Trafikförvaltningen
Ledningsstaben
Juridik

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

TJÄNSTEUTLÅTANDE
2022-01-13

Trafiknämnden
2022-01-25, punkt 6

Ärende
TN 2021-0010

Infosäkerhetsklass
K1 (Öppen)

Dataskyddsombudets rapportering avseende verksamhetsåret 20201

Ärendebeskrivning

Ärendet avser Dataskyddsombudets rapportering om dataskyddsarbetet på trafikförvaltningen under verksamhetsåret 2021.

Beslutsunderlag

Förvaltningschefens tjänsteutlåtande samt nedanstående underlag.

- Dataskyddsombudets rapport avseende verksamhetsåret 2021, bilaga 1

Förslag till beslut

Förvaltningschefen föreslår att trafiknämnden beslutar följande.

1. Nämnden godkänner Dataskyddsombudets rapportering avseende verksamhetsåret 2021.

Förslag och motivering

Sammanfattning

De åtta 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 åtgärder behöver genomföras för att ytterligare säkerställa trafikförvaltningens efterlevnad av Dataskyddsförordningen.

Ett av de mest grundläggande kraven i Dataskyddsförordningen är att samtliga personuppgiftsbehandlingar ska vara dokumenterade. Ett större antal personuppgiftesbehandlingar har identifierats, men ännu inte dokumenterats. Att åtgärda denna iakttagelse kommer ytterligare säkerställa trafikförvaltningens efterlevnad av Dataskyddsförordningen och även ha en 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 granskning och uppföljning samt genom informations- och utbildningsinsatser.

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

Överväganden och motivering

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

Riskbedömning
Att samtliga personuppgiftsbehandlingar ännu inte är dokumenterade medför att TF har svårare att tillvarata de registrerades rättigheter i enlighet med förordningen. Det finns därför en risk för att TF 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 sanktionsavgift påförs.

Trafikförvaltningen
Ledningsstaben
Juridik

TJÄNSTEUTLÅTANDE
2022-01-13

Ärende
TN 2021-0010

Infosäkerhetsklass
K1 (Öppen)

Konsekvenser för miljön
Inga konsekvenser att redovisa.

Sociala konsekvenser
Inga konsekvenser att redovisa.

David Lagneholm
Förvaltningschef

Trafikförvaltningen
Ledningsstaben
Juridik

INFORMATIONSÄRENDE
2021-12-03
Version

Ärende/Dok. id.
2209240

Infosäk. klass
K1 (Öppen)

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

Dataskyddsombudets rapport avseende verksamhetsåret 2021, bilaga 1

Inledning

Denna rapport innehåller en övergripande redogörelse för hur dataskyddsarbetet har bedrivits på trafikförvaltningen under 2021 kopplat till bestämmelserna i Dataskyddsförordningen.

De organisationer som avses i rapporten är trafiknämnden och däri ingående verksamheter AB Storstockholms Lokaltrafik och Waxholms Ångfartygs AB. Dessa organisationer benämns i fortsättningen gemensamt trafikförvaltningen/TF.

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 trafikförvaltningen har dokumenterat sina personuppgiftsbehandlingar
2. hur trafikförvaltningen har hanterat de registrerades rättigheter
3. hur trafikförvaltningen har hanterat personuppgiftsincidenter
4. hur trafikförvaltningen har hanterat 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
8. den tillsyn som Integritetsskyddsmyndigheten påbörjade 2018 kopplat till kroppsburna kameror i biljettkontrollen

2 Rapportering per delområde

2.1 Hur trafikförvaltningen har dokumenterat sina personuppgiftsbehandlingar

Trafiknämnden 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 Dataskyddsförordningen.

Varje informationsägare/verksamhetschef inom trafikförvaltningen är ansvarig för att se till att dennes verksamhetsområde har dokumenterat sina personuppgiftsbehandlingar.

Under året har ett antal behandlingar upptagits i trafikförvaltningens förteckning.

2.1.1 Iakttagelser

Det kan konstateras att det återstår ett flertal behandlingar att dokumentera utifrån 2019 och 2020 års prioriterade områden. Under 2020 identifierades ett sjuttiotal behandlingar som inte tidigare varit dokumenterade och under 2021 har ytterligare ett drygt sextiotal behandlingar identifierats.

Att samtliga personuppgiftsbehandlingar ännu inte är dokumenterade medför att TF har svårare att tillvarata de registrerades rättigheter i enlighet med förordningen. Det finns därför en risk för att TF 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 trafikförvaltningen har hanterat de registrerades rättigheter

Varje person vars personuppgifter TF hanterar har rätt att från TF:

- Få ut ett registerutdrag, dvs. i detalj få veta vilka uppgifter TF 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 TF gå med på de registrerades begäran enligt ovan.

Förfrågningarna hanteras i enlighet med upprättade rutiner och checklista av i huvudsak DSO-funktionen men även av SL Kundtjänst som hanterar förfrågningar som enbart berör kundärenden.

Under året har det inkommit ett hundratjugotal förfrågningar från registrerade. Majoriteten har avsett registerutdrag eller begäran om radering, ett fåtal har avsett andra typer av dataskyddsfrågor. 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 TF. Detta leder till att de förfrågningar som inkommer 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 trafikförvaltningen 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 TF 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 ett knappt fyrtiotal 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 ingen personuppgiftsincident rapporterats till IMY.

Sex personuppgiftsincidenter har bedömts som allvarliga, men man har bedömt det som osannolikt att incidenten medfört risker för den registrerade, nivå två. Incidenterna berör antingen ett fåtal registrerade eller liten mängd personuppgifter. Övriga personuppgiftsincidenter har bedömts som begränsat allvarliga, nivå tre. Majoriteten av dessa avser röjande av personuppgift och är kopplade till kundtjänst-ärenden. I dessa fall beror röjandet på den mänskliga faktorn. Vid samtliga tillfällen är det en enstaka individ som drabbats.

2.3.1 Iakttagelser

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

Medvetenheten hos TF:s medarbetare kring vad som är en personuppgiftsincident och hur dessa ska rapporteras och hanteras har inte ökat nämnvärt enligt den medarbetar-enkät 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 trafikförvaltningen 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.

2020 genomförde Dataskyddsombudet elva granskningar och under 2021 har nio granskningar genomförts.

2.4.1 Iakttagelser

Brister som noterats vid granskningar under året avser bland annat nedanstående.

- Mindre brister i personuppgiftsbehandlingar och konsekvensbedömningar.
- Brister i kunskap om hantering av personuppgiftsincidenter och TF:s process för personuppgiftsincidenter.
- Personuppgiftsbiträdesavtal har inte upprättats med personuppgiftsbiträde.

Bristande kunskap om personuppgiftsincidenter och hur dessa ska hanteras inom trafikförvaltningen medför att trafikförvaltningen inte har en fullständig bild över de eventuella risker som kan påverka de registrerades rättigheter och friheter.

Att personuppgiftsbiträdesavtal inte upprättats kan få till följd att personuppgiftsbiträdet behandlar de personuppgifter som biträdet uppdragits att behandla på ett

felaktigt sätt. Detta medför i sin tur att de registrerades rättigheter och friheter kan komma att påverkas.

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. 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. TF.

En e-utbildning som ger basala kunskaper i dataskyddsförordningen erbjuds samtliga 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 TF som hanterar personuppgifter.

Nya informationsägare/verksamhetschefer erhåller, i samband med att nya personuppgiftsbehandlingar fastställs, utbildning i vad rollen Informationsägare innebär. Särskilt fokus läggs på hantering av personuppgiftsincidenter.

För att medarbetarna ska få en bättre insyn i vad som händer på TF men även i omvärlden kopplat till dataskyddsförordningen distribueras 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-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 TF. Mötena skapar transparens, 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 TF är det få som genomfört den lärarledda utbildningen.

2.6.2 Åtgärdsförslag

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 personuppgiftsansvarige, dvs. TF ansvarar för och ska kunna påvisa att grundprinciperna efterlevs. Detta innebär i praktiken att TF ska kunna visa upp dokumentation som beskriver att man efterlever kraven i dataskyddsförordningen.

2.7.1 Iakttagelser

Under året har hanteringen av personuppgifter kopplat till införandet av Microsoft 365 och Teams identifierats som ett område som behöver utredas noggrant innan användningen av tjänsterna påbörjas.

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

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

2.7.2 Åtgärdsförslag

Användningen av molnbaserade applikationer behöver fortsatt ses över med hänvisning till dataskyddsförordningens krav och ny rättspraxis.

2.8 Den tillsyn som Integritetsskyddsmyndigheten påbörjade 2018 kopplat till kroppsburna kameror i biljettkontrollen

Integritetsskyddsmyndigheten har som en av sina huvuduppgifter att övervaka och verkställa tillämpningen av dataskyddsförordningen inklusive att genomföra tillsyn. IMY har också korrigerande befogenheter som i korthet innebär att de kan:

- Utfärda varningar eller reprimander till en personuppgiftsansvarig
- Införa en begränsning av, inklusive förbud mot, behandling
- Förelägga om rättelse eller radering av personuppgifter
- Påföra administrativa sanktionsavgifter

Den 22 november 2018 inledde IMY en tillsyn mot AB SL:s hantering av personuppgifter kopplat till användningen av kroppsburna kameror i biljettkontrollen.

Den 21 juni 2021 kom IMY:s beslut i ärendet. IMY anser att kroppsburna kameror i biljettkontrollen kan användas för att förebygga och dokumentera hotfulla situationer, men att tiden för förinspelningen behöver minskas till maximalt 15 sekunder. Myndigheten anser däremot inte att kroppsburna kameror kan användas på motsvarande sätt för att säkerställa identitet på den som rest utan giltigt färdbevis. Här räcker det i stället med exempelvis stillbilder och ingen ljudinspelning. IMY konstaterar också att SL brustit i sitt sätt att informera om användningen av kroppsburna kameror, bland annat vad gäller att inte enbart bild utan även ljud spelas in.

IMY utfärdar därför en administrativ sanktionsavgift mot SL på 16 miljoner kronor. SL har överklagat beslutet till förvaltningsrätten. Målet är inte avgjort i domstol ännu.