Region Hallands Dataskyddsombud
Ellen Bäckman
2025-04-11

Revisionsrapport

Revision av Driftsnämnden för kollektivtrafiks efterlevnad av dataskyddsförordningen

Region Halland

Dataskyddsombudets bedömning

Dataskyddsombudet har funnit följande brister avseende Driftsnämnden för Kollektivtrafiks dataskyddsarbete och efterlevnad av dataskyddsförordningen:

- Nämndens (då bolagets) registerförteckning är inte uppdaterad sedan 2020. Det har skett sporadiska anmälningar av nya personuppgiftsbehandlingar till dataskydd sedan 2023, men det står klart att de uppgifter om pågående personuppgifter som finns att tillgå inte är kompletta.
- Nämnden har inte gjort några konsekvensbedömningar, eller utvärderat huruvida konsekvensbedömningar behöver genomföras i samband med ny personuppgiftsbehandling. Det är möjligt att nämnden inte har några behandlingar som enligt GDPR ska föregås av konsekvensbedömning, men utan information om utvärdering är det omöjligt att bedöma.
- Nämnden har under 2024 inte rapporterat några personuppgiftsincidenter. Det är möjligt att det inte har förekommit några incidenter, men osannolikt. Dataskyddsombudet bedömer att nämnden sannolikt har underlåtit rapporteringsplikten på grund av bristande kunskap och kompetens.

Dataskyddsombudets rekommendationer

Dataskyddsombudet rekommenderar att nämnden omgående kartlägger sina personuppgiftsbehandlingar, både i rollen som personuppgiftsansvarig och personuppgiftsbiträde, och säkerställer att information om behandlingarna registreras i de centrala register som finns hos Informationssäkerhetsavdelningen.

Vidare rekommenderas nämnden säkerställa att medarbetare får utbildning gällande dataskyddsfrågor, och hur dessa ska hanteras i enlighet med gällande rätt och regionala rutiner. Detta bör leda till att incidentrapporteringar sker i rätt ordning och att dokumentation så som konsekvensbedömning, eller utvärdering av om konsekvensbedömning behövs, tas fram.

De sektorspecifika rutiner som Hallandstrafiken har tagit fram behöver ses över, flera anses i delar vara inaktuella eller felaktiga.

En process för systematisk uppföljning av personuppgiftsbiträden, och tillhörande PUB-avtal och instruktioner, bör tas fram. De PUB-avtal som har granskats är gamla med bristande instruktioner, och i vissa fall har ägarförhållandena ändrats på ett sådant sätt att en översyn är nödvändig för att säkerställa att biträdena hanterar personuppgifter för nämndens räkning på ett lagligt sätt.

Bakgrund till revisionen

Enligt artikel 39 dataskyddsförordningen ska dataskyddsombudet övervaka den personuppgiftsansvariges efterlevnad av förordningen och tillhörande författningar. Att genomföra revisioner är ett sätt för dataskyddsombudet att utföra denna arbetsuppgift på ett systematiskt sätt.

Inom Region Halland är varje nämnd, styrelse och bolag personuppgiftsansvarig för den personuppgiftsbehandling som sker inom ramen för dess verksamhet. Det innebär att

Driftsnämnden för Kollektivtrafik (DNKT) är personuppgiftsansvarig för den personuppgiftsbehandling som sker inom ramen för Hallandstrafikens verksamhet.

Med anledning av att Hallandstrafiken, som numera leds av Driftsnämnden för Kollektivtrafik, fram till januari 2023 utgjorde ett regionalt bolag bedömde dataskyddsombudet att det fanns anledning att granska hur övergången till nämnd har gått. Dataskyddsombudet har i detta arbete haft för avsikt att granska huruvida nämnden efterlever den styrning som följer av centrala styrdokument inom Region Halland samt i övrigt efterlever dataskyddsförordningen och tillhörande författningar.

För information om viktiga begrepp och grundläggande dataskyddsprinciper, se Bilaga 1.

Revisionens omfattning och metod

Dataskyddsombudet har valt att granska vissa delar av nämndens dataskyddsarbete. För detta har dataskyddsombudet begärt att få tillgång till registerförteckning, konsekvensbedömningar och information om personuppgiftsincidenter från 2024. Dataskyddsombudet har även fått del av rutiner, specifika för Hallandstrafiken, avseende hantering av registrerades rättigheter. Dessa har granskats.

Dataskyddsombudet har vidare valt ut två system, som enkom används av Hallandstrafiken/DNKT, för en närmare granskning av personuppgiftsflöde och dokumentation i form av registerförteckning, avtal och eventuella konsekvensbedömningar. Systemen som valdes ut är Planet och Skolportalen.

Revisionen har genomförts både genom intervjuer med medarbetare hos Hallandstrafiken, samt granskning av tillhandahållna dokument.

Nedan följer dataskyddsombudets fynd på de olika områdena, tillsammans med bedömning och rekommendation.

Resultat

Registerförteckning

Enligt artikel 30 dataskyddsförordningen ska varje personuppgiftsansvarig föra ett register över behandling som utförts under dess ansvar. Detta register ska bland annat innehålla information om namn och kontaktuppgifter till den personuppgiftsansvarige samt dataskyddsombudet, ändamålen med behandlingen, en beskrivning av kategorierna av registrerade, information om personuppgifterna som behandlas, information om gallringsfrister m.m. Enligt samma artikel anges även att varje personuppgiftsbiträde ska föra ett register över de behandlingar som biträdet utför åt en personuppgiftsansvarig.

Inom ramen för denna granskning har dataskyddsombudet dels tagit del av en registerförteckning för Hallandstrafiken, senast uppdaterad 21 september 2020, samt tagit ut de behandlingar som finns registrerade för DNKT i det centralt hanterade registret.

Enligt Regions Hallands rutin 'Personuppgifter – behandling av' ska all behandling av personuppgifter anmälas till Dataskyddsenheten (numera Informationssäkerhetsavdelningen). Informationssäkerhetsavdelningen ansvarar för att hålla samtliga register samlade, och ska på anmälan från verksamheterna lägga till eller ta bort behandlingar från registret. Det finns register för när Region Halland är personuppgiftsansvarig, och när Region Halland är

personuppgiftsbiträde. I det centrala registret finns det i dagsläget 16 personuppgiftsbehandlingar anmälda från DNKT som personuppgiftsansvarig. I Hallandstrafikens gamla registerförteckning, som inte har uppdaterats sedan 2020, finns över 100 personuppgiftsbehandlingar angivna.

Det står klart att någon komplett och aktuell registerförteckning för DNKT inte finns tillgänglig. Sedan 2020 har dåvarande bolaget och nuvarande nämnden brustit i sin skyldighet att säkerställa att en registerförteckning enligt GDPR finns och hålls uppdaterad. Från och med övergången till nämnd, 2023, har förvisso vissa behandlingar anmälts till Informationssäkerhetsavdelningen, men undertecknad bedömer att det står klart att långt ifrån alla behandlingar har anmälts. Detta är enligt dataskyddsombudets bedömning mycket allvarligt, då en uppdaterad registerförteckning är nödvändig för att en personuppgiftsansvarig ska kunna visa att de vet vad de har för personuppgiftsbehandlingar och att de tar ansvar för att de personuppgifter som behandlas hanteras på ett lagligt, korrekt och öppet sätt i förhållande till de registrerade.

Dataskyddsombudet rekommenderar att nämnden omgående kartlägger vilka personuppgiftsbehandlingar som sker inom ramen för nämndens verksamhet, och att dessa behandlingar därefter anmäls till Informationssäkerhetsavdelningen enligt gällande styrdokument så att samtliga behandlingar finns i det centrala registret. Vidare är det nödvändigt att medarbetare får information om kravet på att anmäla nya eller ändrade personuppgiftsbehandlingar till Informationssäkerhetsavdelningen.

Konsekvensbedömning

Enligt artikel 35 dataskyddsförordningen ska den personuppgiftsansvarige utföra en konsekvensbedömning avseende dataskydd innan personuppgiftsbehandling påbörjas om behandlingen sannolikt leder till hög risk för fysiska personers rättigheter och friheter. För att avgöra om en behandling sannolikt leder till hög risk ska aspekter såsom behandlingens typ, t.ex. användning av ny teknik, behandlingens omfattning, ändamål och art beaktas. Som exempel medför behandling av känsliga personuppgifter många gånger hög risk för de registrerade. Den personuppgiftsansvarige ska rådfråga dataskyddsombudet vid genomförande av en konsekvensbedömning.

Dataskyddsombudet har fått uppgift om att inga konsekvensbedömningar har genomförts hos Hallandstrafiken/DNKT, varken före eller efter övergången till nämnd. Det är för dataskyddsombudet inte möjligt att med all säkerhet säga att någon av nämndens personuppiftsbehandlingar ska ha föregåtts av konsekvensbedömning, då komplett information om pågående behandlingar saknas (se ovan avsnitt om registerförteckning) men undertecknad vågar påstå att det sannolikt finns vissa behandlingar hos DNKT som kan medföra vissa risker för de registrerade. Ett sådant exempel skulle kunna vara den handläggning som sker i Websolen, där registrerades hälsouppgifter behandlas i samband med handläggning av tillstånd för färdtjänst.

Dataskyddsombudet bedömer att nämndens, och förvaltningens, medarbetare behöver tydlig information och/eller utbildning om när en konsekvensbedömning ska genomföras. Dataskyddsombudet rekommenderar även att nämnden går igenom sina personuppgiftsbehandlingar för att säkerställa att det inte pågår någon behandling som medför hög risk för de registrerade. Om man finner att det finns sådana behandlingar rekommenderar dataskyddsombudet att nämnden antingen avslutar den behandlingen eller gör en konsekvensbedömning i efterhand, för att säkerställa att eventuella risker omhändertas.

Personuppgiftsincidenter

En personuppgiftsincident är en säkerhetsincident som leder till att personuppgifter förstörs, går förlorade, ändras eller kommer i orätta händer. Det har ingen betydelse om det har skett oavsiktligt eller med avsikt. Region Halland har en lagstadgad skyldighet att anmäla incidenter som kan innebära en risk för de registrerade till Integritetsskyddsmyndigheten inom 72 timmar. Vid höga risker finns det även en skyldighet att informera de registrerade om händelsen. Enligt Region Hallands rutiner rapporteras personuppgiftsincidenter till Informationssäkerhetsavdelningen som utreder ärendet.

Under 2024 har inga personuppgiftsincidenter rapporterats från DNKT till Informationssäkerhetsavdelningen. Undertecknad finner det dock osannolikt att inga incidenter ska ha inträffat under året, varför detta får antas bero på bristande kunskap. Dataskyddsombudet bedömer att nämndens, och förvaltningens, medarbetare behöver tydlig information och/eller utbildning om vad som utgör personuppgiftsincidenter och hur dessa ska rapporteras internt.

Styrdokument

Undertecknad har tagit del av fyra rutiner från Hallandstrafiken, framtagna innan övergång till nämnd. Rutinerna avser 'Registerutdrag', 'Resekort', 'Rätt att bli bortglömd' och 'begäran från tredje man'.

Utan att gå in på detaljer finner undertecknad att det finns anledning att se över i vilken mån dessa rutiner kan anses överflödiga, i de fall hanteringen redan regleras av regionala styrdokument. Detta är till exempel aktuellt gällande hantering av registerutdrag, där det finns regional styrning i rutinen 'Registerutdrag enligt dataskyddsförordningen'. I de fall dessa rutiners avsedda processer inte omfattas av regional styrning bör DNKT se över rutinerna för att säkerställa att dessa är uppdaterade och användbara, samt säkerställa att hänvisningar till rättslig grund för en behandling stämmer. Undertecknad har noterat att man i vissa fall hänvisar till intresseavvägning som rättslig grund. Intresseavvägning som rättslig grund får inte användas av myndigheter, varför denna rättsliga grund inte ska användas nu när Hallandstrafiken har övergått till nämnd. Gällande rutinen som avser begäran från tredje man har undertecknad förstått att den används bland annat när andra myndigheter, såsom polismyndigheten, begär uppgifter från nämnden. Vid en sådan begäran ska en sekretessprövning enligt Offentlighet- och sekretesslagen (2009:400) göras innan utlämnande, vilket inte framkommer av rutinen. Undertecknad rekommenderar att nämnden tar hjälp av ansvarig regionjurist för att uppdatera/skriva om rutinen på ett lämpligt sätt, vilket bedöms som särskilt aktuellt med beaktande av de nya reglerna som började gälla den 1 april, genom lag (2025:170) om skyldighet att lämna uppgifter till de brottsbekämpande myndigheterna.

Dataskyddsombudet rekommenderar en översyn av förvaltningsspecifika rutiner kopplade till dataskydd, samt att nämnden säkerställer att medarbetare hos förvaltningen får information/utbildning gällande det ledningssystem av informationssäkerhet och dataskydd som finns på övergripande regional nivå.

Stickprov system

Planet m.m.

Dataskyddsombudet har i samtal med systemförvaltaren för Planet fått en bild av vad det är för personuppgifter som behandlas i Planet och integrerade system, och varför. Planet är ett boknings- och planeringssystem för bl.a. sjukresor, färdtjänst, skolskjuts och närtrafik. Planet är kopplat till systemen Websolen, som är ett handläggningssystem, och Pluto, som hanterar fakturor. Samtliga system levereras av samma leverantör. Avtal och PUB-avtal finns upprättat med leverantören PLANit, som numera är uppköpta av Voyagerr.

I Planet och Pluto hanteras inga känsliga personuppgifter, däremot hanteras känsliga uppgifter i Websolen i samband med handläggning av tillstånd för färdtjänst. Inom ramen för denna handläggning behandlas känsliga personuppgifter i form av hälsouppgifter, såsom läkarintyg.

Gallring sker i systemen i enlighet med gällande informationshanteringsplan. Strikt behörighetstilldelning sker och uppföljning av gällande behörigheter sker en gång per år. Information om behandlingen/behandlingarna finns delvis angiven i den gamla registerförteckningen från 2020. Enligt muntlig uppgift ska all behandling ske inom Sverige.

Dataskyddsombudet har läst PUB-avtalet och kan konstatera att detta är gammalt (daterat 16 maj 2018) och att instruktionerna är bristfälliga. Vidare har ägarförhållandena hos leverantören förändras sedan detta tecknades. Voyagerr är dessutom ett kanadensiskt bolag, vilket kan innebära risk för tredjelandsöverföring.

Dataskyddsombudet rekommenderar att nämnden så snart som möjligt ser över PUB-avtalet och instruktionerna, ser över hur och i vilken omfattning leverantören behandlar personuppgifter för nämndens räkning samt analyserar huruvida de ändrade ägarförhållandena medför några risker för de registrerade. Det kan även vara lämpligt att se över om en DPIA behöver genomföras. Vidare ska behandlingarna registreras i regionens centrala registerförteckning.

Skolportalen och CRM

Systemet Skolportalen blev också utvald för stickkontroll. Efter samtal med medarbetare som arbetar med Skolportalen stod det klart att Skolportalen primärt används av Hallandstrafikens kunder, och att det är kunderna (kommuner och skolor) som är personuppgiftsansvariga för de personuppgifter som läggs in i systemet. Syftet med systemet är att kunderna ska kunna beställa och köpa skolbiljetter till de elever som bedöms vara berättigade till det. Handläggning och bedömning av rätt till skolbiljett hanteras enkom av kunderna. Systemet är framtaget av leverantören Sopra Steria på uppdrag av Hallandstrafiken och ett tre andra regioner. DNKT är i denna behandling att anse som personuppgiftsbiträde till kunderna, och Sopra Steria är personuppgiftsbiträde i förhållande till DNKT. Behandlingen finns angiven i Hallandstrafikens gamla registerförteckning, men saknas i den regionala förteckningen avseende personuppgiftsbehandlingar som regionen utför som personuppgiftsbiträde.

I samtalet framgick det att Skolportalen är integrerat med Hallandstrafikens CRM-system, som också är framtaget av samma leverantör. Det är i detta system Hallandstrafiken hanterar kunders kontaktuppgifter, biljetter, historik och DNKT bedöms vara personuppgiftsansvarig för denna personuppgiftsbehandling. Lösningen driftas på servrar i Sverige. Denna behandling finns inte angiven varken i den gamla registerförteckningen eller i det centrala registret. Undertecknad har tagit del av det befintliga PUB-avtalet som finns mellan Region Halland, genom Hallandstrafiken

AB, och Sopra Steria för den behandling leverantören gör med anledning av CRM-lösningen. Det kan konstateras att avtalet är gammalt, daterat 2019-11-21, och att en översyn av avtalet och instruktionerna kan vara på sin plats.

Dataskyddsombudets rekommendation är, liksom tidigare, att DNKT säkerställer att de personuppgiftsbehandlingar som pågår finns angivna i de regionala register som finns hos Informationssäkerhetsavdelningen. Vidare rekommenderar dataskyddsombudet att DNKT ser över PUB-avtalet och instruktionerna avseende CRM-lösningen och uppdaterar dessa om behov finns.

Bilagor

Bilaga 1_viktiga begrepp

Halmstad, 2025-04-11

Ellen Bäckman, Dataskyddsombud

Bilaga 1 – Viktiga begrepp dataskyddsförordningen (DSF)

Viktiga begrepp

En *personuppgift* är varje upplysning som avser en identifierad eller identifierbar fysisk person (nedan kallad en registrerad), varvid en identifierbarfysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet (artikel 4.1 DSF).

En *behandling* av personuppgifter är en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring (artikel 4.2 DSF).

Den *personuppgiftsansvarige* är en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter; om ändamålen och medlen för behandlingen bestäms av unionsrätten eller medlemsstaternas nationella rätt kan den personuppgiftsansvarige eller de särskilda kriterierna för hur denne ska utses föreskrivas i unionsrätten eller i medlemsstaternas nationella rätt (artikel 4.7 DSF).

Personuppgiftsbiträdet är en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning (artikel 4.8 DSF).

En *mottagare* är en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ till vilket personuppgifterna utlämnas, vare sig det är en tredje part eller inte; offentliga myndigheter som kan komma att motta personuppgifter inom ramen för ett särskilt uppdrag i enlighet med unionsrätten eller medlemsstaternas nationella rätt ska dock inte betraktas som mottagare; offentliga myndigheters behandling av dessa uppgifter ska vara förenlig med tillämpliga bestämmelser för dataskydd beroende på behandlingens syfte (artikel 4.9 DSF).

En *tredje part* är en fysisk eller juridisk person, offentlig myndighet, institution eller organ som inte är den registrerade, den personuppgiftsansvarige, personuppgiftsbiträdet eller de personer som under den personuppgiftsansvariges eller personuppgiftsbiträdets direkta ansvar är behöriga att behandla personuppgifterna (artikel 4.10 DSF).

Dataskyddsförordningens grundprinciper

DSF omfattar ett antal grundprinciper för behandling av personuppgifter. Syftet med registret över behandlingar är att göra det möjligt för Datainspektionen att övervaka Region Hallands behandling av personuppgifter. Detta inkluderar en övervakning av Region Hallands efterlevnad av DSF:s grundprinciper. Detta avsnitt redovisar DSF:s grundprinciper.

Personuppgifter ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade (laglighet, korrekthet och öppenhet, artikel 6.1(a) DSF).

Personuppgifter ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål. Ytterligare behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1 ska inte anses vara oförenlig med de ursprungliga ändamålen (ändamålsbegränsning, artikel 6.1(b) DSF).

Personuppgifter ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas (uppgiftsminimering, artikel 6.1(c) DSF).

Personuppgifter ska vara korrekta och om nödvändigt uppdaterade. Alla rimliga åtgärder måste vidtas för att säkerställa att personuppgifter som är felaktiga i förhållande till de ändamål för vilka de behandlas raderas eller rättas utan dröjsmål (korrekthet, artikel 6.1(d) DSF).

Personuppgifter får inte förvaras i en form som möjliggör identifiering av den registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas. Personuppgifter får lagras under längre perioder i den mån som personuppgifterna enbart behandlas för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1, under förutsättning att de lämpliga tekniska och organisatoriska åtgärder som krävs enligt denna förordning genomförs för att säkerställa den registrerades rättigheter och friheter (lagringsminimering, artikel 6.1(e) DSF).

Personuppgifter ska behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder (integritet och konfidentialitet, artikel 6.1(f) DSF).

Den personuppgiftsansvarige ska ansvara för och kunna visa att ovanstående grundprinciper efterlevs (ansvarsskyldighet, artikel 6.2 DSF).