

Styrelsen	2025-02-20
Handling nr	8.7
Handläggare	Joakim Holt
Daterad	2025-01-28
Reviderad	

**Till
Styrelsen för Västtrafik AB**

Rapport dataskyddsombud

Västtrafik ska en gång per år rapportera en sammanställning från dataskyddsombudet till styrelsen. Rapporten för 2024 bifogas.

FÖRSLAG TILL BESLUT

Med anledning av ovanstående föreslås styrelsen besluta
att notera den lämnade informationen till protokollet.

Skövde dag som ovan

Lars Backström

Rapport

Dataskyddsbud

2025-02-20

Innehållsförteckning

Inledning	3
Omfattning och metod	3
Efterlevnad av dataskyddsförordningen	3
Registrerade personuppgiftsbehandlingar	3
Bolagets efterlevnad	4
Grundläggande principer	4
Bolagets efterlevnad	4
Personuppgiftsincidenter	4
Bolagets efterlevnad	5
Konsekvensbedömning	5
Bolagets efterlevnad	5
Personuppgiftsbiträdesavtal	5
Bolagets efterlevnad	6
Lagringsminimering, arkivering och gallring	6
Bolagets efterlevnad	6
Registrerades rättigheter	6
Bolagets efterlevnad	7
Känsliga och skyddsvärda	7
Bolagets efterlevnad	7
Skydd av uppgifter	7
Bolagets efterlevnad	8
Sammanfattning och rekommendationer	8

Inledning

Dataskyddsförordningen (GDPR¹) reglerar hur myndigheter, bolag och andra organisationer får hantera personuppgifter. Som personuppgift räknas all typ av information som kan kopplas till en nu levande fysisk person. Varje organisation, oavsett verksamhet, behandlar därmed personuppgifter i någon omfattning och måste därmed förhålla sig till dataskyddsförordningens regler.

Förordningen ställer en rad krav; från säker hantering av information, till kontroll över vilka personuppgifter som hanteras, var, varför och hur samt kontinuerlig utvärdering av risker för enskildas fri- och rättigheter. Det är bolaget som är personuppgiftsansvarig för den personuppgiftsbehandling som sker inom dess verksamhet och därmed ytterst ansvarig för att förordningens krav följs.

Omfattning och metod

Denna rapport sammanfattar Västtrafik AB:s efterlevnad av dataskyddsförordningen fördelat på nio områden. Områdena beskrivs närmare i rapporten nedan.

Rapporten lämnas av bolagets dataskyddsombud. Dataskyddsombud är en roll som bolaget är skyldigt att utse enligt dataskyddsförordningen och har i uppdrag att granska och rapportera om bolagets efterlevnad. Därutöver har dataskyddsombudet även i uppgift att ge råd och stöd om skyldigheter som följer av lagen samt fungera som kontaktpunkt gentemot enskilda och tillsynsmyndigheten IMY². Denna rapportens slutsatser redovisas till Västtrafiks styrelse årligen som en del av dataskyddsombudets uppdrag.

Efterlevnad av dataskyddsförordningen

I detta avsnitt sammanfattas bolagets efterlevnad av dataskyddsförordningen inom nio områden. Områdena beskrivs under respektive rubrik nedan.

Registrerade personuppgiftsbehandlingar

Varje personuppgiftsansvarig ska enligt artikel 30 ha en förteckning över sina personuppgiftsbehandlingar (en registerförteckning) där bland annat syfte, kategorier av registrerade, typer av personuppgifter och lagringstid framgår. Registerförteckningen är en förutsättning för att överhuvudtaget kunna efterleva dataskyddsförordningen, då den anger vilka personuppgifter som behandlas, hur och varför.

¹ EU:s dataskyddsförordning General Data Protection Regulation.

² IMY Integritetsskyddsmyndigheten, <https://www.imy.se/>

Årets granskning omfattar huruvida bolagets samtliga personuppgiftsbehandlingar har registrerats och om innehållet i registerförteckningen motsvarar kraven i artikel 30.

Bolagets efterlevnad

Bolagets registerförteckning är i stora drag komplett och innehåller i stort nödvändig information. Vissa behandlingar och viss information saknas dock och behöver kompletteras för att registerförteckningen ska räknas som helt komplett.

Grundläggande principer

Grundläggande principer för behandling av personuppgifter anges i artikel 5 i dataskyddsförordningen. Principerna fungerar som vägledning för hur personuppgifter får hanteras och genomsyrar övriga krav på dataskydd. Principer handlar bland annat om att ha en rättslig grund, enbart behandla så många personuppgifter som behövs för ett visst syfte, iaktta proportionalitet, inte spara uppgifter längre än de behövs och ha tillräcklig säkerhet.

Årets granskning omfattar huruvida bolaget har rutiner för att säkerställa att de grundläggande principerna beaktas.

Bolagets efterlevnad

I samband med upprättandet av nya behandlingar i registerförteckningen, upphandlingar och förändringar utvärderas även om behandlingen följer de grundläggande principerna. Utvärdering görs även i samband med konsekvensbedömningar (även kallad DPIA). Årets granskning har dock inte omfattat huruvida enskilda personuppgiftsbehandlingar iakttar principerna.

Dataskyddsombudet involveras regelbundet i rådgivning och stöd när verksamheten gör förändringar. Bolagets efterlevnad anses vara god.

Personuppgiftsincidenter

Varje personuppgiftsansvarig ska ha processer för att upptäcka, utreda, åtgärda och anmäla vissa personuppgiftsincidenter till tillsynsmyndigheten IMY.

Det innebär att medarbetare ska kunna identifiera när en personuppgiftsincident har hänt, veta hur den ska rapporteras och att det finns processer för att ta hand om en bekräftad incident. Det är även av vikt att incidenten leder till uppdaterade rutiner och arbetssätt för att förhindra nya incidenter.

Årets granskning omfattar huruvida bolaget har en process för att upptäcka, dokumentera och anmäla personuppgiftsincidenter.

Bolagets efterlevnad

Bolaget har en framtagen process som uppfyller kraven på hantering av personuppgiftsincidenter. Under 2024 inträffade 15 personuppgiftsincidenter, varav en var allvarlig nog att rapporteras till IMY. Inga åtgärder har krävts av IMY till följd av denna.

Antalet incidenter bedöms vara heltäckande och att rapporteringsviljan i verksamheten är fortsatt god.

Konsekvensbedömning

Om det finns en hög risk för enskildas fri- och rättigheter när personuppgifter behandlas, ska den personuppgiftsansvarige göra en konsekvensbedömning.

Exempel på situationer då en hög risk kan föreligga är: övervakning eller kartläggning av personer i beroendesituation, behandling av känsliga personuppgifter eller användning av ny teknik.

Konsekvensbedömningens syfte är både att säkerställa att enskildas fri- och rättigheter respekteras och är även ett sätt för den personuppgiftsansvarige att visa att dataskyddslagstiftningen följs.

Årets granskning omfattar huruvida bolaget dels genomfört en riskbedömning för att bedöma om en konsekvensbedömning krävs och om konsekvensbedömningen är gjord.

Bolagets efterlevnad

Bolaget har delvis genomfört riskbedömningar för att bedöma om konsekvensbedömning krävs eller ej. Konsekvensbedömningar har genomförts för många av de behandlingar som granskats men det har saknats för enskilda behandlingar.

Stor vikt har även under året lagts på dokumentation av kamerabevakning där Västtrafik AB ansvarar för ca 14 000 kameror på fordon och i resecentrum i regionen. Efterlevnaden bedöms som fortsatt god.

Personuppgiftsbiträdesavtal

Personuppgiftsbiträdesavtal ska tecknas om en personuppgiftsansvarig anlitar en extern part som behandlar personuppgifter åt den personuppgiftsansvariga. Den externa parten är då biträde till den personuppgiftsansvariga och ska genom avtalet förbindas att endast behandla personuppgifter efter instruktioner från den ansvarige. Syftet med avtalet är att säkerställa att enskildas personuppgifter skyddas även när det är någon annan än den personuppgiftsansvarige som behandlar personuppgifterna.

Årets granskning omfattar huruvida personuppgiftsbiträdesavtal tecknats där så krävs.

Bolagets efterlevnad

Bolaget har tecknat personuppgiftsbiträdesavtal med sina biträden.

Lagringsminimering, arkivering och gallring

Lagringsminimering är en av dataskyddsprinciperna och handlar om att personuppgifter endast får behandlas så länge de behövs för ändamålet. Inom offentlig verksamhet innebär lagringsminimering att det finns ordning och reda bland myndighetens information, att information rensas, arkiveras och gallras. *Västtrafiks Policy för Arkivbeskrivning och beskrivning av allmänna handlingar för Västtrafik AB*³ är det styrdokument som styr Västtrafiks hantering av allmänna handlingar.

Årets granskning omfattar huruvida bolaget har en uppdaterad informationshanteringsplan och om arkivering och gallring utförs enligt den.

Bolagets efterlevnad

Bolaget har en aktuell informationshanteringsplan, dock gallras och arkiveras inte all information efter den. Granskningen visar dock att gallring av personuppgifter för kameror och kunddata följer planen och är automatiserad. Dataskyddsombudet rekommenderar att ta in gallring och arkivering som en (minst) årlig aktivitet i respektive verksamhets verksamhetsplan eller liknande, om det avser personuppgifter.

Registrerades rättigheter

Enskilda har ett antal rättigheter i förhållande till sina personuppgifter, enligt nedan:

- Rätt att vända sig till en personuppgiftsansvarig för att få bekräftat om ens personuppgifter behandlas och i så fall få tillgång till dessa (Rätt till tillgång – även kallat ”registerutdrag”).
- Rätt att få information om hur personuppgifter hanteras (rätten till information).
- Under vissa förutsättningar få sina uppgifter raderade eller rättade (rätten till radering och rättelse).
- Rätt att invända, dvs. motsätta sig, mot en personuppgiftsbehandling och även begära begränsning av personuppgifternas användning (rätten att göra invändningar och begära begränsning).
- Rätt att inte bli föremål för automatiskt beslutsfattande.

³ VT P 001 Västtrafiks Policy för Arkivbeskrivning och beskrivning av allmänna handlingar för Västtrafik AB. Beslutas av Västtrafiks styrelse årligen vid konstituerande sammanträde.

- Rätt att få ut sina personuppgifter på ett strukturerat sätt för att använda de hos någon annan (rätt till dataportabilitet – gäller enbart i få specifika fall inom offentlig förvaltning).

Årets granskning omfattar huruvida bolaget har processer för att hantera registrerades rättigheter som följer de grundläggande kraven i dataskyddsförordningen.

Bolagets efterlevnad

Bolaget har rutiner för att hantera registerutdrag (rätten till tillgång), dataportabilitet och begäran om rättelse. Däremot är inte processen för att hantera övriga rättigheter lika tydlig varken hur de ska hanteras internt eller kommunikationen gentemot de registrerade. Bolaget informerar om hur personuppgifter hanteras via olika hemsidor. Det finns dock vissa avvikelser i information till anställda om vissa behandlingar som adresseras inom pågående HR-projekt.

Känsliga och skyddsvärda

Det finns ett generellt förbud i dataskyddsförordningen mot att använda känsliga personuppgifter. Det är enbart tillåtet om ett av undantagen är tillämpliga, därför är det viktigt att veta om behandling av eventuella känsliga personuppgifter är lagligt. Förutom känsliga personuppgifter finns det en grupp personuppgifter som benämns som extra skyddsvärda personuppgifter. Dessa kräver inte ett undantag för att det ska vara tillåtet att hantera dem, men är samtidigt av en karaktär som kräver att de skyddas med högre säkerhet. Dessa typer av uppgifter och känsliga personuppgifter får enbart hanteras enligt särskilda rutiner och i system/lagringsytor som har högre säkerhet.

Årets granskning omfattar huruvida bolaget har rättslig grund för behandling av känsliga personuppgifter och huruvida rutiner finns för hantering av känsliga och extra skyddsvärda personuppgifter.

Bolagets efterlevnad

Det har inte framkommit att bolaget behandlar känsliga personuppgifter utan rättslig grund. Både känsliga och extra skyddsvärda personuppgifter hanteras enligt särskilda rutiner som bedöms effektiva.

Skydd av uppgifter

En av de grundläggande principerna är integritet och konfidentialitet som handlar om att kunna säkerställa personuppgifternas konfidentialitet (att inga uppgifter röjs för obehöriga), tillgänglighet (att uppgifterna är tillgängliga när de behövs) och riktighet (att uppgifterna är korrekta). Med andra ord handlar det om att arbeta

aktivt med informationssäkerhet. Årets granskning omfattar huruvida bolaget har ett informationssäkerhetsarbete och genomför analyser kopplat till detta, exempelvis informationsklassning och riskanalys.

Bolagets efterlevnad

Bolaget har en antagen spelregel för informationssäkerhet och dataskydd som är ledningssystem för informationssäkerhet. Under 2024 har granskning av bolagets informationssäkerhetsarbete genomförts utifrån regional styrning. Inga ytterligare åtgärder görs därmed i denna granskning.

Sammanfattning och rekommendationer

Bolaget efterlever dataskyddsförordningen, inga stora risker har identifierats.

Inom några områden krävs åtgärder för att uppfylla kraven i sin helhet.

Dataskyddsombudet ger därför följande rekommendationer:

- Fortsätta arbetet med komplettering av registerförteckningen, särskilt inom pågående HR-projekt.
- Genomföra och dokumentera konsekvensbedömningar där dataskyddsförordningen kräver det. Särskild vikt bör läggas på processer där personer med skyddad identitet förekommer.
- Säkerställa att gallring och arkivering utförs enligt informationshanteringsplanen där det idag inte sker automatiskt.
- Förtydliga processen internt och för de registrerade om hur de kan utöva sina samtliga rättigheter och uppdatera informationstexterna till de registrerade så att de i sin helhet speglar hur bolaget hanterar personuppgifter.

Upprättad av: Joakim Holt, Dataskyddsombud, 2025-01-28

//