillhandahåller de registrerade och ange hur den tillgängliggörs.

Obs! Det är mycket viktigt att frågorna besvaras av eller i samråd med rätt befattningar/roller inom förvaltningen/bolaget för att resultatet ska bli korrekt. Säkerställ även en lämplig förankring av svaren inom organisationen innan de översänds till dataskyddsombudet.

Underlaget ska ha inkommit till dataskyddsombudet senast den 15 mars 2022.

Har du frågor, kontakta ditt huvudansvarige dataskyddsombud.

Bilaga 3

Fördjupad kontroll Kretslopp- och vatten

Kontrollpunkt 11: Kamerabevakning (del 2)

Ni ombeds besvara följande **uppföljande/förtydligande frågor** samt skicka in viss dokumentation avseende er användning av kamerabevakning.

1. Vilka platser kamerabevakar ni? Detta ska beskrivas även utifrån vilka områden/ytor på platsen som kamerabevakas tex. entrén utvändigt, entrén invändigt, trapphus, specifika rum.

    - **Uppföljande fråga:** Förvaltningen bedömer sig inte kunna besvara dataskyddsombudets frågor gällande vilka specifika delar som kamera bevakas då det anses utgöra en säkerhetsrisk. Utan den begärda informationen kan dataskyddsombudet inte utföra sitt uppdrag. Dataskyddsombudet vill därför ta del av förvaltningens dokumenterade bedömning i frågan, inkl. hänvisningar till tillämpliga lagrum för att inte tillgängliggöra den begärda informationen.
        a. Ange ändamålet och rättslig grund för behandlingen/behandlingarna.
        b. Har ni sökt tillstånd för den kamerabevakning som ni utför? Om inte, ange varför.

    - **Uppföljande fråga:** Förvaltningen bedömer inte att dataskyddsombudet kan ta del av exempel på de tillstånd som förvaltningen har för kamerabevakningen då det anses utgöra en säkerhetsrisk. Utan den begärda informationen kan dataskyddsombudet inte utföra sitt uppdrag. Dataskyddsombudet vill ta del av förvaltningens dokumenterade bedömning i frågan, inkl. hänvisningar till tillämpliga lagrum för att inte tillgängliggöra den begärda informationen.

2. Har ni utfört konsekvensbedömningar eller andra typer av dokumenterade bedömningar/analyser för er kamerabevakning? Om ja, skicka även in denna dokumentation.

- **Uppföljande fråga:** Då förvaltningen i del 1 inte besvarade frågan om ifall konsekvensbedömningar eller andra typer av dokumenterade bedömningar/analyser är genomförda för kamerabevakningen, kvarstår denna i del 2.

  Förvaltningen bör, oaktad eventuell sekretess, kunna ange ifall någon konsekvensbedömning genomförts för kamerabevakningen. Om en konsekvensbedömning gjorts önskar dataskyddsombudet ta del av förvaltningens motivering till varför inte dataskyddsombudet involverats i arbetet med denna.

3. Vilken teknik använder ni och vilka leverantörer använder ni?

   - **Uppföljande frågor:** Förvaltningen anger att filmerna i kamerorna lagras i sex månader innan de gallras. Hur har förvaltningen gjort bedömningen att filmerna behöver sparas i sex månader? Hur bedöms proportionaliteten och nödvändigheten i denna del av behandlingen? Bifoga eventuell dokumentation.

     Dataskyddsombudet önskar också en mer utförlig beskrivning av den teknik som används. Kan personer identifieras? Skiljer detta sig mellan de platser som kamera bevakas? Om filter används, är detta permanent eller kan det lyftas bort? Sker inspelningen med ljudupptagning? Vem/vilka har tillgång till filmerna? Etc.

   a. Finns personuppgiftsbiträdesavtal upprättade med de leverantörer som ni använder? Bifoga dessa avtal.

4. Hur informerar ni de registrerade om kamerabevakningen som utförs? Bifoga den information som ni tillhandahåller de registrerade och ange hur den tillgängliggörs.

Kompletterande förtydligande fråga:
Dataskyddsombudet efterfrågar en beskrivning av hur kamerabevakningen på de olika platserna används. Är det t.ex. enbart inspelat material som förvaltningen tittar på vid behov i efterhand eller sker realtidsövervakning? Ange även när kamerabevakningen sker och, om denna sker dygnet runt, om anställda som arbetar på platserna därmed förekommer på filmerna. Vilka åtgärder har förvaltningen vidtagit för att minimera kamerabevakningens påverkan på de anställdas integritet?

Obs! Det är mycket viktigt att frågorna besvaras av eller i samråd med rätt befattningar/roller inom förvaltningen/bolaget för att resultatet ska bli korrekt. Säkerställ även en lämplig förankring av svaren inom organisationen innan de översänds till dataskyddsombudet. Om ni inte vet hur frågan ska besvaras, fråga t.ex. dataskyddskontakten eller dataskyddsombudet.

Underlaget ska ha inkommit till dataskyddsenheten **senast den 5 augusti 2022.**

Har ni frågor, kontakta dataskyddsenheten (dso@intraservice.goteborg.se).