Göteborgs Stad

Årsrapport för dataskyddsarbetet 2023

Göteborgs Stads Kollektivtrafik AB

2023-12-20

Innehåll

1 Inledning

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

1.1 Dataskyddsombud i Göteborgs Stad

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

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

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

2 Särskilda iakttagelser 2023

2.1 Stadenövergripande

2.1.1 Förutsättningar för en hållbar digitalisering

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

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

Dataskyddsombudet bedömer att det inom Staden finns en felaktig uppfattning om att det är omöjligt att följa GDPR och samtidigt driva den digitala utvecklingen framåt. Det finns också en felaktig uppfattning om att GDPR är en lagstiftning som inte är obligatorisk att följa. Dataskyddsombudet vill därför särskilt lyfta att dessa uppfattningar är problematiska och medför risker i form av att dataskydds-perspektivet förbises i digitaliseringsarbetet. Fokus behöver därför skiftas från att betrakta reglerna i dataskyddslagstiftningen som hinder, till att i stället fokusera på syftet med lagstiftningen och använda den som en grund att utgå från i utvecklingen av innovations- och digitaliseringslösningar. Ett sådant fokus kommer gynna enskilda individer och samtidigt medföra en mer hållbar och rättssäker digitalisering i samhället på lång sikt.

3 Granskning av dataskyddsarbetet 2023

3.1 Kontroll av fasta kontrollpunkter

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

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

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

3.2 Resultat från kontrollen 2023

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

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

3.2.1 Kontrollpunkt 1: Dataskyddsorganisation

Verksamhetens skattning av risknivå

Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att verksamheten bedriver ett systematiskt dataskyddsarbete inom ramen för kontrollpunkten och att inga risker av betydelse föreligger.

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

GSK är ett bolag med få anställda och småskaliga personuppgiftsbehandlingar med förhållandevis låga risker. Dataskyddsarbetet behöver stå i proportion till detta, vilket dataskyddsombudet anser att det gör. Eftersom den operativa dataskyddsorganisationen också i stort sett utgörs av bolagets högsta ledning får frågorna en aktualitet på högsta nivå som är okonventionellt, men enligt dataskyddsombudets förmenande positivt.

3.2.2 Kontrollpunkt 2: Personuppgiftsincidenter

Verksamhetens skattning av risknivå

Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att verksamheten bedriver ett systematiskt dataskyddsarbete inom ramen för kontrollpunkten och att inga risker av betydelse föreligger.

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.

Dataskyddsombudet rekommenderar att bolaget fortsätter att arbeta aktivt med att förbättra och/eller bibehålla de goda förutsättningarna som finns för att identifiera och hantera personuppgiftsincidenter. Ett konkret förbättringsområde är att ta fram dokumenterade arbetssätt för hur information till de registrerade ska tillhandahållas vid en incident med höga risker

3.2.3 Kontrollpunkt 3: Biträdesavtal och andra överenskommelser

Verksamhetens skattning av risknivå

Dataskyddsombudets bedömning

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

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.

Av bolagets svar utläser dataskyddsombudet att det finns rutiner för att bedöma om nya leverantörer är personuppgiftsbiträden och rutiner för att teckna avtal med dessa. Årets skattningar är i stort sett identiska med föregående års. Detta innebär bl.a. att bolaget enligt egen uppskattning fortsatt saknar biträdesavtal i ca 50 % av fallen där detta krävs, vilket utgör en påtaglig risk. Verksamheten saknar fortfarande också, med ledning av svaren på dataskyddsombudets kontrollfrågor, fullgoda dokumenterade arbetssätt för att bedöma kedjan av underbiträden, huruvida avtal om delat/gemensamt personuppgiftsansvar behöver upprättas vid anlitande av leverantör eller interna samarbeten i Göteborgs Stad. Verksamheten saknar också delvis dokumenterade arbetssätt för att genomföra efterlevnadskontroller av anlitade biträden. Frågan om tecknande av biträdesavtal där så krävs bör vara en prioriterad fråga för bolaget, allra helst som det även var en rekommendation från dataskyddsombudet förra året.

Bolaget rekommenderas att:

- Teckna biträdesavtal i samtliga fall där så krävs för att säkerställa efterlevnad av GDPR.

- Ta fram dokumenterade arbetssätt för att kunna genomföra efterlevnadskontroller av biträden, bedöma om och när avtal om gemensamt personuppgiftsansvar behöver tecknas, samt slutligen för att kunna bedöma kedjan av underbiträden som anlitas av leverantörer

3.2.4 Kontrollpunkt 4: Register över personuppgiftsbehandlingar

Verksamhetens skattning av risknivå

Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att verksamheten bedriver ett systematiskt dataskyddsarbete inom ramen för kontrollpunkten och att inga risker av betydelse föreligger.

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

Kontrollpunkten har varit en prioriterad fråga för bolaget under året. Dataskyddsombudet kan konstatera att GSK har gjort ett bra arbete med att ta fram ett behandlingsregister och implementera det i sitt dataskyddsarbete. Sammantaget är det mycket positivt och visar att bolaget har alla möjligheter att bedriva ett gediget arbete med sitt dataskydd.

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 verksamhetens bedömning om att det förekommer risker som är omfattande och kräver omgående åtgärder. Dessa risker är framför allt hänförliga till värdering av verksamhetens informationstillgångar Bolaget är dock medvetet om bristen och ett arbete har påbörjats under hösten med att värdera och identifiera information utifrån K/R/T i enlighet med stadens styrande dokument. Dataskyddsombudet har också haft en dialog med verksamheten angående genomförandet av interna kontroller för att säkerställa följsamheten gentemot GDPR. Idag utförs inga sådana kontroller.

Dataskyddsombudet rekommenderar bolaget att:

- Fortsätta det påbörjade arbetet med värdering av informationstillgångar
- Ta fram dokumenterade arbetssätt för att genomföra interna efterlevnadskontroller

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, men har ingen anledning att göra en annan bedömning än den som verksamheten

har gjort avseende risknivå. Dataskyddsombudet vill dock upprepa sin bedömning från föregående års årsrapport.

Bolaget svar på kontrollfrågorna indikerar att medarbetarna regelbundet utbildas inom dataskydd och att den allmänna kunskapsnivån ger goda förutsättningar för att bedriva dataskyddsarbetet. Höga skattningar på denna punkt innebär att i princip alla anställda korrekt ska kunna identifiera en personuppgiftsincident, att relevanta roller ska veta hur och när en konsekvensbedömning ska göras och att ansvariga ska ha koll på tillvägagångssätt när registrerade utövar sina rättigheter i förhållande till bolaget. Såvida detta inte stämmer in på bolaget bör verksamheten se över arbetet inom denna kontrollpunkt.

3.2.7 Kontrollpunkt 7: Informationsplikt

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 inte verksamhetens bedömning utan anser tvärtom att det inom kontrollpunkten föreligger höga risker som omgående kräver insatser ifrån ledningsnivå.

Dataskyddsenheten höll under våren 2023 en särskild informationsinsats rörande informationsplikten enligt GDPR. Dataskyddsombudets bedömning är rent generellt att det finn stora brister i den information som lämnas till de registrerade, detta gäller inte enbart för GSK utan är en genomgående brist hos i princip samtliga verksamheter i Göteborgs Stad. Efter att ha tittat närmare på bolagets integritetspolicy är dataskyddsombudets uppfattning att den information som lämnas inte uppfyller kraven i artikel 12–14 i GDPR.

Bristerna består både i vilken information som lämnas och sättet på vilket informationen lämnas. Dataskyddsombudet rekommenderade redan i 2022 års årsrapport att policyn behövde ses över. Policyn är gemensam för tre bolag och det framgår inte vilka personuppgiftsbehandlingar som faktiskt sker hos respektive bolag. Policyn innehåller inte heller konkreta uppgifter om ändamål eller nämner vilka rättsliga grunder som bolaget lutar sig mot, utan anger endast i generella ordalag olika exempel på vad som skulle kunna förekomma.

Bolaget rekommenderas därför att:

- Se över samtliga delar i bolagets integritetspolicy och genomföra en omarbetning av underlaget för att säkerställa att informationsplikten enligt GDPR uppfylls.

- Se över den information som lämnas till de registrerade, oavsett sammanhang, och de arbetssätt som tillämpas för att säkerställa att informationsplikten gentemot de registrerade uppfylls.

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 delar verksamhetens bedömning om att det förekommer risker som är omfattande och kräver omgående åtgärder. Dataskyddsombudet vill samtidigt framhålla att bolagets resultat inom kontrollpunkten hamnar på en låg nivå på grund av arbetet med informationsklassning. Övriga delar av kontrollpunktens innehåll är sådant som bolaget uppfyller väl och aktivt har arbetat med.

Eftersom verksamheten under hösten också inlett ett arbete med att aktivt genomföra informationsklassningar (se kontrollpunkt 5) nöjer sig dataskyddsombudet med att rekommendera bolaget att:

- Fortsätta det påbörjade arbetet med värdering av informationstillgångar

3.2.9 Kontrollpunkt 9: Konsekvensbedömning/samråd

Verksamhetens skattning av risknivå

Dataskyddsombudets bedömning

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

Dataskyddsombudet delar verksamhetens bedömning om att det förekommer risker som är omfattande och kräver omgående åtgärder. Skattningen är i de flesta delar samma som bolaget angivit i tidigare års enkäter. Bolaget har alltså inte arbetat aktivt med att åtgärda de risker som identifierats. Dataskyddsombudets rekommendationer är därför de samma som lämnats i tidigare års årsrapporter.

Dataskyddsombudet rekommenderar att bolaget:

- Genomför en kartläggning av de behandlingar med hög risk som utförs och där det saknas konsekvensbedömningar. Därefter bör en handlingsplan tas fram för att på sikt säkerställa att konsekvensbedömningar genomförs för samtliga behandlingar där detta krävs.

3.2.10 Kontrollpunkt 10: IT-projekt och upphandling

Verksamhetens skattning av risknivå

Dataskyddsombudets bedömning

Verksamhetens resultat indikerar att det inom kontrollpunkten föreligger omfattande risker som kräver omgående åtgärder. Bolaget uppger som förklaring till sin skattning av kontrollpunkten att inga nya upphandlingar eller IT-projekt sker i dagsläget. Det är, på grund av bolagets ovissa framtid, inte heller något som kommer att ske på sikt då bolagets helägda dotterbolag är under försäljning/avveckling. Utifrån läget framstår bolagets svar i denna del som rimliga och dataskyddsombudet lämnar inga särskilda rekommendationer i denna del, men vill dock lyfta att för det fall att upphandlingar eller införande av nya system m.m. planeras behöver dataskyddsperspektivet säkerställas.

3.2.11 Kontrollpunkt 11: IT-system och digitala verktyg

Verksamhetens skattning av risknivå

Dataskyddsombudets bedömning

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

Dataskyddsombudet saknar överblick över hur användningen av IT-system och digitala verktyg ser ut i bolaget men har inte heller någon anledning att göra en annan bedömning än den som görs av bolaget.

I likhet med föregående kontrollpunkt beror vissa av svaren, med låga värden, på dataskyddsombudets kontrollfrågor, enligt bolaget på att inga nya tjänster och verktyg införs utifrån rådande läge. Så länge bolaget behandlar personuppgifter behöver dock GDPR följas och skyddet för personuppgifterna säkerställas. Det innebär att det behöver finnas kontroll och översikt över de tjänster och digitala verktyg som används och användningen behöver ske på ett säkert sätt.

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.

Utifrån bolagets svar framgår att verksamheten har omhändertagit tidigare rekommendation från dataskyddsombudet och har implementerat dokumenterade arbetssätt för att hantera begäran om registerutdrag från de registrerade, vilket är positivt. Framöver rekommenderar dataskyddsombudet bolaget att:

- Verka för en medvetenhet inom organisationen om de registrerades rättigheter.

- Ta fram dokumenterade arbetssätt för att bedöma 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): Behörighetsstyrning - Personec

Verksamheten gavs följande rekommendationer:

- Dataskyddsombudet rekommenderar att bolaget ser över hur loggning kan användas och när/hur dessa kontrolleras.

- Se över hanteringen av personuppgiftsbiträdesavtal/överenskommelser och instruktioner till personuppgiftsbiträdet.

- Bolaget rekommenderas att definiera sina behandlingar i Personec, bedöma om de uppfyller kraven för när en konsekvensbedömning ska göras samt i förevarande fall genomföra en konsekvensbedömning

Kommentarer och rekommendationer:

Uppföljningen visar att verksamheten har vidtagit åtgärder i enlighet med samtliga rekommendationer. Fortsatt uppföljning kommer ske inom ramen för de fasta kontrollpunkterna om inget särskilt föranleder att det behöver följas upp separat.

4 Rekommenderade fokusområden 2024

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

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

- Kontrollpunkt 3: Biträdesavtal och andra överenskommelser
  Bolaget rekommenderas teckna biträdesavtal i samtliga fall där så krävs för att säkerställa efterlevnad av GDPR.

  Ta fram dokumenterade arbetssätt för att kunna genomföra efterlevnadskontroller av biträden, bedöma om och när avtal om gemensamt personuppgiftsansvar behöver tecknas, samt slutligen för att kunna bedöma kedjan av underbiträden som anlitas av leverantörer.

- Kontrollpunkt 7: Informationsplikt
  Bolaget rekommenderas se över samtliga delar i bolagets integritetspolicy och genomför en omarbetning av underlaget för att säkerställa att informationsplikten enligt GDPR uppfylls.

  Se över den information som lämnas till de registrerade, oavsett sammanhang, och de arbetssätt som tillämpas för att säkerställa att informationsplikten gentemot de registrerade uppfylls.

5 Bilagor

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

Bilaga 2: Kontrollplan för dataskyddsarbetet 2023–2024