Trafikförvaltningen
Ledningsstaben
Juridik

Handläggare
Nathalie Drugge
08-686 32 81
nathalie.drugge@sll.se

TJÄNSTEUTLÅTANDE
2021-04-28

Färdtjänstnämnden
2021-05-19, punkt 8

Ärende
FTN 2021-0016

Infosäkerhetsklass
K1 (Öppen)

Dataskyddsombudets rapportering avseende verksamhetsåret 2020

Ärendebeskrivning

Ärendet avser Dataskyddsombudets rapportering om dataskyddsarbetet inom trafikförvaltningens färdtjänstverksamhet under verksamhetsåret 2020.

Beslutsunderlag

Förvaltningschefens tjänsteutlåtande samt nedanstående underlag.

- Dataskyddsombudets rapport avseende verksamhetsåret 2020, bilaga 1

Förslag till beslut

Förvaltningschefen föreslår att färdtjänstnämnden beslutar följande.

1. Nämnden godkänner Dataskyddsombudets rapportering avseende verksamhetsåret 2020.

Förslag och motivering

Sammanfattning

De nio delområden som rapporten omfattar är kopplade till grundläggande krav i Dataskyddsförordningen.
Metodiken som har valts i rapporten är att per delområde redovisa genomfört dataskyddsarbete, dokumentera iakttagelser, och lämna förslag på hur iakttagelserna kan åtgärdas.

Det finns ett antal iakttagelser som pekar på att aktiviteter behöver genomföras för att ytterligare stärka färdtjänstverksamhetens efterlevnad av Dataskyddsförordningen.

Ett av de mest grundläggande kraven i Dataskyddsförordningen är att samtliga personuppgiftsbehandlingar ska vara dokumenterade. Ett antal personuppgiftesbehandlingar har identifierats som ännu inte dokumenterats. Att åtgärda denna iakttagelse kommer ytterligare säkerställa färdtjänstverksamhetens efterlevnad av Dataskyddsförordningen och även ge positiv inverkan på andra iakttagelser.

Bakgrund

Dataskyddsombudets roll och mandat
Dataskyddsombudets roll är att skydda de registrerades fri- och rättigheter inom personuppgiftsområdet. Det görs genom uppföljning av att dataskyddsförordningen efterlevs samt genom informations- och utbildningsinsatser.

Dataskyddsombudet är därutöver verksamhetens stöd i frågor som rör dataskydd samt kontaktpunkt för tillsynsmyndigheten (i Sverige Integritetsskyddsmyndigheten, tidigare Datainspektionen) och de registrerade.

Överväganden och motivering

Ekonomiska konsekvenser
Förslagna åtgärder bedöms kunna genomföras inom ramen för verksamhetens budget.

Riskbedömning
Att samtliga personuppgiftsbehandlingar ännu inte är dokumenterade medför att färdtjänstverksamheten har svårare att tillvarata de registrerades rättigheter i enlighet med förordningen. Det finns därför en risk för att verksamheten inte har en fullständig bild över de eventuella risker som pågående personuppgiftsbehandlingar kan medföra.

På grund av att alla personuppgiftsbehandlingar ännu inte är dokumenterade finns det risk för att det förekommer fler personuppgiftsincidenter än vad som rapporteras.

Trafikförvaltningen
Ledningsstaben
Juridik

TJÄNSTEUTLÅTANDE
2021-04-28

Ärende
FTN 2021-0016

Infosäkerhetsklass
K1 (Öppen)

Om föreslagna åtgärder inte genomförs kan en tillsyn av Integritetsskyddsmyndigheten ytterst medföra varningar, reprimander, ett förbud mot behandling, samt att sanktionsavgift påförs.

Konsekvenser för miljön
Inga konsekvenser att redovisa.

Sociala konsekvenser
Inga konsekvenser att redovisa.

David Lagneholm
Förvaltningschef

Trafikförvaltningen
Ledningsstaben
Juridik

INFORMATIONSÄRENDE
2021-04-08

Ärende/Dok. id.
2006724

Infosäk. klass
K1 (Öppen)

Handläggare
Nathalie Drugge
08-686 32 81
nathalie.drugge@sll.se

Dataskyddsombudets rapport avseende verksamhetsåret 2020, bilaga 1

1 Inledning

Denna rapport innehåller en övergripande redogörelse för hur dataskyddsarbetet har bedrivits på trafikförvaltningens färdtjänstverksamhet under 2020 kopplat till regelverket i Dataskyddsförordningen.

Den organisation som avses i rapporten är färdtjänstnämnden.

Rapporten innehåller också identifierade iakttagelser med förslag på åtgärder. Metodiken som har valts i denna rapport är att per identifierat delområde redovisa genomfört dataskyddsarbete, dokumentera iakttagelser, och lämna förslag på hur iakttagelserna kan åtgärdas.

1.1 De delområden som belyses för 2020 är:

1. hur färdtjänstverksamheten har dokumenterat sina personuppgiftsbehandlingar
2. hur färdtjänstverksamheten har hanterat de registrerades rättigheter
3. hur färdtjänstverksamheten har hanterat personuppgiftsincidenter
4. hur färdtjänstverksamheten har genomfört hanteringen av personuppgifter kopplat till specifika personuppgiftsbehandlingar (granskning enligt plan)
5. vilken kunskap medarbetare på trafikförvaltningen har om förordningen (genom årlig enkät)
6. hur Dataskyddsombudet har genomfört informationsinsatser och utbildning av verksamheten
7. iakttagelser som identifierats av Dataskyddsombudet vid granskningar
8. hur färdtjänstverksamheten agerar kring personuppgiftshanteringen kopplat till Schrems II-domen

Trafikförvaltningen
Ledningsstaben
Juridik

INFORMATIONSÄRENDE
2021-04-08

Ärende/Dok. id.
2006724

Infosäk. klass
K1 (Öppen)

2 Rapportering per delområde

2.1 Hur färdtjänstverksamheten har dokumenterat sina personuppgiftsbehandlingar

Färdtjänstnämnden är enligt förordningen skyldig att föra ett register, eller med ett annat ord en förteckning, över samtliga behandlingar av personuppgifter. Detta register ska upprättas skriftligen, vara tillgängligt i elektroniskt format och hållas uppdaterat. På begäran ska registret göras tillgängligt för tillsynsmyndigheten, Integritetsskyddsmyndigheten (IMY). Vad som ska finnas med i förteckningen beskrivs i artikel 30 i GDPR.

Färdtjänstverksamheten hanterar även sjukresor.

Under året har en ny behandling dokumenterats och upptagits i färdtjänstnämndens förteckning.

För att intensifiera arbetet med dokumentationen av prioriterade personuppgiftsbehandlingar hade DSO-funktionen för 2020 planerat särskilda punktinsatser. Till följd av omprioriteringar med anledning av pandemin har dock detta initiativ inte genomförts. Även verksamheten har fått göra nya prioriteringar pga. pandemin, vilket försenar arbetet med att dokumentera personuppgiftsbehandlingarna.

2.1.1 Iakttagelser

Det kan konstateras att det återstår ett flertal behandlingar att dokumentera.

Att samtliga personuppgiftsbehandlingar ännu inte är dokumenterade medför att färdtjänstverksamheten har svårare att tillvarata de registrerades rättigheter i enlighet med förordningen. Det finns därför en risk för att färdtjänstverksamheten inte har en fullständig bild över de eventuella risker som pågående personuppgiftsbehandlingar kan innebära.

Vid en tillsyn kan IMY bl.a. utfärda varningar, reprimander, ett förbud mot behandling, samt att påföra sanktionsavgifter.

2.1.2 Förslag till åtgärder

Färdigställandet av personuppgiftsbehandlingarna är beroende av att ansvarig verksamhet gör riktade insatser för att hantera de behandlingar som ännu inte är dokumenterade. Sådana insatser kan göra det nödvändigt att omprioritera i den löpande verksamheten.

2.2 Hur färdtjänstverksamheten har hanterat de registrerades rättigheter

Varje person vars personuppgifter färdtjänstverksamheten hanterar har rätt att från verksamheten:

- Få ut ett registerutdrag, dvs. i detalj få veta vilka uppgifter färdtjänstverksamheten har om individen.
- Begära att personuppgifterna som avser hen ska raderas.
- Begära att personuppgifterna som avser hen ska rättas.

Under vissa förutsättningar i förordningen ska färdtjänstverksamheten gå med på de registrerades begäran enligt ovan.

Förfrågningarna hanteras i enlighet med upprättade rutiner och checklista av i huvudsak ärendeansvarig på färdtjänstverksamheten.

Under året har det inkommit ett knappt hundratal förfrågningar från registrerade om registerutdrag. Samtliga förfrågningar har hanterats inom den i förordningen kravställda månaden.

2.2.1 Iakttagelser

De brister som finns kan hänföras till att samtliga personuppgiftsbehandlingar inte finns dokumenterade på färdtjänstverksamheten. Detta leder till att de förfrågningar som kommer in inte kan garanteras innehålla alla personuppgifter om personen i fråga. Indikationer på att utlämnade utdrag saknar personuppgifter har dock inte inkommit.

2.2.2 Förslag till åtgärder

Färdigställandet av personuppgiftsbehandlingarna är beroende av att ansvarig verksamhet gör riktade insatser för att hantera de behandlingar som ännu inte är dokumenterade. Sådana insatser kan göra det nödvändigt att omprioritera i den löpande verksamheten.

2.3 Hur färdtjänstverksamheten har hanterat personuppgiftsincidenter

För att kunna leva upp till skyldigheterna enligt Dataskyddsförordningen är det viktigt att organisationer som behandlar personuppgifter har rutiner på plats för att kunna upptäcka, rapportera och utreda personuppgiftsincidenter.

En personuppgiftsincident är en informationssäkerhetshändelse som har påverkat sekretessen, integriteten eller tillgängligheten till personuppgifter. En personuppgiftsincident är en informationssäkerhetsincident som leder till:

- oavsiktlig eller avsiktlig förstöring
- förlust eller ändring
- obehörigt röjande
- obehörig åtkomst

av behandlade personuppgifter.

Enligt Dataskyddsförordningen måste alla organisationer anmäla vissa typer av personuppgiftsincidenter till IMY inom 72 timmar efter det att överträdelsen har upptäckts. Alla identifierade och inrapporterade personuppgiftsincidenter på färdtjänstverksamheten ska dokumenteras även om de inte leder till att incidenten rapporteras till IMY.

Det är informationsägaren/verksamhetschefen som ansvarar för att hantera inkomna personuppgiftsincidenter enligt den fastställda incidenthanteringsprocessen på TF.

Under året har det rapporterats in tjugoåtta personuppgiftsincidenter.

De dokumenterade incidenterna delas upp i fyra nivåer, nivå ett är den allvarligaste nivån och behöver rapporteras in till IMY.

Under året har två personuppgiftsincidenter rapporterats till IMY. I båda fallen handlar det om obehörigt röjande, dvs. personuppgifter har spridits på ett felaktigt sätt. Personerna som är berörda har förlorat kontrollen över sina personuppgifter. I båda fallen har alla fyra involverade personer blivit informerade om de inträffade och de felaktiga uppgifterna returnerade till färdtjänstverksamheten.

I de övriga inrapporterade personuppgiftsincidenterna handlar det också om obehörigt röjande men personuppgifterna som röjts har inte varit av känslig karaktär. I dessa fall beror röjandet på den mänskliga faktorn. Vid alla tillfällen är det en enstaka individ som drabbats.

2.3.1 Iakttagelser

Eftersom samtliga personuppgiftsbehandlingar på färdtjänstverksamheten ännu inte är dokumenterade finns det risk för att det förekommer fler personuppgiftsincidenter än vad som rapporteras.

Medvetenheten hos trafikförvaltningens medarbetare kring vad som är en personuppgiftsincident och hur dessa ska rapporteras och hanteras har ökat enligt den medarbetarenkät som genomförts 2019 och 2020.

2.3.2 Förslag till åtgärder

Färdigställandet av personuppgiftsbehandlingarna är beroende av att ansvarig verksamhet gör riktade insatser för att hantera de behandlingar som ännu inte är dokumenterade. Sådana insatser kan göra det nödvändigt att omprioritera i den löpande verksamheten.

2.4 Hur färdtjänstverksamheten har genomfört hanteringen av personuppgifter kopplat till specifika personuppgiftsbehandlingar (granskning enligt plan)

Syftet med granskningarna är att säkerställa att TF har en korrekt och rättssäker hantering av personuppgifter. Detta görs genom att granska arbetssätt och systemstöd, identifiera iakttagelser samt följa upp att föreslagna förbättringsåtgärder genomförs. Varje dokumenterad personuppgiftsbehandling ska under en 3-årsperiod bli föremål för granskning. En granskningsplan upprättas för respektive verksamhetsår. Fokus för respektive granskning bestäms utifrån; 3-årig rullande granskningsplan, nya lagkrav, utfall från tidigare granskningar, identifierade risker och personuppgiftsincidenter.

Under 2020 granskades färdtjänstverksamhetens personuppgiftsbehandlingar.

2.4.1 Iakttagelser

Vid granskningstillfället konstaterades att konsekvensbedömningar saknas. Brister i dokumentation av konsekvensbedömningar medför att färdtjänstverksamheten inte har en fullständig bild över de eventuella risker som pågående personuppgiftsbehandlingar kan innebära, vilka i sin tur kan påverka de registrerades rättigheter och friheter.

2.4.2 Förslag till åtgärder

I samband med den planerade granskningen är informationsägaren ansvarig för att ta fram förslag till förbättringsåtgärder samt genomföra dessa för att åtgärda

identifierade brister. DSO-funktionen följer upp planen tills bristerna är åtgärdade.

2.5 Vilken kunskap medarbetare på trafikförvaltningen har om förordningen genom årlig enkät

En enkät skickades ut till ca 20 % av totala antalet medarbetare och konsulter. Drygt hälften besvarade enkäten vilket är något högre antal än 2019. Vid jämförelse av resultat mellan 2019 och 2020 års enkät kan konstateras att kunskapen om hantering av personuppgifter har ökat, vilket också bekräftas genom ett ökat inflöde av identifierade personuppgiftsbehandlingar.

2.5.1 Iakttagelser

Sammantaget kan konstateras att medvetenhet om att personuppgifter hanteras av många av oss i det vardagliga arbetet kan höjas ytterligare och detsamma gäller den grundläggande kunskapsnivån.

2.5.2 Förslag till åtgärder

Inkludera e-utbildningen i de utbildningar som är obligatoriska för alla medarbetare att genomföra.

Den lärarledda utbildningen blir obligatorisk för informationsägare och medarbetare som i sitt arbete hanterar personuppgifter.

2.6 Hur Dataskyddsombudet har genomfört informationsinsatser och utbildning av verksamheten

En av Dataskyddsombudet huvuduppgifter är att informera och utbilda medarbetare hos den personuppgiftsansvariga, dvs. färdtjänstverksamheten.

En e-utbildning som ger basala kunskaper i dataskyddsförordningen erbjuds alla medarbetare via en regiongemensam utbildning som finns tillgänglig i utbildningsportalen Lärtorget.

Lärarledd utbildning erbjuds varje månad (utom juli och december). Denna utbildning riktar sig till samtliga medarbetare på trafikförvaltningen som hanterar personuppgifter.

För att medarbetarna ska få en bättre insyn i vad som händer på trafikförvaltningen men även i omvärlden kopplat till dataskyddsförordningen skickar jag ut ett nyhetsbrev regelbundet inom förvaltningen. Brevet innehåller information om hur internt och externt dataskyddsarbete påverkar

medarbetarna och den personuppgiftsbehandling de arbetar med. Nyhetsbrevet kommer ut fyra gånger per år.

DSO ordnar interna nätverksmöten fyra gånger per år för att medarbetarna som i sitt arbete hanterar personuppgifter ska få möjlighet att skapa nya kontakter inom trafikförvaltningen. Mötena skapar transparents, kunskaps- och erfarenhetsöverföring samt bidrar till att framtagna rutiner, processer, mallar, arbetssätt utvecklas.

2.6.1 Iakttagelser

E-utbildningen ingår inte i utbildningspaketet för nyanställda. Med hänvisning till att en personuppgiftsansvarig ska kunna påvisa att personalen är kunnig om reglerna i förordningen är målsättningen att e-utbildningen ska bli obligatorisk.

2.6.2 Åtgärdsförslag

Inkludera e-utbildningen i de utbildningar som är obligatoriska för alla medarbetare att genomföra.

Den lärarledda utbildningen blir obligatorisk för informationsägare och medarbetare som i sitt arbete hanterar personuppgifter.

2.7 Brister som identifierats av Dataskyddsombudet vid granskningar

Den mest prioriterade uppgiften för Dataskyddsombudet är att övervaka att organisationen följer dataskyddsförordningen. Det innebär bland annat att samla in information om hur organisationen behandlar personuppgifter, kontrollera att organisationen följer gällande lagstiftning, myndigheters föreskrifter och interna policys, riktlinjer och rutiner.

En av huvudprinciperna i dataskyddsförordningen är principen om ansvarsskyldighet. Denna princip innebär att den personuppgiftsansvariga, dvs. färdtjänstverksamheten ansvarar för och ska visa att grundprinciperna efterlevs. Detta innebär i praktiken att färdtjänstverksamheten ska kunna visa upp dokumentation som beskriver att man efterlever kraven i dataskyddsförordningen.

2.7.1 Iakttagelser

Dokumentationen för identifierade behandlingar behöver arbetas vidare med.

Att samtliga personuppgiftsbehandlingar inte är dokumenterade medför att färdtjänstverksamheten har svårare att tillvarata de registrerades rättigheter i

enlighet med förordningen. Det finns därför en risk att färdtjänstverksamheten inte har en fullständig bild över de eventuella risker som pågående personuppgiftsbehandlingar kan innebära.

Brister i hanteringen av personuppgifter kan också leda till att personuppgiftsincidenter inträffar, exempelvis att uppgifter röjs eller hamnar i orätta händer. Detta kan få negativa konsekvenser för de vars personuppgifter färdtjänstverksamheten hanterar.

Vid en tillsyn kan IMY bl.a. utfärda varningar, reprimander, ett förbud mot behandling, samt att påföra sanktionsavgifter.

2.7.2 Åtgärdsförslag

Färdigställandet av personuppgiftsbehandlingarna är beroende av att ansvarig verksamhet gör riktade insatser för att hantera de behandlingar som ännu inte är dokumenterade. Sådana insatser kan göra det nödvändigt att omprioritera i den löpande verksamheten.

2.8 Hur färdtjänstverksamheten agerar kring personuppgiftshanteringen kopplat till Schrems II-domen

I dataskyddsförordningen föreskrivs att överföring av personuppgifter till tredje land (i dataskyddsförordningen avses ett land utanför EU/EES) endast får ske under förutsättning att det aktuella tredje landet säkerställer en adekvat skyddsnivå för dessa uppgifter.

Ansvaret för att tillse att överföring av personuppgifter till tredje land är laglig vilar på den personuppgiftsansvariga, i det här fallet färdtjänstnämnden, genom färdtjänstverksamheten.

I ett mål från EU-domstolen som avgjordes under 2020, det s.k. Schrems II-målet, har domstolen bedömt om det är lagligt för Facebook att överföra personuppgifter till USA med stöd av antingen EU-US Privacy Shield – eller EU-kommissionens publicerade standardavtalsklausuler för överföring av personuppgifter till länder utanför EU/EES.

Enligt domen ger regleringen i Privacy Shield inte det skydd som krävs för överföring av personuppgifter till USA, varför sådan överföring inte längre kan ske med stöd av Privacy Shield.

En överföring till USA och annat tredje land med stöd av EU:s standardavtalsklausuler är som utgångspunkt möjligt, men behöver enligt domen ses över. Eftersom standardavtalsklausulerna är en överenskommelse mellan två parter, men inte inkluderar myndigheterna i tredje land där mottagaren befinner sig, är det osäkert om överföring av personuppgifter på rent avtalsrättslig grund med stöd av standardavtalsklausuler kan säkerställa en adekvat skyddsnivå.

När det gäller överföring av personuppgifter till USA kan det för närvarande inte slås fast om en överföring kan ske enbart med stöd av dessa klausuler. Skälet är att vissa amerikanska myndigheter, genom olika typer av övervakningsåtgärder, under vissa förhållanden skulle kunna få tillgång till personuppgifter.

Det finns ingen övergångsperiod, domen meddelades den 16 juli 2020 och gäller därmed direkt.

2.8.1 Iakttagelser

Inom färdtjänstverksamheten finns det personuppgiftsbehandlingar där personuppgifter överförs till bolag i tredje land.

En heltäckande bild av hur många avtal inom färdtjänstverksamheten som berörs och behöver hanteras är vid skrivandet av denna rapport inte klarlagt.

2.8.2 Åtgärdsförslag

De personuppgiftsbehandlingar som berörs behöver ses över med hänsyn till Schrems II-domen.

Åtgärder behöver även riktas mot pågående och kommande upphandlingar och inköp för att säkra att eventuell tredjelandsöverföring efterlever ny rättspraxis.

För att komplettera de reaktiva åtgärderna ovan föreslås att trafikförvaltningen implementerar en strategi för tredjelandsöverföringar.