Årsrapport för dataskyddsarbetet 2023

Göteborgs Spårvägar AB

2023-12-18

Innehåll

1 Inledning

Dataskyddsförordningen (GDPR) har tillkommit för att särskilt skydda människors rätt till integritet, och för att värna var och ens rätt att få ha kontroll över vad som sker med uppgifter om ens person. Rätten till en fredad privat sfär och personlig integritet är grundläggande i ett demokratiskt samhälle och är ett av fundamenten på vilket många andra av våra demokratiska rättigheter vilar. Dataskyddsreglerna styr hur personuppgifter får samlas in, användas och hanteras för att säkerställa att uppgifterna används korrekt och rättvist. Lagstiftningen finns till för att skydda individen från skada och sätter ramarna för hur personuppgifter får behandlas i en alltmer digital värld. Dataskydd handlar i grunden om att skapa ett socialt hållbart samhälle.

1.1 Dataskyddsombud i Göteborgs Stad

I Göteborgs Stad fullgör dataskyddsenheten på Intraservice uppdraget som dataskyddsombud för förvaltningar och bolag. Vad som är dataskyddsombudets uppgifter framgår direkt av lagstiftningen. Dataskyddsombudet ska ge råd, rekommendationer och informera om frågor som rör behandlingar av personuppgifter. Dataskyddsombudet har även i uppdrag att oberoende granska verksamheternas arbete med dataskyddsfrågor för att säkerställa att dataskyddslagstiftningen efterlevs.

Enligt lag ska dataskyddsombudet rapportera till högsta förvaltningsnivå och i Göteborgs Stad innebär det att dataskyddsombudet rapporterar direkt till nämnder och styrelser. Dataskyddsombudet lämnar årligen en rapport om verksamhetens dataskyddsarbete till varje nämnd och bolag i Göteborgs Stad. I rapporten redogör dataskyddsombudet för de iakttagelser som gjorts och det kontrollarbete som genomförts. För 2023 bestod kontrollarbetet av en granskning av fasta kontrollpunkter och i årsrapporten presenteras resultaten från denna tillsammans med dataskyddsombudets bedömning. Årsrapporten innehåller även resultaten från dataskyddsombudets årliga uppföljning av verksamhetens hantering av lämnade rekommendationer från tidigare genomförda kontroller.

Årsrapporten är avsedd att kunna användas som ett stöd för verksamheten i sitt fortsatta arbete med dataskydd. Det är upp till varje verksamhet att besluta om hur det interna dataskyddsarbetet ska utformas utifrån verksamhetens förutsättningar för att på bästa sätt kunna hantera identifierade risker.

2 Särskilda iakttagelser 2023

2.1 Stadenövergripande

2.1.1 Förutsättningar för en hållbar digitalisering

Fokus på ny teknik och AI har en enorm potential för att göra våra liv bättre, men den digitala utvecklingen blir inte hållbar utan begränsningar. Utan tydlig styrning i arbetet med digital innovation är risken att det går fort och att man i sin iver att röra sig framåt glömmer att hänsyn behöver tas till den personliga integriteten och att personuppgifter behandlas på ett korrekt sätt. Verksamheter i Göteborgs stad behöver tydligt ha med sig integritetsaspekten vid framtagandet av innovativa och nya lösningar inom till exempel AI. Arbetet med att säkerställa att personuppgifter behandlas enligt reglerna i dataskyddslagstiftningen behöver genomsyra arbetet inom de kommunala verksamheterna på alla olika plan. Det gäller allt från rutiner och processer för det dagliga arbetet, till arbetet med innovations- och digitaliseringslösningar för framtidens arbetssätt inom Göteborgs Stad.

Som en stor offentlig aktör har Göteborg som stad att förvalta alla invånare och besökares förtroende. Oavsett om det handlar om elever, vårdnadshavare, brukare inom socialtjänst, eller någon annan kategori av kommuninvånare, så ska man kunna känna sig trygg med att användandet av innovativ teknik sker med respekt för den personliga integriteten och de regelverk som finns för att skydda enskildas personuppgifter. I takt med att tekniken tar en allt större plats i våra liv ökar också riskerna för att spåra och övervaka människor. På det rättsliga området har detta fört med sig att regleringarna på EU-nivå blir fler och alltmer komplexa. För att utvecklingen ska kunna ske på ett långsiktigt hållbart sätt är det nödvändigt att varje verksamhet förstår de regelverk som finns, och varför de finns. Man kan naturligtvis se det som en balansakt, men som dataskyddsombud vill vi vara extra tydliga med att balansen alltid behöver vara lagd till de enskilda registrerades fördel och aldrig får innebära att verksamheter tummar på det regelverk som finns till för att skydda personuppgifter. Verksamheterna behöver följa dataskydds-lagstiftningen på samma sätt som man behöver följa all annan lagstiftning.

3 Granskning av dataskyddsarbetet 2023

3.1 Kontroll av fasta kontrollpunkter

Under 2023 har dataskyddsombudet kontrollerat verksamhetens dataskyddsarbete utifrån de tolv fasta kontrollpunkterna. Kontrollen har genomförts genom en enkät. Enkäten består av tolv punkter (”fasta kontrollpunkter”) där varje punkt innehåller ett antal delfrågor i form av påståenden och/eller skattningsfrågor. Enkäten är avsedd att spänna över de viktigaste delarna inom dataskyddsarbetet för att på så sätt fånga in en större bredd av frågor. Metoden syftar till att få till ett långsiktigt och systematiskt arbetssätt som möjliggör uppföljning över tid.

I arbetet används en modell som består av fyra kategorier, vilka representerar fyra olika risknivåer. Verksamheten får utifrån sina svar ett värde som visar vilken risknivå verksamheten befinner sig på inom respektive kontrollpunkt. Genom att arbeta med risknivåer möjliggörs ett riskbaserat arbetssätt för både verksamhet och dataskyddsombud, då resultaten ger en bild av vad verksamheten behöver prioritera i dataskyddsarbetet framåt.[1]

Risknivå	Beskrivning	Färgkod
Nivå 1	Höga risker identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten.	
Nivå 2	Risker identifierade som bedöms vara omfattande och/eller kräver omgående åtgärder.	
Nivå 3	Risker identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga.	
Nivå 4	Inga direkta risker av betydelse identifierade. Indikerar att verksamheten bedriver ett systematiskt dataskyddsarbete.	

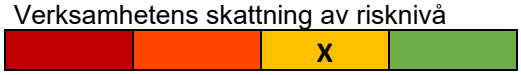
3.2 Resultat från kontrollen 2023

I detta avsnitt anges vilken risknivå verksamheten befinner sig inom för respektive kontrollpunkt, baserat på verksamhetens svar på de fasta kontrollpunkterna. Under varje kontrollpunkt presenteras även dataskyddsombudets bedömning gällande verksamhetens risker utifrån de iakttagelser som dataskyddsombudet gjort under året. För beskrivning av respektive kontrollpunkt se bilaga 2.

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

3.2.1 Kontrollpunkt 1: Dataskyddsorganisation

Verksamhetens skattning av risknivå



Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger risker som behöver åtgärdas, men att dessa inte är brådskande, omfattande eller allvarliga.

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

Svaren från bolaget indikerar att organisationen inte anser att dataskydd är en integrerad och naturlig del i alla verksamhetens delar och det kan också utläsas att det saknas dokumenterade arbetssätt för att regelbundet involvera dataskyddsombudet. Det framgår även tydligt att det saknas tillräckliga resurser för ett fullgott dataskyddsarbete.

Genom dialog med verksamheten har dataskyddsombudet uppfattat att det i organisationen i stort verkar finnas en ovilja att ta hänsyn till dataskyddsfrågor. Denna tendens är också något som dataskyddsombudet noterat i flera av de frågor som verksamheten involverat dataskyddsombudet i, till exempel frågan om drogtester vid anställning av sommarvikarier. För att göra dataskydd till en naturlig och självklar del av det dagliga arbetet krävs det att det inom alla delar av verksamheten finns förståelse för att GDPR är en lag jämte många andra lagar som måste följas och att lagstiftningen varken är valbar eller något som kan prioriteras bort. För att leva upp till lagstiftningens krav är det också en förutsättning att dataskyddsorganisationen inom bolaget har tillräckliga resurser till sitt förfogande.

I besvarandet av årets enkät har verksamheten involverat fler delar av organisationen vilket har gett ett lägre, men mer rättvisande resultat av bolagets risknivåer inom de olika kontrollpunkterna. Dataskyddsombudet ser detta som ett positivt steg, även om resultatet som sådant då blir sämre.

Dataskyddsombudet rekommenderar bolaget att:

- Utreda hur, och säkerställa att resurser kan allokeras för att ett fullgott dataskyddsarbete ska kunna bedrivas.

- Utreda hur, och säkerställa att de olika verksamhetsdelarna kan involveras i dataskyddsarbetet för att säkerställa att dataskyddsorganisationen når ut till samtliga delar.

- Ta fram definierade rapporteringsvägar för att säkerställa att relevant information om dataskyddsfrågor når rätt nivå inom verksamheten.

- Ta fram dokumenterade arbetssätt som säkerställer att dataskyddsombudet på ett mer systematiskt sätt informeras om och involveras i alla frågor rörande dataskydd.

- Tillse att dataskyddsperspektivet beaktas vid inledandet av alla personuppgiftsbehandlingar.

3.2.2 Kontrollpunkt 2: Personuppgiftsincidenter

Verksamhetens skattning av risknivå

Dataskyddsombudets bedömning

Bolagets resultat indikerar att det inom kontrollpunkten föreligger risker som behöver åtgärdas, men att dessa inte är brådskande, omfattande eller allvarliga.

Dataskyddsombudet har inte involverats i några frågor kopplat till kontrollpunkten, men har ingen anledning att göra en annan bedömning än den som verksamheten har gjort avseende risknivå. Av bolagets egen skattning framgår dock att det saknas ett systematiskt arbete med att följa upp inträffade incidenter.

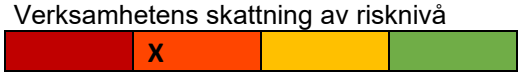
Dataskyddsombudet rekommenderar bolaget att:

- Ta fram dokumenterade arbetssätt som möjliggör uppföljning av dokumenterade incidenter och som gör att sådan uppföljning blir en naturlig del i dataskyddsarbetet.

- Ta fram dokumenterade arbetssätt för att på ett korrekt sätt avgöra när och hur man ska kunna informera de registrerade vid en inträffad personuppgiftsincident.

3.2.3 Kontrollpunkt 3: Biträdesavtal och andra överenskommelser

Verksamhetens skattning av risknivå



Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger omfattande risker som kräver omgående åtgärder

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

Det är också oroande att många av dessa risker är kvarstående från föregående år och att de rekommendationer som dataskyddsombudet lämnade då inte verkar ha hörsammats eller åtgärdats av verksamheten. De rekommendationer som lämnas nu är därför i allt väsentligt dom samma som de som lämnades 2022. 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.

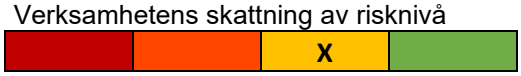
Eftersom avsaknaden av biträdesavtal och dokumenterade arbetssätt inom området utgör en hög risk för bolaget rekommenderar dataskyddsombudet verksamheten att:

- Omgående genomföra en kartläggning av behandlingar där biträden anlitas, för att därigenom kunna identifiera i vilka fall det behöver upprättas personuppgiftsbiträdesavtal.

- Ta fram rutiner för att kontrollera anlitade biträden samt för att vid anlitande av nya biträden kontrollera deras underbiträden.

3.2.4 Kontrollpunkt 4: Register över personuppgiftsbehandlingar

Verksamhetens skattning av risknivå



Dataskyddsombudets bedömning

Bolagets resultat indikerar att det inom kontrollpunkten föreligger risker som behöver åtgärdas, men att dessa inte är brådskande, omfattande eller allvarliga.

Dataskyddsombudet har inte involverats i några frågor kopplat till kontrollpunkten, men har ingen anledning att göra en annan bedömning än den som verksamheten har gjort avseende risknivå. Utifrån bolagets svar har dataskyddsombudets rekommendationer från tidigare år till viss del omhändertagits, men utifrån den egna skattningen är det tydligt att det fortfarande finns saker som behöver förbättras.

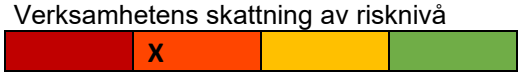
Dataskyddsombudet rekommenderar bolaget att:

- Säkerställa att de behandlingar som dokumenterats i behandlingsregistret innehåller all den information som krävs enligt artikel 30 i GDPR.

- Ta fram ett fungerande och dokumenterat arbetssätt för att kontinuerligt uppdatera registret med behandlingar som tillkommit eller förändrats.

3.2.5 Kontrollpunkt 5: Övergripande styrning av dataskyddsarbetet

Verksamhetens skattning av risknivå



Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger omfattande risker som kräver omgående åtgärder.

Dataskyddsombudet delar bolagets bedömning om att det förekommer risker som är omfattande och kräver omgående åtgärder. Oroande är att ingen av de rekommendationer som dataskyddsombudet lämnade i 2022 års rapport verkar ha omhändertagits. Snarare förefaller det, att döma av bolagets egen skattning, som att bolaget tagit några kliv bakåt i sitt systematiska arbete inom kontrollpunkten.

Bolagets svar indikerar att det saknas en övergripande strategi för 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 och lägga sina resurser på fel frågor.

Utifrån den egna skattningen rekommenderas bolaget att:

- Tydliggöra sin strategi för det övergripande dataskyddsarbetet i dokumenterade arbetssätt.

- Säkerställa att verksamhetens informationstillgångar identifieras och värderas utifrån behovet av konfidentialitet, riktighet och tillgänglighet i enlighet med stadens styrande dokument inom informationssäkerhet.

- Ta fram och fastställa en informationssäkerhetspolicy som på ett tydligt och enkelt sätt tillgängliggörs för berörda medarbetare.

- Regelbundet genomföra interna efterlevnadskontroller för att säkerställa följsamhet mot GDPR.

3.2.6 Kontrollpunkt 6: Utbildning

Verksamhetens skattning av risknivå

Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger risker som behöver åtgärdas, men att dessa inte är brådskande, omfattande eller allvarliga.

Dataskyddsombudet har inte involverats i några frågor kopplat till kontrollpunkten under året, men har ingen anledning att göra en annan bedömning än den som verksamheten har gjort avseende risknivå. Att döma av verksamhetens egen skattning har också fler av dataskyddsombudets tidigare rekommendationer omhändertagits och markanta förbättringar har skett, bland annat avseende kartläggningen av vilken kunskapsnivå som krävs för olika befattningar, vilket är mycket positivt. Samtidigt framgår det att den generella kunskapsnivån om dataskyddsfrågor fortfarande är för låg.

Dataskyddsombudet rekommenderar bolaget att:

- Fortsätta verka för att höja kunskapsnivån inom den egna organisationen genom informations- och utbildningsinsatser.

- Ta fram dokumenterade arbetssätt för att följa upp och bibehålla kunskapsnivån hos medarbetarna efter det att utbildningar har genomförts.

3.2.7 Kontrollpunkt 7: Informationsplikt

Verksamhetens skattning av risknivå

Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger omfattande risker som kräver omgående åtgärder.

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

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. Av verksamhetens egen skattning framgår att det finns brister i den information som lämnas till de registrerade både avseende innehåll och tillgänglighet. Det finns också brister i verksamhetens arbete med att kontinuerligt se över och uppdatera informationen.

Bolaget har tagit fram en ny integritetspolicy vilken dataskyddsombudet har tagit del av för att lämna synpunkter. Man har också arbetat med att lämna korrekt information i form av skyltning i anslutning till den kamerabevakning som bolaget utför. Att verksamheten arbetar aktivt med frågan är positivt och ett bra första steg. Mycket arbete kvarstår dock.

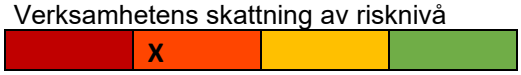
Dataskyddsombudet rekommenderar bolaget att:

- Se över all information som lämnas till de registrerade och tillse att den uppfyller kraven i artikel 12–14 i GDPR.

- Ta fram dokumenterade arbetssätt för att säkerställa att informationen kontinuerligt ses över och hålls uppdaterad.

3.2.8 Kontrollpunkt 8: E-post och dokumenthantering

Verksamhetens skattning av risknivå



Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger omfattande risker som kräver omgående åtgärder.

Dataskyddsombudet har inte involverats i några frågor kopplat till kontrollpunkten, men har ingen anledning att göra en annan bedömning än den som verksamheten har gjort avseende risknivå. I allt väsentligt är dock riskerna kvarstående från föregående år och tidigare rekommendationer kvarstår därför.

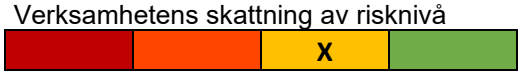
Bolagets svar visar att det finns behov av att se över verksamhetens informationsklassificering av personuppgiftsbehandlingar, och att kontrollera så att detta görs i enlighet med Göteborgs Stads riktlinjer för informationssäkerhet. Det behöver även tas fram anvisningar för hur information i olika informationsklasser 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.

Dataskyddsombudet rekommenderar bolaget att:

- I första hand ta fram en handlingsplan för arbetet med att informations-klassificera personuppgiftsbehandlingar, och sedan genomföra klassning.
- Ta fram dokumenterade arbetssätt som säkerställer en regelbunden uppföljning av klassningen.
- Ta fram dokumenterade arbetssätt för att informera medarbetarna om dokumenthantering och gallring kopplat till kraven i GDPR, inbegripet hanteringen av personuppgifter i e-post.
- Informera de registrerade direkt i samband med upprättande av kontakt om hur deras personuppgifter hanteras.

3.2.9 Kontrollpunkt 9: Konsekvensbedömning/samråd

Verksamhetens skattning av risknivå



Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger risker som behöver åtgärdas, men att dessa inte är brådskande, omfattande eller allvarliga.

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

Dataskyddsombudets bedömning är att bolaget i grund och botten har de förutsättningar som krävs vad gäller kunskap och kompetens för att kunna bedriva ett fullgott arbete med konsekvensbedömningar. Verksamhetens svar indikerar också detta och visar att det finns dokumenterade arbetssätt på plats för att kunna arbeta korrekt och effektivt med frågorna. Dataskyddsombudets uppfattning är att verksamheten kommit i gång med sitt bedömningsarbete på ett bra sätt. I likhet med många andra verksamheter i Göteborgs stad har dock bolaget en restskuld av behandlingar med höga risker för vilka man inte hunnit göra någon konsekvensbedömning.

Med ledning av den dialog som dataskyddsombudet fört med verksamheten avseende konsekvensbedömningar som genomförts under året vill dataskyddsombudet också särskilt lyfta att det trots god kompetens hos verksamheten verkar föreligga vissa oklarheter kring syftet med en konsekvensbedömning och hur dessa ska genomföras. Dataskyddsombudet uppfattar inte dessa oklarheter som ett utslag av bristande kompetens, utan snarare som en otydlig styrning och oklara mandat kring genomförandet av konsekvensbedömningar. Syftet med en konsekvensbedömning är att förutsättningslöst kartlägga riskerna för de registrerade med en personuppgiftsbehandling, inte att försöka bortse från uppenbara risker i syfte att legitimera genomförandet av en behandling. Bolaget behöver därför ta ett omtag kring hur arbetet med konsekvensbedömningar ska utföras och framför allt tydliggöra ansvarsfördelningen kring genomförandet.

Dataskyddsombudet rekommenderar bolaget att:

- Ta fram konsekvensbedömningar för behandlingar med höga risker som man ännu inte har bedömt.

- Ta fram dokumenterade arbetssätt för hur beslut om att vidta åtgärder för att möta kvarstående risker ska hanteras och dokumenteras, samt för hur uppföljning ska ske för de åtgärder som beslutats.

- Tydliggöra vem som har mandat inom organisationen att genomföra och fastställa konsekvensbedömningar.

3.2.10 Kontrollpunkt 10: IT-projekt och upphandling

Verksamhetens skattning av risknivå

Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger risker som behöver åtgärdas, men att dessa inte är brådskande, omfattande eller allvarliga.

Dataskyddsombudet delar till viss del verksamhetens bedömning, men gör till skillnad ifrån verksamheten bedömningen att det inom kontrollpunkten

förekommer risker som är omfattande och kräver omgående åtgärder. Ett exempel på detta är införandet av bolagets system för händelserapportering där dataskyddsfrågor inte beaktats i tillräcklig utsträckning eller i rätt tid. Trots att bolaget arbetat med införandet under lång tid har dataskyddsfrågorna först beaktats mot slutet och i mycket nära anslutning till införandet. Detta 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. Enligt dataskyddsombudets uppfattning visar hanteringen på bristande kompetens och indikerar att det saknas förståelse för vikten av att säkerställa skydd för personuppgifter.

Mot bakgrund av detta, och utifrån bolagets egen skattning rekommenderar dataskyddsombudet att bolaget:

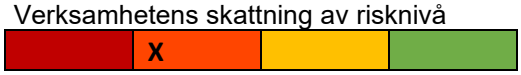
- Alltid beaktar dataskyddsperspektivet genom att systematiskt och kontinuerligt bedöma risker med personuppgiftsbehandlingar i samband med införande av nya system och digitala lösningar

- Via kravställning säkerställer skyddet av personuppgifter och följsamhet mot GDPR, vad gäller principerna om inbyggt dataskydd och dataskydd som standard. Samt ser till att det finns dokumenterade arbetssätt inom organisationen som gör att detta följs.

- Säkerställer att det finns dokumenterade arbetssätt som gör att dataskyddsombudet involveras redan från start vid införande av nya tjänster och i projekt och att kontinuerliga uppdateringar kommuniceras vid förändringar av betydelse.

3.2.11 Kontrollpunkt 11: IT-system och digitala verktyg

Verksamhetens skattning av risknivå



Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger omfattande risker som kräver omgående åtgärder.

Dataskyddsombudet har inte involverats i några frågor kopplat till kontrollpunkten, bortsett ifrån bolagets användning av kamerabevakning (se fördjupad kontroll och uppföljning av denna) men har ingen anledning att göra en annan bedömning än den som verksamheten har gjort avseende risknivå.

Bolaget har genomgående angett låga och medellåga värden i skattningen på denna punkt. 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.

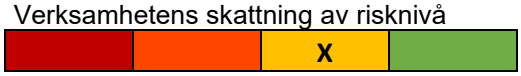
Dataskyddsombudet rekommenderar därför att bolaget:

- Kartlägger alla de IT-system och digitala verktyg som används och säkerställer att de kontrolleras för följsamhet mot GDPR.

- Tar fram dokumenterade arbetssätt för tilldelning av behörigheter och åtkomster i IT-system, som säkerställer att medarbetares tillgång till personuppgifter är anpassade och begränsade till det som är nödvändigt för att medarbetaren ska kunna utföra sina arbetsuppgifter.

3.2.12 Kontrollpunkt 12: Hantering av registrerades rättigheter

Verksamhetens skattning av risknivå



Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger risker som behöver åtgärdas, men att dessa inte är brådskande, omfattande eller allvarliga.

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

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

Bolaget rekommenderas att:

- Genom utbildning eller informationsinsatser inom organisationen stärka medvetenheten om de registrerades rättigheter och när dessa begränsas.

- Säkerställa att dokumenterade arbetssätt finns på plats för att bedöma inkomna invändningar och hantera situationer där de registrerades rättigheter begränsas.

3.3 Uppföljning

3.3.1 Uppföljning av rekommendationer lämnade inom ramen för tidigare genomförda kontroller

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

Kontroll (2022): Fördjupad kontroll av kamerabevakning

Verksamheten gavs följande 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.

Kommentarer och rekommendationer:

Uppföljningen visar att verksamheten fortfarande har förbättringsområden inom denna kontroll. Följande åtgärder har vidtagits

- Översyn av beslut om tillstånd för bevakning av depåer har utförts. Tillstånd kommer sökas för de platser där bevakningen är tillståndspliktig.

- Frågan om porttelefoner är utredd och tillstånd kommer sökas för kamerabevakning

- Ändamål och rättslig grund har dokumenterats för kamerabevakning vid depåer.

Följande rekommendationer återstår och uppföljning av dessa kommer att ske under 2024.

- *Utred och slutligen ta ställning till samt dokumentera bedömning av personuppgiftsansvaret avseende kamerabevakning på spårvagnar*
  Bolaget har i sitt svar på dataskyddsombudets uppföljning angett att Västtrafik anser sig personuppgiftsansvarig för all kamerabevakning på spårvagnar. I dialog med verksamheten under december 2023 framkommer dock att Västtrafik ånyo ändrat inställning i frågan. Dataskyddsombudets rekommendation om att slutligen ta ställning i frågan kvarstår därför.

- *Utred behandlingen och personuppgiftsansvaret vid den behandling av personuppgifter som sker via tillgång till bildströmmar från trafikkontorets kameror.* Bolaget har uppgett att personuppgiftansvaret för bevakningen vid Hammarkullens station är utrett. Dataskyddsombudet noterar dock att övrig kamerabevakning inom gemensam trafikledning för spår (TLI) fortfarande är under utredning. Rekommendationen kvarstår därför.

- *Se över lagringstid för inspelat material och tydligt motivera och dokumentera bedömningarna. Bolaget har utfört en översyn och gjort bedömningen att lagringstiden är motiverad utifrån personalresurser.* Dataskyddsombudet har tagit del av bedömningen men anser inte att verksamhetens hänvisning till personalresurser är tillräckligt för att motivera lagringstiden på 168 timmar. Rekommendationen kvarstår därför.

- *Genomföra/färdigställa konsekvensbedömningar för samtliga behandlingar gällande kamerabevakning där detta krävs.* Dataskyddsombudet saknar fortfarande fullständiga och uppdaterade konsekvensbedömningar för bolagets användning av kamerabevakning och bolaget har uppgett att man

efter inrådan från dataskyddsombudet kommer ta ett omtag i frågan. Rekommendationen kvarstår därför.

- *Komplettera styrande dokument med information om vad som gäller för kamerabevakning/personuppgiftsbehandlingar via kamera vid depåer samt porttelefoner.* Komplettering av styrande dokument behöver fortfarande genomföras. Rekommendationen kvarstår därför.

- *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.* Verksamheten uppger att korrekt skyltning av kamerabevakade platser är på gång men att fördröjning har skett på grund av arbetet med intern och extern integritetspolicy. Rekommendationen kvarstår därför.

4 Rekommenderade fokusområden 2024

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

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

- Kontrollpunkt 1: Dataskyddsorganisation
  Dataskyddsombudet rekommenderar att bolaget lägger fokus på att se över kontrollpunkten i sin helhet för att säkerställa en ändamålsenlig och adekvat resurssatt dataskyddsorganisation med tydliga mandat att driva dataskyddsfrågor i verksamheten.

- Kontrollpunkt 3: Biträdesavtal och andra överenskommelser
  Bolaget rekommenderas att genomföra en kartläggning av behandlingar där biträden anlitas, för att därigenom kunna identifiera i vilka fall det behöver upprättas personuppgiftsbiträdesavtal.

  Ta fram rutiner för att kontrollera anlitade biträden samt för att vid anlitande av nya biträden kontrollera deras underbiträden.

- Kontrollpunkt 11: IT system och andra verktyg (Kamerabevakning)
  Bolaget bör prioritera att omhänderta samtliga kvarstående rekommendationer ifrån dataskyddsombudets fördjupade kontroll från 2022 avseende bolagets användning av kamerabevakning.

5 Bilagor

Bilaga 1: Diagram över resultat av fasta kontrollpunkter, jämfört med 2022.

Bilaga 2: Kontrollplan för dataskyddsarbetet 2023–2024