Göteborgs Stad

Årsrapport för dataskyddsarbetet 2022

Göteborgs Spårvägar AB

2022-12-22

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

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

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 en kontroll av bolagets användning av kamerabevakning. Resultatet av kontrollen presenteras i sin helhet i bilaga 2.

Dataskyddsombudet har i rapporten gjort flera iakttagelser som innebär att bolaget avseende sin kamerabevakning inte uppfyller kraven enligt aktuell rättslig reglering och har därför lämnat ett antal rekommendationer till verksamheten om att vidta åtgärder.

Sammanfattade rekommendationer:

- Utreda och slutligen ta ställning till samt dokumentera bedömning av personuppgiftsansvaret avseende kamerabevakning på spårvagnar

- Utreda behandlingen och personuppgiftsansvaret vid den behandling av personuppgifter som sker via tillgång till bildströmmar från trafikkontorets kameror. Om rättsliga förutsättningar saknas behöver behandlingen omedelbart avbrytas.
- Genomför översyn av beslut om tillstånd för kamerabevakning vid depå Slottsskogen och depå Majorna
- Utreda och ta ställning till om kameror i porttelefoner utgör kamerabevakning enligt definitionen och om tillstånd behöver sökas
- Se över lagringstid för inspelat material och tydligt motivera och dokumentera bedömningarna
- Dokumentera ändamål och rättslig grund för kamerabevakning vid depåer
- Utreda och dokumentera ändamål och rättslig grund för kameror i porttelefoner. Om ändamål och rättslig grund saknas behöver behandlingen avbrytas.
- Genomföra/färdigställa konsekvensbedömningar för samtliga behandlingar gällande kamerabevakning där detta krävs.
- Komplettera styrande dokument med information om vad som gäller för kamerabevakning/personuppgiftsbehandlingar via kamera vid depåer samt porttelefoner
- Skyndsamt åtgärda bristande information till registrerade avseende kamerabevakning/personuppgiftsbehandlingar vid depåer samt porttelefoner. Om bolaget har personuppgiftsansvar för behandling via trafikkontorets kameror behöver informationsplikten uppfyllas även här.

2.2.2 Uppföljning av tidigare genomförda kontroller

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

Fördjupad kontroll (2021): Hantering av anställdas personuppgifter: Positioneringsteknik (GPS)

Verksamheten gavs följande rekommendationer:

- Genomföra en kartläggning av personuppgiftsbehandlingar där positioneringsteknik används och/eller förekommer, och bedöma huruvida behandlingarna kan motiveras med hänvisning till ändamål, nödvändighet och rättslig grund.
- Genomföra konsekvensbedömningar för identifierade personuppgiftsbehandlingar där positioneringsteknik används och/eller förekommer.
- Skriftligen informera de anställda om personuppgiftsbehandlingarna

Kommentarer och rekommendationer:

Uppföljningen visar att verksamheten har påbörjat åtgärder i enlighet med lämnade rekommendationer. Bolaget har pågående konsekvensbedömningar avseende

personlarm och GPS-enheter i bilar och arbetar med att ta fram heltäckande information till de registrerade.

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

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]

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 Göteborgs Spårvägar AB:s 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

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

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:

Bolaget har inom denna punkt angett varierande värden i sin skattning där flera påståenden skattas med det högsta värdet och två med det näst lägsta. Svaren indikerar att bolaget inte anser att dataskydd är en integrerad och naturlig del i alla verksamhetens delar och det kan utläsas att det saknas rutiner för att regelbundet involvera dataskyddsombudet. Dataskyddsombudet delar denna uppfattning och bedömer att det krävs insatser för att komma till rätta med bristerna.

Det är positivt att bolaget anser sig ha definierade roller och ansvar och att det finns tydligt utpekat vem som ska göra vad och vilka rapporteringsvägar som ska följas. Dataskyddsombudets uppfattning är att detta funnits under en begränsad tid och anser att bolaget behöver utvärdera sitt arbetssätt och undersöka om det följs och om det är ändamålsenligt och effektivt.

Dataskyddsombudet rekommenderar att bolaget utreder hur de olika verksamhetsdelarna kan involveras i dataskyddsarbetet för att säkerställa att dataskyddsorganisationen når ut till samtliga delar. För att göra dataskydd till en naturlig och självklar del av det dagliga arbetet krävs också att det inom alla delar finns förståelse för att GDPR är en lag jämte de många andra som måste följas och att lagstiftningen varken är valbar eller något som kan prioriteras bort.

Utifrån skattningen rekommenderas att bolaget tar fram rutiner som säkerställer att dataskyddsombudet på ett mer systematiskt sätt informeras om och involveras i alla frågor rörande dataskydd.

2.4.2 Kontrollpunkt 2: Personuppgiftsincidenter

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

Dataskyddsombudets kommentarer:

Bolagets arbete med personuppgiftsincidenter sker enligt skattningen på ett övergripande systematiskt och effektivt sätt. Dataskyddsombudet delar överlag denna uppfattning men vill ändå lyfta att det, trots riskplaceringen, finns åtgärder som behöver vidtas.

Bolaget har skattat sig lågt vad gäller att regelbundet informera medarbetare om vad personuppgiftsincidenter är och hur de ska hanteras. Det är en grundläggande förutsättning för ett fullgott dataskyddsarbete att alla som behöver det har fått utbildning och information om dataskydd. I detta ingår att utbilda om personuppgiftsincidenthantering. Utan utbildning och information riskerar många incidenter att missas vilket kan medföra att brister i skyddet av personuppgifter inte upptäcks. Dataskyddsombudet rekommenderar att bolaget tar fram en rutin för att regelbundet och vid behov säkerställa att medarbetare informeras om vad personuppgifter är och hur dessa ska hanteras inom bolaget.

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:

Utifrån bolagets skattning finns det inom detta område omfattande risker som omgående kräver åtgärder. Bolaget har angett att det finns tecknat personuppgiftsbiträdesavtal i ca 50 % av fallen då detta krävs, att det till stor del saknas efterlevnadskontroller och att det inte finns tillräckliga rutiner/kompetens för att bedöma hela kedjan av biträden/underbiträden.

Eftersom avsaknaden av biträdesavtal utgör en hög risk för bolaget rekommenderar dataskyddsombudet att det omgående genomförs en kartläggning av behandlingar där biträden anlitas, för att därigenom kunna identifiera i vilka fall det behöver upprättas personuppgiftsbiträdesavtal.

Bolaget rekommenderas också att ta fram rutiner för att kontrollera anlitade biträden samt för att vid anlitande av nya biträden kontrollera deras underbiträden. Det behöver också säkerställas att det inom bolaget finns kompetens att bedöma denna kedja. Utifrån det ansvar bolaget har vid anlitande av biträden enligt artikel 28 GDPR (den s.k. ”omsorgsplikten”) föreligger här en risk för att bolaget inte kan uppfylla kraven enligt GDPR och bolaget rekommenderas att under det kommande året prioritera arbetet med personuppgiftsbiträdesavtal.

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:

Dataskyddsombudet tolkar bolagets svar i denna del som att det finns en dokumenterad ansvarsfördelning för att hålla behandlingarna i registret uppdaterade men att i princip allt övrigt saknas. Eftersom endast ca 25 % av bolagets behandlingar finns upptagna i registret och de som är angivna där inte anges innehålla den information som krävs finns det här stora risker för bolaget.

Utöver att det i de flesta fall är ett krav enligt förordningen att ha ett aktuellt och uppdaterat personuppgiftsregister, kan det också vara ett användbart hjälpmedel i verksamhetens dataskyddsarbete då det ger en överblick över de behandlingar som sker. Utifrån bolagets egen skattning uppfyller bolaget inom denna punkt inte sina skyldigheter enligt GDPR. Dataskyddsombudet rekommenderar därför att bolaget prioriterar arbetet med personuppgiftsregistret.

2.4.5 Kontrollpunkt 5: Övergripande strategi för dataskydd

Kontrollpunkten avser verksamhetens övergripande strategi för att arbeta med dataskydd.

Dataskyddsombudets kommentarer:

Bolagets svar indikerar att det inom denna kontrollpunkt finns risker som kräver åtgärder, särskilt vad gäller att ha en övergripande strategi och att arbeta systematiskt med dataskyddsfrågor. En avsaknad av överblick och tydlig styrning i hur dataskyddsarbetet bedrivs innebär stora risker eftersom man bland annat riskerar att fokusera sina resurser på fel frågor.

Utifrån den egna skattningen rekommenderas bolaget att i dokumenterade handlings- och/eller verksamhetsplan, rutiner och policys tydliggöra sin strategi för det övergripande dataskyddsarbetet.

Bolaget rekommenderas också att säkerställa att verksamhetens informationstillgångar identifieras och värderas utifrån behovet av konfidentialitet, riktighet och tillgänglighet i enlighet med stadens styrande dokument inom informationssäkerhet. Man rekommenderas även att ta fram och fastställa en informationssäkerhetspolicy som på ett tydligt och enkelt sätt tillgängliggörs för berörda medarbetare.

2.4.6 Kontrollpunkt 6: Utbildning

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

Dataskyddsombudets kommentarer:

Bolaget har inom denna punkt angett varierande värden i sin skattning vilket genererar en placering inom risknivå tre. Det kan utifrån svaren utläsas att medarbetare regelbundet ges möjlighet att delta i utbildningar och att det i relativt hög utsträckning genomförs regelbundna utbildningsinsatser. Det kan dock även utläsas att den allmänna kunskapsnivån inte är tillräckligt god, att kunskapsnivån inte följs upp tillräckligt och att det behöver ske en kartläggning av kunskapsnivå och utbildningsbehov för roller och befattningar.

En grundläggande förutsättning för att kunna säkerställa ett fullgott dataskyddsarbete är att verksamhetens medarbetare har tillräcklig kunskap om hur de ska hantera personuppgifter på rätt sätt. För att kunna säkerställa att medarbetarna erbjuds rätt utbildningsinsatser rekommenderas bolaget att kartlägga vilka utbildningar och andra kompetenshöjande insatser som behövs inom verksamheten, samt följa upp kunskapsnivån efter genomförda utbildningar. Det rekommenderas också att bolaget ser över de regelbundna utbildningarna som ändå verkar erbjudas och säkerställa att dessa leder till en högre allmän kunskapsnivå inom dataskydd.

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:

Bolaget har i denna del angett genomgående låga värden i sin skattning vilket medför en placering i riskområde ett vilket indikerar att det här finns höga risker. I förhållande till förra årets enkät utgör detta en försämring men dataskyddsombudet vill här notera att detta troligtvis ger en mer rättvisande bild över hur väl bolaget i denna del uppfyller sina skyldigheter enligt GDPR. Dataskyddsombudet anser det vara mycket positivt att bolaget har insikt i vilka brister som finns och därmed belyser aktuella risker.

Utifrån gällande rättslig reglering, vägledningar samt aktuell praxis kan det konstateras att det ställs mycket höga krav på personuppgiftsansvariga att informera registrerade om hur deras personuppgifter behandlas. En förutsättning

för att kunna göra detta korrekt är att ha överblick, kontroll och kunskap om de behandlingar som utförs. Bolaget har i vissa delar arbetat med att se över och revidera informationen som ges till registrerade, vilket är positivt. Eftersom det är många behandlingar som det fortfarande inte ges information om kvarstår emellertid ett stort arbete.

Bolaget rekommenderas att kartlägga vilka behandlingar som man i dagsläget inte informerar om, ta fram en plan för hur denna information ska ges och arbeta med att säkerställa att den är komplett. Bolaget rekommenderas även att ta fram rutiner som anger både instruktioner kring när/hur policyn ska uppdateras och också utpekar vem/vilken roll inom bolaget som ansvarar för att detta görs. Ytterligare rekommendationer kopplat till informationsskyldigheten framgår även av den fördjupade kontrollen.

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:

Dataskyddsombudet har ingen anledning att göra en annan bedömning än den som bolaget har gjort avseende risknivå kopplat till dokumenthantering, gallring och informationsklassningen. I sammanhanget rekommenderas bolaget att följa upp och kontrollera så att hanteringen av personuppgifter i e-post genomförs i enlighet med gällande rutiner och anvisningar.

Principerna om uppgifts- och lagringsminimering är grundläggande i dataskyddsförordningen. Det ställs också höga krav på att hantera uppgifter tillräckligt säkert. Bolagets svar visar att det finns behov av att se över verksamhetens informationsklassificering av personuppgiftsbehandlingar, och kontrollera så att detta görs i enlighet med Göteborgs Stads riktlinjer för informationssäkerhet. Det behöver även tas fram anvisningar för hur information i olika informationsklasser ska hanteras och vilka lagringsytor som får användas. För att verksamheten ska kunna säkerställa att rätt nivå av skydd bibehålls behöver även dessa bedömningar regelbundet ses över. Göteborgs Spårvägar AB rekommenderas därför ta fram en handlingsplan för arbetet med att informationsklassificera personuppgiftsbehandlingar, anvisning för hur lagring/hantering får ske samt rutiner som säkerställer en regelbunden uppföljning av klassningen.

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:

Att genomföra konsekvensbedömningar är i många fall ett absolut krav och om detta inte genomförs riskerar man som verksamhet att missa att vidta åtgärder som behövs för att säkerställa de registrerades rättigheter. Vid en tillsyn kan det också innebära sanktionsavgifter från tillsynsmyndigheten. Arbetet med konsekvensbedömningar bör vara en del av den övergripande strategin för dataskyddsarbetet i verksamheten och den interna dataskyddsorganisationen bör fungera på ett sätt som säkerställer att inga nya eller förändrade behandlingar påbörjas utan att en bedömning görs om behovet av en konsekvensbedömning.

Utifrån skattningen rekommenderar dataskyddsombudet att bolaget genomför en kartläggning för att identifiera för vilka högriskbehandlingar som konsekvensbedömningar saknas samt ta fram handlingsplan för att genomföra dem. Bolaget rekommenderas också att ta fram rutiner för att säkerställa att konsekvensbedömningar genomförs i rätt tid och i enlighet med GDPR, samt att det sker uppföljning av redan genomförda konsekvensbedömningar samt rutin för att följa upp beslutade åtgärder. Vidare rekommenderas bolaget att ta fram rutiner för inhämtande av registrerades synpunkter.

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:

Bolaget har på denna punkt skattat sitt arbete med låga och medellåga värden vilket innebär att det här finns risker identifierade som omgående behöver åtgärder. Dataskyddsombudet har ingen anledning att göra en annan bedömning än den som bolaget här gör.

Här vill dataskyddsombudet särskilt lyfta införandet av det nya systemet för händelserapportering där dataskyddsfrågor inte beaktats i tillräcklig utsträckning eller i rätt tid. Dataskyddsombudet har själv fått be om uppdateringar och lägesrapporter och dataskyddsbedömningar har enligt dataskyddsombudet inte avhandlats med tillräcklig hänsyn till gällande lagstiftning. Trots att bolaget arbetat

med införandet under lång tid har dataskyddsfrågorna först beaktats mot slutet och i mycket nära anslutning till införandet trots medvetenhet om att underlag tar tid att ta fram och att ändringar och justeringar kan behöva göras beroende på vilka risker som framkommer vid en konsekvensbedömning. Hanteringen visar enligt dataskyddsombudet på bristande kompetens och indikerar att det saknas förståelse för vikten av att säkerställa skydd för personuppgifter.

Mot bakgrund av bolagets egen skattning rekommenderar dataskyddsombudet att bolaget tar fram rutiner för att säkerställa dataskyddsperspektivet från start vid införande av nya lösningar. Bolaget rekommenderas också att ta fram rutiner för att via kravställning säkerställa skyddet av personuppgifter och säkerställa följsamhet mot GDPR vad gäller inbyggt dataskydd och dataskydd som standard. Bolaget behöver även säkerställa att dataskyddsombudet involveras redan från start vid införande av nya tjänster och i projekt och att kontinuerliga uppdateringar sker.

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:

Bolaget har genomgående angett låga och medellåga värden i skattningen på denna punkt. Dataskyddsombudet har under året inte fått indikationer som innebär en avvikande bedömning. Sammantaget indikerar skattningen att bolaget inte anser sig ha överblick över sina IT-system och digitala verktyg, kontroll över hur det ges tillgång/behörighet till dessa och hur användandet följs upp och kontrolleras. Dataskyddsombudet rekommenderar därför att bolaget kartlägger alla de IT-system och digitala verktyg som används och säkerställer att de kontrolleras för följsamhet mot GDPR.

Bolaget rekommenderas också att ta fram rutiner för att säkerställa att dataskyddsperspektivet vid införande och användandet av kostnadsfria tjänster som t.ex. gratisappar. Det behöver även finnas överblick över kommunikationskanaler och rutin för att kontrollera att dessa uppfyller kraven enligt GDPR.

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:

Bolaget har inom denna punkt angett varierande värden i skattningen och det kan utläsas att bolaget anser sig i viss mån ha koll på hantering av begäran om registerutdrag men att det finns brister vad gäller beredskap för att hantera vissa andra rättigheter. Dataskyddsombudet gör ingen annan bedömning än den som bolaget gör i denna del.

Bolaget rekommenderas att genom utbildning eller informationsinsatser stärka medvetenheten om registrerades rättigheter, ta fram process för att få fram efterfrågad information vid begäran om registerutdrag samt säkerställa att bolaget har förutsättningar att bedöma inkomna invändningar.

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 bolaget under 2023 prioriterar följande delar av dataskyddsarbetet:

- Kontrollpunkt 3: Biträdesavtal och andra överenskommelser
- Kontrollpunkt 4: Personuppgiftsregister
- Kontrollpunkt 10: IT-projekt och upphandling

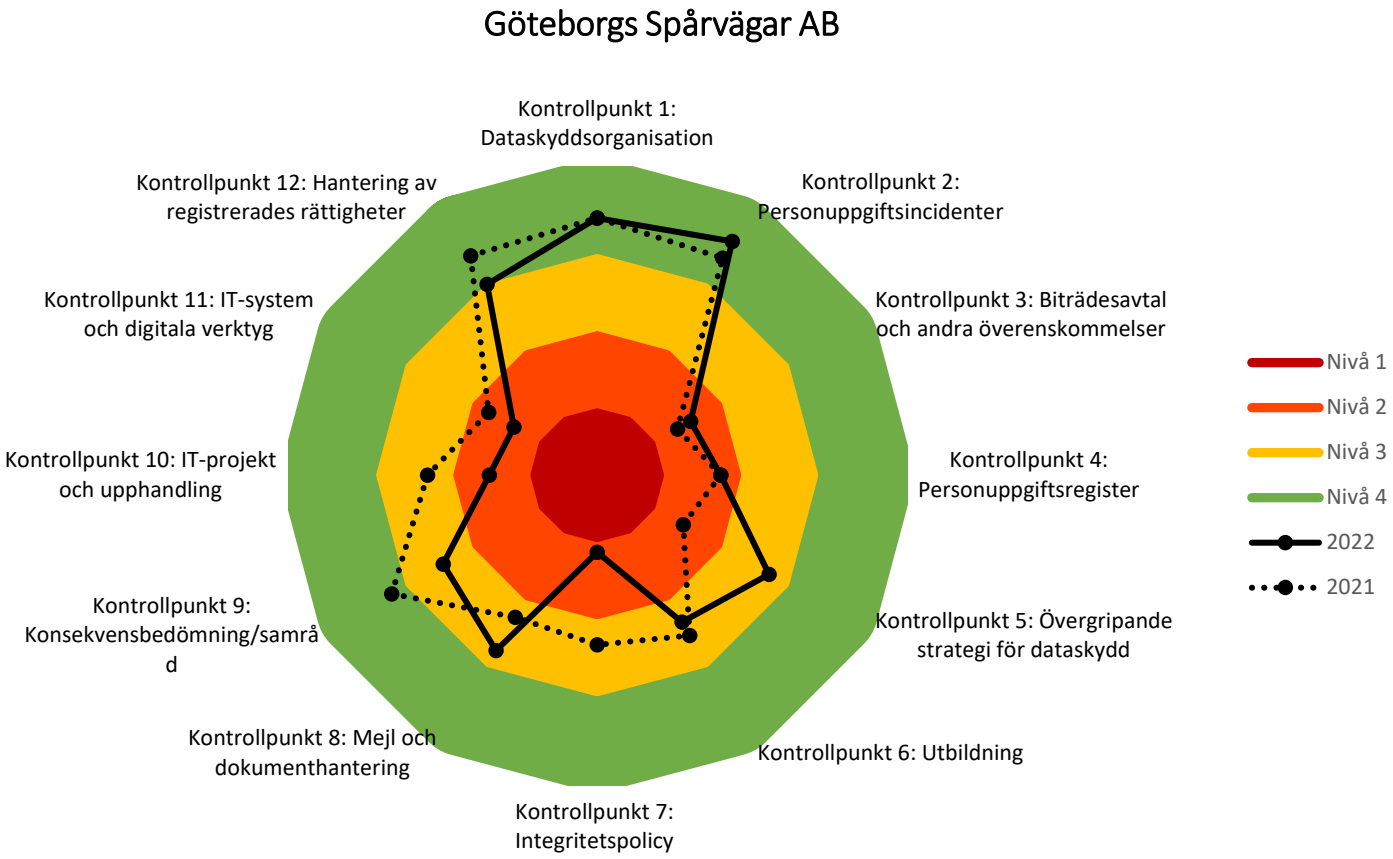
3 Bilagor

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

Bilaga 2: Fördjupad kontroll 2022, kamerabevakning

Bilaga 1

Diagram över resultat av fasta kontrollpunkter, jämfört med 2021.



Fördjupad kontroll

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.

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 GDPR. 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.

Göteborgs Spårvägar AB:s användning av kamerabevakning

Göteborgs Spårvägar AB (GSAB) använder kameror för att bevaka depåområden samt i porttelefoner till entréer. Bolaget har emellertid uttryck osäkerhet kring om kamerorna kopplade till porttelefonerna utgör kamerabevakning enligt definitionen.

Bolaget angav inledningsvis i kontrollen att det också sker kamerabevakning på spårvagnar i staden och att man även för denna bevakning var personuppgiftsansvarig. Denna uppfattning har under kontrollens gång justerats eftersom Västtrafik hävdar att de är personuppgiftsansvariga för denna kamerabevakning och att GSAB istället är personuppgiftsbiträde. Dataskyddsombudets uppfattning är att detta dock inte är helt utrett och dataskyddsombudet uppmanar därför bolaget att omgående utreda frågan för att i så fall kunna ta fullt ansvar enligt GDPR.

Dataskyddsombudets generella reflektion efter arbetet med denna kontroll är att det har varit mycket svårt att få tydlig och konkret information från bolaget om hur, när och varför bolaget kamerabevakar. Ny eller justerad information har vid flera tillfällen framkommit efter att följd/kontrollfrågor ställts vilket enligt dataskyddsombudet indikerar att det saknas överblick och kontroll hos bolaget. För vissa frågor saknas dessutom fortfarande svar. Detta är enligt dataskyddsombudet allvarligt och anmärkningsvärt, särskilt eftersom kamerabevakning är en åtgärd som ska användas restriktivt och endast efter grundliga och kompletta bedömningar och analyser.

Det finns också en stor oklarhet kopplad till de kameror som enligt bolaget ägs av trafikkontoret och vars material GSAB har tillgång till. GSAB har angett att bolaget för dessa är personuppgiftsbiträde till trafikkontoret och att det finns tillgång till flertalet kameror. Huruvida detta är avstämt med trafikkontoret och om det finns personuppgiftsbiträdesavtal med förvaltningen är oklart. Mot bakgrund av att det är omständigheterna som avgör vem som är ansvarig respektive biträde anser dataskyddsombudet det vara mycket oklart huruvida bolaget verkligen är biträde. Dataskyddsombudet rekommenderar därför att bolaget, tillsammans med trafikkontoret, går igenom vem som har tillgång till vad, varför tillgången behövs och vem som följaktligen har ansvaret.

Dataskyddsombudets rekommendationer

Tillstånd

GSAB angav i sitt första svar på kontrollen avseende depåerna att endast den bevakning som sker vid Slottskogsdepån är tillståndspliktig och att det för denna bevakning finns tillstånd. Bolaget ändrade sedan sitt svar och angav att även kamerabevakning för sin depå i Majorna är tillståndspliktig och att tillstånd finns, vilket också bifogades. I beslutet anges att kamerabevakningen sker i realtid och det inte sker någon inspelning/lagring. Av svar på fråga om hur lagring ser ut för den kamerabevakning som sker vid depåerna har dock dataskyddsombudet fått motstridig information eftersom bolaget då svarat att lagring sker och att material sparas i sju dagar. Detta gäller enligt svaren både för Majorna och för Slottsskogen.

Att övervakningen enbart skulle ske i realtid har enligt Länsstyrelsen (som 2017 då beslutet fattades ansvarade för dessa tillstånd, IMY har sedan dess tagit över detta ansvar)

påverkat beslutet eftersom det begränsar integritetsintrånget. Beslutet gäller dessutom uttryckligen enbart för kameraövervakning dygnet runt *i realtid*. Om bolaget utför annan typ av kamerabevakning är det dataskyddsombudets uppfattning att tillståndet inte längre är giltigt och att ett nytt tillstånd, om tillstånd fortfarande krävs, behöver sökas med en korrekt återgivning av omständigheterna kring bevakningen. Dataskyddsombudet rekommenderar att det omgående görs en översyn av beslutet.

Dataskyddsombudet har inte sett tillståndsbeslutet för kamerabevakningen vid Slottskogsdepån men rekommenderar att även detta kontrolleras och ses över av bolaget.

Vad gäller porttelefonerna som är utrustade med kamera är det dataskyddsombudets uppfattning att detta kan röra sig om kamerabevakning såsom den definieras i kamerabevakningslagen. Med kamerabevakning menas ”*att en tv-kamera, ett annat optisk-elektroniskt instrument eller en därmed jämförbar utrustning, utan att manövreras på platsen, används på ett sätt som innebär varaktig eller regelbundet upprepad personbevakning*”. Utrustningen som används passar in i definitionen och eftersom kameran aktiveras vid varje påringning kan det nog också anses vara regelbundet upprepad personbevakning. Bolaget rekommenderas att utreda och dokumentera sin bedömning om porttelefonerna i detta avseende. GSAB har inte svarat på frågan om vilket ändamål och rättlig grund man har för personuppgiftsbehandlingen som sker och det är för dataskyddsombudet därför oklart om bevakningen kan vara tillståndspliktig. Bolaget rekommenderas att omgående utreda detta och ta ställning till om tillstånd behöver sökas eller ej. Det ska understrykas att även om kamerorna vid porttelefonerna inte skulle anses utgöra kamerabevakning enligt definitionen så är det fortfarande en personuppgiftsbehandling vilket medför att kraven i GDPR ändå behöver följas.

Tider och platser som kamerabevakas

Dataskyddsombudet tolkar de inkomna svaren som att kamerabevakningen vid depåerna sker dygnet runt och att det inspelade materialet sparas i sju dagar. GSAB har också skickat in skisser över vilket upptagningsområde kamerorna vid depåerna har. Avseende porttelefonerna tolkar dataskyddsombudet det som att de filmar vid påringning och att bildströmmen endast är tillgänglig i realtid. Det framgår inte vilket upptagningsområde dessa kameror har.

Vad gäller upptagningsområdet är det viktigt det enbart omfattar det som syftet med bevakningen kräver och alltså inte samlar in fler personuppgifter än vad som är nödvändigt. Dataskyddsombudet har utifrån det inlämnade underlaget inga synpunkter på depåkamerornas upptagningsområde.

Utifrån det angivna syftet med depåkamerorna (förebygga och förhindra brott samt säkerställa flöde vid inkörning av spårvagn, förbereda vagnsfördelning och upptäcka/förhindra stopp i körfält) förefaller det rimligt att kamerabevakningen sker dygnet runt. Mot bakgrund av att huvudregeln för lagring av inspelat material, om lagring behöver ske, är 72 h behöver det ses över om inte lagringstiden, som i dagsläget är sju dagar, kan förkortas. I detta kan det t.ex. vägas in hur lång tid det tar för verksamheten att upptäcka en incident och hur lång tid det tar att omhänderta materialet för att skicka det till polisen vid brott. Dataskyddsombudet rekommenderar att bolaget ser över lagringstiden och om en längre tid än 72 h bedöms vara nödvändig, tydligt motiverar och dokumenterar denna bedömning.

Ändamål och rättslig grund

Depåer

Som angivits ovan har ändamålet med dessa kamerabevakningar angivits vara att förbygga/förhindra brott samt av trafikskäl. Rättslig grund för detta är enligt bolaget allmänt intresse. Svaren som inkommit i denna del har enligt dataskyddsombudet varit spretiga och ger inte intrycket att bolaget helt vet vad ändamålet är. Detta visas också av att bolaget för depån i Majorna har behövt korrigera sitt svar avseende om tillstånd finns eller inte, där det inledningsvis angetts att det enbart har skett bevakning utifrån en trygghets/brottsförebyggande synpunkt, vilket sedan visat sig inte stämma. Att ha ett tydligt avgränsat ändamål är en grundläggande del i att följa dataskyddsförordningen och för en så pass integritetsingripande åtgärd som kamerabevakning, som dessutom kan vara tillståndspliktig, får det inte finnas några tvivel kring vilka dessa ändamål är. Dataskyddsombudet rekommenderar därför att bolaget för varje depå där kamerabevakning sker tydligt dokumenterar ändamålet med bevakningen samt tydligt anger vilken rättslig grund som finns för behandlingarna.

Porttelefoner

Bolaget har för den personuppgiftsbehandling som sker via porttelefonerna inte angivit vilket ändamål man har eller vilken rättslig grund som bolaget tillämpar. Huruvida detta beror på slarv från bolagets sida eller om det inte finns en utförd bedömning är för dataskyddsombudet oklart. Om det beror på det senare utgör det en allvarlig brist som dataskyddsombudet rekommenderar att bolaget åtgärdar omedelbart. Om det saknas ändamål och rättslig får en behandling inte utföras och bolaget behöver avbryta behandlingarna.

Trafikkontorets kameror

Som framgår ovan har bolaget angett att man är personuppgiftsbiträde i förhållande till trafikkontoret. Dataskyddsombudet har inte tagit del av den utredning som denna bedömning grundar sig på. Dataskyddsombudet anser det dock, till skillnad från bolaget, att det nog är mer sannolikt att man skulle vara att betraktas som personuppgiftsansvarig för den behandling som sker när GSAB tar del av bildströmmarna. Det skulle innebära att det i så fall behöver finnas ett ändamål och en rättslig grund, bland annat. Om bolaget är personuppgiftsansvarig och detta inte finns skulle behandlingen omgående behöva avbrytas. Dataskyddsombudet rekommenderar, som också framgår inledningsvis, att frågan utreds tillsammans med trafikkontoret.

Konsekvensbedömningar och dokumenterade bedömningar/analyser

Bolaget har i svaret till dataskyddsombudet inkluderat en riskbedömning för kamerabevakning vid depåerna. Det anges också att det finns pågående konsekvensbedömningar för depåerna och för porttelefonerna.

Eftersom kamerabevakningen som bolaget utför medför personuppgiftsbehandlingar ska det enligt GDPR bedömas om kravet för att genomföra konsekvensbedömningar är uppfyllt. Även om en verksamhet har tillstånd för kamerabevakningen behöver denna bedömning göras. Eftersom bolaget anger att det finns påbörjade konsekvensbedömningar utgår dataskyddsombudet från att bolaget bedömt att kraven för

konsekvensbedömningar för de angivna behandlingarna är uppfyllda. Dataskyddsombudet rekommenderar att bolaget prioriterar arbetet med dessa konsekvensbedömningar mot bakgrund av de risker som finns för de registrerade i och med bevakningen.

Säkerhet för bevakningen

Vad gäller porttelefonerna anges det att kamerorna enbart filmar i realtid och att lagring alltså inte sker. Leverantören av dessa kameror behandlar enligt bolaget inga personuppgifter och är alltså inte att betrakta som personuppgiftsbiträden. Enligt bolagets svar är det receptionspersonal samt anställda på trafikledning som har tillgång till bildströmmen.

Vad gäller kamerorna på depåerna lagras det inspelade materialet på en intern server och leverantören av dessa kameror anges inte heller på något sätt behandla bolagets personuppgifter varför inte heller denna leverantör bedömts vara personuppgiftsbiträde. Av inlämnat svar är det tre personer/roller som har tillgång till det inspelade materialet vilka utgörs av säkerhetschef, trafiksäkerhetschef samt säkerhetsutvecklare. Bolaget har även bifogat styrande dokument kopplat till kamerabevakning, dessa utgörs av ”Regler för tystnadsplikt gällande hantering av videoinspelat material från kameraövervakning”, ”Göteborgs Spårvägars policy för kamerabevakning” och ”Regler för videodiskhantering samt hantering av material från bevakningskamera”. Dataskyddombudet anser det positivt att bolaget arbetar aktivt med styrande dokument vilket kan utgöra en viktig del i arbetet med att säkerställa skyddet för personuppgifter. Den framtagna policyn är dock generellt formulerad och skulle behöva kompletteras av ytterligare regler för hur den praktiska hanteringen får gå till. Reglerna för videodiskhantering är mer praktiskt och konkret men verkar främst beröra hanteringen av inspelat material från spårvagnar, där det är oklart om spårvägen ens är personuppgiftsansvarig. Dataskyddsombudet rekommenderar därför att de styrande dokumenten kompletteras med information om vilka regler som gäller för bolagets kamerabevakning vid depåerna samt för kamerabevakningen-/personuppgiftsbehandlingen som sker via porttelefonerna.

Information till de registrerade

Depå

Bolaget har skickat in bilder på de skyltar som finns uppsatta vid depåerna i Majorna och Slottsskogen för att informera om att det förekommer kamerabevakning. Denna information uppfyller inte det kravet på information enligt dataskyddsförordningen. Bolaget har också angett att ingen ytterligare information finns tillgänglig för anställda som får sina personuppgifter behandlade via bevakningen. Bristen på korrekt och komplett information är enligt dataskyddsombudet allvarlig och är något som bolaget skyndsamt behöver åtgärda. Dataskyddsombudet rekommenderar att bolaget 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”.

Porttelefoner

Vad gäller porttelefonerna anger bolaget att ingen information om personuppgiftsbehandlingen finns att tillgå. Oaktat om behandlingen innebär kamerabevakning eller ej behöver informationsplikten uppfyllas. Dataskyddsombudet rekommenderar att avsaknaden av information åtgärdas omgående.

Vad gäller behandlingen via trafikkontorets kameror och kamerorna på spårvagnarna är, som tidigare konstaterats, personuppgiftsansvaret oklart. Om det framkommer att bolaget har ett personuppgiftsansvar behöver informationsplikten uppfyllas även för dessa behandlingar.

Sammanfattade rekommendationer

- Utreda och slutligen ta ställning till samt dokumentera bedömning av personuppgiftsansvaret avseende kamerabevakning på spårvagnar
- Utreda behandlingen och personuppgiftsansvaret vid den behandling av personuppgifter som sker via tillgång till bildströmmar från trafikkontorets kameror. Om rättsliga förutsättningar saknas behöver behandlingen omedelbart avbrytas.
- Genomför översyn av beslut om tillstånd för kamerabevakning vid depå Slottsskogen och depå Majorna
- Utreda och ta ställning till om kameror i porttelefoner utgör kamerabevakning enligt definitionen och om tillstånd behöver sökas
- Se över lagringstid för inspelat material och tydligt motivera och dokumentera bedömningarna
- Dokumentera ändamål och rättslig grund för kamerabevakning vid depåer
- Utreda och dokumentera ändamål och rättslig grund för kameror i porttelefoner. Om ändamål och rättslig grund saknas behöver behandlingen avbrytas.
- Genomföra/färdigställa konsekvensbedömningar för samtliga behandlingar gällande kamerabevakning där detta krävs.
- Komplettera styrande dokument med information om vad som gäller för kamerabevakning/personuppgiftsbehandlingar via kamera vid depåer samt porttelefoner
- Skyndsamt åtgärda bristande information till registrerade avseende kamerabevakning/personuppgiftsbehandlingar vid depåer samt porttelefoner. Om bolaget har personuppgiftsansvar för behandling via trafikkontorets kameror behöver informationsplikten uppfyllas även här.

Bilagor

- Information om fördjupad kontroll 2022
- Frågeunderlag fördjupad kontroll 2022, del 1 och 2

Information om fördjupad kontroll 2022

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.

Fördjupad kontroll 2022

Kontrollpunkt 11: 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.
    c. Är ni ensamt personuppgiftsansvariga för den kamerabevakning som utförs? Om inte, beskriv hur personuppgiftsansvaret är uppdelat.
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.

Fördjupad kontroll 2022

Kontrollpunkt 11: Kamerabevakning (del 2)

Ni ombeds besvara följande **uppföljande 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.
    - *GSAB:s svar:*
        1. *Spårvagn.*
        2. *Vid påringning på porttelefon på Depå Rantorgets entré plan 1 och plan 2 startar en realtidsövervakning. Utvändig övervakning.*
        3. *Vid påringning på porttelefon vid staketgräns på depå Ringön startar en realtidsövervakning. Utvändig övervakning.*
        4. *Vid påringning på porttelefon entré in till Trafikledningen på Depå Rantorget startar en realtidsövervakning. Utvändig övervakning.*
        5. *Vid påringning på porttelefon entré in till Trafikledningen från korridor på Depå Rantorget startar en realtidsövervakning. Invändig övervakning.*
        6. *Depåområde Majorna. Utvändig övervakning – Se område bifogad fil*
        7. *Depåområde Slottsskogen. Utvändig över vakning – Se område på bifogad fil.*
    - **Uppföljande fråga:** I ett annat svar anges att kameror finns i Hammarkullen, som inte är med i listan. Beskriv hur kamerorna i Hammarkullen sitter och används.
        a. Ange ändamålet och rättslig grund för behandlingen/behandlingarna.
    - *GSAB:s svar: Göteborgs Spårvägar anser att kamerabevakningen är en behandling som är nödvändig för att utföra en uppgift av allmänt intresse enligt artikel 6.1e i dataskyddsförordningen.*
    - **Uppföljande fråga:** Svaret innehåller endast redogörelse om rättslig grund, ange också ändamålet med respektive behandlingen. Ange även den reglering ur vilken det går att

utläsa att behandlingen (kamerabevakningen) är av allmänt intresse. Glöm alltså inte att ange rättslig grund och ändamål för samtliga förekomster av kamerabevakning.

   b. Har ni sökt tillstånd för den kamerabevakning som ni utför? Om inte ange varför.
   c. Är ni ensamt personuppgiftsansvariga för den kamerabevakning som utförs? Om inte, beskriv hur personuppgiftsansvaret är uppdelat.

- *GSAB:s svar: GS är ensamt personuppgiftsansvariga för samtliga kameror förutom ev. kamerorna i Hammarkullen som ägs av Trafikkontoret. Det är enbart ett fåtal anställda på Göteborgs Spårvägar som kan ta del av inspelning från kamerorna på spårvagnarna. Dessa arbetar på Säkerhetsenheten, 12 personer samt 1 person på IT-enheten. Västtrafik eller annan part kan inte se inspelat material. Hammarkullens kameror ägs av Trafikkontoret. Materialet visas i realtid. Trafikledningen GS kan se bilder från kamerorna. Så även ett fåtal personer på Trafikkontoret.*
- **Uppföljande fråga:** Vad menas ”ev. kamerorna i Hammarkullen”? Är frågan inte utredd? Motivera ert svar.

2. Har ni utfört konsekvensbedömningar eller andra typer av dokumenterade bedömningar/analyser för er kamerabevakning? Om ja, skicka även in denna dokumentation.
   - **Uppföljande fråga:** Den bifogade riskanalysen har rubriken ”*Konsekvensbedömning kamerabevakning på spårvagn, dnr 122-21*”. Själva konsekvensbedömningen är emellertid inte inskickad, finns det en sådan konsekvensbedömning? I så fall, skicka in underlaget. Finns det riskanalyser utförda även för kamerabevakning på depåerna och porttelefonerna? Skicka in eventuellt underlag.
3. Vilken teknik använder ni och vilka leverantörer använder ni?
   a. Finns personuppgiftsbiträdesavtal upprättade med de leverantörer som ni använder? Bifoga dessa avtal.
      - *GSAB:s svar: Nej, varken Stanley Security eller LåsTeam är ej bärare av personuppgifter som uppkommer i och med kamerabevakning.*
      - **Uppföljande frågor:** Har ni alltså gjort bedömningen att de leverantörer som används inte är personuppgiftsbiträden till Göteborgs Spårvägar AB? Beskriv i så fall hur verksamheten har kommit till denna slutsats.
4. Hur informerar ni de registrerade om kamerabevakningen som utförs? Bifoga den information som ni tillhandahåller de registrerade och ange hur den tillgängliggörs.
   - **Uppföljande fråga:** Bifoga kopior på den information som ges till de registrerade. Vi vill alltså veta vilken information som finns uppsatt t.ex. vid de olika depåerna, vid porttelefonerna

och vilken information som ges till dem som reser med spårvagn.

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 dataskyddsombudet **senast den 9 juni 2022.**

Har du frågor, kontakta huvudansvarigt dataskyddsombud.