Trafikförvaltningen
Ledningsstaben
Juridik

Handläggare
Nathalie Drugge
+46 8 123 332 81
nathalie.drugge@regionstockholm.se

TJÄNSTEUTLÅTANDE
2021-12-20

Färdtjänstnämnden
2022-01-26, punkt 4

Ärende
FTN 2021-0057

Infosäkerhetsklass
K1 (Öppen)

Dataskyddsombudets rapportering avseende verksamhetsåret 2021

Ärendebeskrivning

Ärendet avser Dataskyddsombudets rapportering om dataskyddsarbetet inom trafikförvaltningens färdtjänstverksamhet under verksamhetsåret 2021.

Beslutsunderlag

Förvaltningschefens tjänsteutlåtande samt nedanstående underlag.

- Dataskyddsombudets rapport avseende verksamhetsåret 2021, bilaga 1

Förslag till beslut

Förvaltningschefen föreslår att färdtjänstnämnden beslutar följande.

1. Nämnden godkänner Dataskyddsombudets rapportering avseende verksamhetsåret 2021.

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 personuppgifts-behandlingar har identifierats men har 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 tillvarata 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, IMY) 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.

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

Konsekvenser för miljön
Inga konsekvenser att redovisa.

Trafikförvaltningen
Ledningsstaben
Juridik

TJÄNSTEUTLÅTANDE
2021-12-20

Ärende
FTN 2021-0057

Infosäkerhetsklass
K1 (Öppen)

Sociala konsekvenser
Inga konsekvenser att redovisa.

David Lagneholm
Förvaltningschef

Trafikförvaltningen
Ledningsstaben
Juridik

INFORMATIONSÄRENDE
2021-12-03
Version

Ärende/Dok. id.
2218086

Infosäk. klass
K1 (Öppen)

Handläggare
Nathalie Drugge
+46 8 123 332 81
nathalie.drugge@regionstockholm.se

Dataskyddsombudets rapport avseende verksamhetsåret 2021, bilaga 1

1 Inledning

Denna rapport innehåller en övergripande redogörelse för hur dataskyddsarbetet har bedrivits på trafikförvaltningens färdtjänstverksamhet under 2021 kopplat till bestämmelserna 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 2021 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 vid granskningar

Trafikförvaltningen
Ledningsstaben
Juridik

INFORMATIONSÄRENDE
2021-12-03
Version

Ärende/Dok. id.
2218086

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, Integritetsskydds-myndigheten (IMY). Vad som ska finnas med i förteckningen beskrivs i artikel 30 i GDPR.

Färdtjänstverksamheten hanterar även sjukresor.

Under året har inga nya behandlingar dokumenterats och upptagits i färdtjänst-nämndens förteckning.

2.1.1 Iakttagelser

Det kan konstateras att det återstår behandlingar att dokumentera. Dessa är: tjänstekort för medarbetare inom regionen, Anbaro undersökningen, uppföljning av taxiförare och resenär, ersättning för utebliven resa samt klagomålshantering

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 medföra en omprioritering 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 trettiotal förfrågningar från registrerade om registerutdrag. Det är färre förfrågningar än under föregående år. 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 medföra en omprioritering 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 personuppgifts-incident 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 23 personuppgiftsincidenter inrapporterats.

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 det ena fallet har även berörda personer blivit informerade om det inträffade.

Dessa två incidenter
I oktober 2021 sändes en begäran om komplettering av färdtjänstansökan till en felaktig adress. Med begäran hade bifogats en kopia på tidigare insänd ansökningsblankett. Eftersom blanketten innehöll vissa uppgifter om sökandes hälsa så gjordes en anmälan till Integrationsskyddsmyndigheten (IMY), som 05-12-21 beslutade att avsluta ärendet utan åtgärd.

I november uppmärksammades brister i inloggningen till tjänsten Talsvar. Användare som bytt lösenord till tjänsten kunde trots detta även logga in med det äldre lösenordet. Efter felsökning kunde tekniker omgående avhjälpa felet. Det finns inga indikationer på att obehöriga har kunnat komma åt de adressuppgifter som finns i systemet, men då incidenten potentiellt kunde ha drabbat ett stort antal resenärer så anmäldes incidenten till IMY som ännu inte återkommit med ett beslut i ärendet.

Övriga 21 inrapporterade personuppgiftsincidenter avser även dessa 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 TF:s medarbetare kring vad som är en personuppgiftsincident och hur dessa ska rapporteras och hanteras har inte ökat nämnvärt enligt den medarbetarenkät som genomförts 2019, 2020 och 2021. 2021-års resultat är något sämre än under föregående år, vilket möjligen kan hänföras till urvalet av respondenter och att ett högre antal konsulter deltagit i årets enkät jämfört med 2020-års enkät.

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 medföra en omprioritering i den löpande verksamheten.

Föreslås att information publiceras på intranätet samt att en kortare digital utbildning om personuppgiftsincidenter tas fram och distribueras till samtliga medarbetare för att ytterligare höja kunskapsnivån.

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 iakttagelser och förbättringsåtgärder genomförs. Varje dokumenterad personuppgiftsbehandling ska årligen uppdateras. Dataskyddsombudet granskar uppdateringen och personuppgiftsbehandlingen återigen fastställas av informationsägaren. En granskningsplan upprättas för respektive verksamhetsår. Fokus för respektive granskning bestäms utifrån; beslutade fokusområden, nya lagkrav, utfall från tidigare granskningar, identifierade risker och personuppgiftsincidenter.

Under 2021 har ingen ny granskning genomförts. De allvarliga iakttagelser som dokumenterades som ett resultat av 2020-års granskning har följts upp under 2021.

2.4.1 Iakttagelser

De allvarliga iakttagelser som rapporterades 2020 kvarstår. Det vill säga att det fortfarande saknas konsekvensbedömningar. 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 på TF. 56 % av de slumpvis utvalda har besvarat enkäten, vilket är något högre än 2020. Vid jämförelse av resultat mellan 2019, 2020 och 2021 års enkät kan konstateras att kunskapen om hantering av personuppgifter inte har ökat nämnvärt. Utifrån att alltfler personuppgiftsbehandlingar identifieras kan det dock konstateras att kunskapen ökar.

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

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 distribueras ett nyhetsbrev

regelbundet ut 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-funktionen 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, ger möjlighet till kunskaps- och erfarenhetsöverföring samt bidrar till att framtagna rutiner, processer, mallar, arbetssätt utvecklas.

2.6.1 Iakttagelser

En personuppgiftsansvarig ska kunna påvisa att personalen som hanterar personuppgifter har kunskap om reglerna i förordningen. Med tanke på den stora mängden personuppgiftsbehandlingar och därmed personer som hanterar personuppgifter på färdtjänstverksamheten är det fler som behöver genomföra den lärarledda utbildningen.

2.6.2 Åtgärdsförslag

Den lärarledda utbildningen blir obligatorisk för nya 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 medföra en omprioritering i den löpande verksamheten.