Ekobrottsmyndigheten
Rättsenheten
Box 22098
101 36 STOCKHOLM

Tillsyn brottsdatalagen (2018:1177) - Ekobrottsmyndighetens rutiner för hantering av personuppgiftsincidenter

Innehållsförteckning

Datainspektionens beslut

Datainspektionen meddelar följande rekommendationer med stöd av 5 kap. 6 § brottsdatalagen (2018:1177):

1. Ekobrottsmyndigheten bör regelbundet utvärdera effektiviteten hos de vidtagna säkerhetsåtgärderna för att upptäcka personuppgiftsincidenter och vid behov revidera dessa för att upprätthålla tillräckligt skydd av personuppgifter.

2. Ekobrottsmyndigheten bör regelbundet kontrollera att rutinerna för hantering av personuppgiftsincidenter följs.

3. Ekobrottsmyndigheten bör regelbundet kontrollera att de interna rutinerna för dokumentation av personuppgiftsincidenter följs.

4. Ekobrottsmyndigheten bör ge sina anställda löpande information och återkommande utbildning i hanteringen av personuppgiftsincidenter och om rapporteringsskyldigheten.

Datainspektionen avslutar ärendet.

Redogörelse för tillsynsärendet

Skyldigheten för den personuppgiftsansvarige – dvs. privata och offentliga aktörer – att anmäla vissa personuppgiftsincidenter till Datainspektionen infördes den 25 maj 2018 genom dataskyddsförordningen[1] (GDPR). Motsvarande anmälningsskyldighet infördes den 1 augusti 2018 i brottsdatalagen (BDL) för s.k. behöriga myndigheter.[2] Skyldigheten att anmäla personuppgiftsincidenter (nedan kallad incident) syftar till att stärka integritetsskyddet genom att Datainspektionen får information om händelsen och kan välja att vidta åtgärder när inspektionen bedömer att det behövs för att den personuppgiftsansvarige ska hantera incidenten på ett tillfredställande sätt och vidta åtgärder för att förhindra att något liknande inträffar igen.

En personuppgiftsincident är enligt 1 kap. 6 § BDL en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring, eller obehörigt röjande av eller obehörig åtkomst till personuppgifter. I förarbetena till lagen anges att det som regel är fråga om en oplanerad händelse som påverkar säkerheten för personuppgifterna på ett negativt sätt och som medför allvarliga konsekvenser för skyddet av uppgifterna.[3] En personuppgiftsincident kan till exempel vara att personuppgifter har skickats till fel mottagare, att tillgången till personuppgifterna har förlorats, att datautrustning som lagrar personuppgifter har tappats bort eller stulits, att någon inom eller utanför organisationen tar del av information som den saknar behörighet till.

En personuppgiftsincident som inte snabbt åtgärdas på lämpligt sätt kan medföra risker för den registrerades rättigheter eller friheter. En incident kan leda till fysisk, materiell eller immateriell skada genom exempelvis

---

[1] EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

[2] En behörig myndighet är enligt i 1 kap. 6 § BDL en myndighet som behandlar personuppgifter i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet.

[3] Prop.2017/18:232 s. 438

diskriminering, identitetsstöld, identitetsbedrägeri, skadat anseende, finansiell förlust samt brott mot sekretess eller tystnadsplikt.

Det kan finnas många orsaker till att en personuppgiftincident uppstår. Av Datainspektionens rapportserie *Anmälda personuppgiftsincidenter* under perioden maj 2018 - december 2019 framgår att de vanligaste orsakerna bakom de anmälda incidenterna var bl.a. den mänskliga faktorn, tekniska fel, antagonistiska angrepp samt brister i organisatoriska rutiner eller processer.[4]

Datainspektionen har inlett detta tillsynsärende mot Ekobrottsmyndigheten i syfte att kontrollera om myndigheten har rutiner på plats för att upptäcka personuppgiftsincidenter och om myndigheten har och har haft rutiner för att hantera personuppgiftsincidenter enligt brottsdatalagen. I granskningen ingår även att kontrollera om Ekobrottsmyndigheten har rutiner för dokumentation av incidenter som svarar mot kraven i brottsdataförordningen (BDF) samt om myndigheten har genomfört informations- och utbildningsinsatser kring personuppgiftsincidenter.

Tillsynen inleddes med en skrivelse till Ekobrottsmyndigheten den 19 juni 2019 och följdes upp med begäran om komplettering den 28 januari 2020. Myndighetens svar på tillsynsskrivelsen kom in den 25 september 2019 och kompletteringen inkom den 18 februari 2020.

Tillämpliga bestämmelser

Den personuppgiftsansvarige ska enligt 3 kap. 2 § BDL, genom lämpliga tekniska och organisatoriska åtgärder, säkerställa och kunna visa att behandlingen av personuppgifter är författningsenlig och att den registrerades rättigheter skyddas. Det innebär att behöriga myndigheter, med hjälp av dessa åtgärder, inte bara ska säkerställa att dataskyddsregelverket följs utan också ska kunna visa att så är fallet. Vilka tekniska och organisatoriska åtgärder som krävs för att skydda personuppgifterna regleras i 3 kap. 8 § BDL.

---

[4] Se Datainspektionens rapportserie om Anmälda personuppgiftsincidenter 2018 (Datainspektionens rapport 2019:1) s 7 f; Anmälda personuppgiftsincidenter januari-september 2019 (Datainspektionens rapport 2019:3) s.10 f. och Anmälda personuppgiftsincidenter 2019 (Datainspektionens rapport 2020:2) s. 12 f.

I förarbetena till lagen anges att organisatoriska åtgärder som avses i 2 § är bl.a. att ha interna strategier för dataskydd, att informera och utbilda personalen och att säkerställa en tydlig ansvarsfördelning. Åtgärder som vidtas för att visa att behandlingen är författningsenlig kan t.ex. vara dokumentation av IT-system, behandlingar och vidtagna åtgärder och teknisk spårbarhet genom loggning och logguppföljning. Vilka åtgärder som ska vidtas får avgöras efter en bedömning i varje enskilt fall.[5] Åtgärderna ska ses över och uppdateras vid behov. De åtgärder som den personuppgiftsansvarige ska vidta enligt denna bestämmelse ska enligt 3 kap. 1 § BDF vara rimliga med beaktande av behandlingens art, omfattning, sammanhang och ändamål och de särskilda riskerna med behandlingen.

Av 3 kap. 8 § BDL framgår att den personuppgiftsansvarige ska vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas, särskilt mot obehörig eller otillåten behandling och mot förlust, förstöring eller annan oavsiktlig skada. I förarbetena till brottsdatalagen anges att säkerheten ska omfatta åtkomstskydd för utrustning, kontroll av datamedier, lagringskontroll, användarkontroll, åtkomstkontroll, kommunikationskontroll, indatakontroll, transportkontroll, återställande, driftsäkerhet och dataintegritet. Denna uppräkning är dock inte uttömmande. Som exempel på organisatoriska säkerhetsåtgärder kan nämnas fastställandet av en säkerhetspolicy, kontroller och uppföljning av säkerheten, utbildning i datasäkerhet och information om vikten av att följa gällande säkerhetsrutiner. Rutiner för anmälan och uppföljning av personuppgiftsincidenter utgör också sådana åtgärder.[6]

Vilka omständigheter som bör beaktas för att uppnå en lämplig skyddsnivå är reglerat i 3 kap. 11 § BDF. Åtgärderna ska åstadkomma en säkerhetsnivå som är lämplig med beaktande av de tekniska möjligheterna, kostnaderna för åtgärderna, behandlingens art, omfattning, sammanhang och ändamål, samt de särskilda riskerna med behandlingen. Särskild hänsyn bör tas till i vilken utsträckning känsliga personuppgifter behandlas och hur integritetskänsliga övriga personuppgifter som behandlas är.[7] Överträdelse av bestämmelser i

[5] Prop. 2017/18:232 s. 453
[6] Prop. 2017/18:232 s. 457
[7] Prop. 2017/18:232 s. 189 f.

3 kap. 2 och 8 §§ BDL kan leda till sanktionsavgifter enligt 6 kap. 1 § 2 BDL.

Den personuppgiftsansvarige ska enligt 3 kap. 14 § BDF dokumentera alla personuppgiftsincidenter. Dokumentationen ska redovisa omständigheterna kring incidenten, dess effekter och de åtgärder som vidtagits med anledning av den. Den personuppgiftsansvarige ska dokumentera alla inträffade incidenter oavsett om den måste anmälas till Datainspektionen eller inte.[8] Dokumentationen ska göra det möjligt för tillsynsmyndigheten att kontrollera efterlevnaden av den aktuella bestämmelsen. Underlåtenhet att dokumentera personuppgiftsincidenter kan föranleda sanktionsavgifter enligt 6 kap. 1 § BDL.

En personuppgiftsincident ska också, enligt 3 kap. 9 § BDL, anmälas till Datainspektionen senast 72 timmar efter det att den personuppgiftsansvarige fått kännedom om incidenten. En anmälan behöver inte göras om det är osannolikt att incidenten har medfört eller kommer att medföra någon risk för otillbörligt intrång i den registrerades personliga integritet. Av 3 kap. 10 § BDL framgår att den personuppgiftsansvarige i vissa fall ska informera den registrerade som berörs av incidenten. Underlåtenhet att anmäla en personuppgiftsincident till Datainspektionen kan leda till administrativa sanktionsavgifter enligt 6 kap. 1 § BDL.[9]

Motivering av beslut

Datainspektionens granskning

Datainspektionen har i detta tillsynsärende att ta ställning till om Ekobrottsmyndigheten har rutiner för att upptäcka personuppgiftsincidenter enligt brottsdatalagen och om myndigheten har och har haft rutiner för att hantera incidenter sedan BDL trädde ikraft. Granskningen omfattar även frågan om efterlevnaden av kravet på dokumentation av incidenter i 3 kap. 14 § BDF. Därutöver ska Datainspektionen ta ställning till om Ekobrottsmyndigheten har genomfört informations- och utbildningsinsatser

[8] Prop. 2017/18:232 s. 198

[9] Ansvaret för överträdelser är strikt. Det krävs alltså varken uppsåt eller oaktsamhet för att sanktionsavgift ska kunna tas ut, se prop. 2017/18:232 s. 481.

för sina anställda med fokus på hantering av personuppgiftsincidenter enligt BDL.

Granskningen omfattar inte innehållet i rutinerna eller utbildningsinsatserna utan är fokuserad på att kontrollera att den granskande myndigheten har rutiner på plats och att den har genomfört utbildningsinsatser för medarbetarna avseende personuppgiftsincidenter. Granskningen omfattar dock om myndighetens rutiner innehåller anvisningar att dokumentera de uppgifter som krävs enligt brottsdataförordningen.

Rutiner för att upptäcka personuppgiftsincidenter

De personuppgifter som behöriga myndigheter hanterar inom ramen för sin brottsbekämpande och brottsutredande verksamhet är i stor utsträckning av känslig och integritetskänslig natur. Verksamhetens karaktär ställer höga krav på de brottsbekämpande myndigheternas förmåga att skydda de registrerades uppgifter genom nödvändiga skyddsåtgärder för att bl.a. förhindra att en incident uppstår.

Skyldigheten att rapportera personuppgiftsincidenter enligt 3 kap. 9 § BDL ska tolkas i ljuset av de generella kraven att vidta lämpliga tekniska och organisatoriska åtgärder, för att säkerställa lämplig säkerhet för personuppgifter, som föreskrivs i 3 kap. 2 och 8 §§. En förmåga att snabbt upptäcka och rapportera en incident är en nyckelfaktor. För att de brottsbekämpande myndigheterna ska kunna leva upp till rapporteringskravet måste de ha interna rutiner och tekniska möjligheter för att upptäcka en incident.

Utifrån verksamhetens behov och med stöd av risk- och sårbarhetsanalyser kan behöriga myndigheter identifiera de områden där det finns en större risk att en incident kan uppstå. Utifrån analyserna kan myndigheterna sedan använda olika instrument för att upptäcka ett säkerhetshot. Dessa kan vara både tekniska och organisatoriska åtgärder. Utgångspunkten är att de vidtagna säkerhetsåtgärderna ska ge tillräckligt skydd och att incidenter inte ska inträffa.

Exempel på tekniska åtgärder är bl.a. intrångsdetektorer som automatiskt analyserar och upptäcker dataintrång och användning av logganalysinstrument för att kunna detektera obehörig åtkomst (loggavvikelser). En ökad insikt om verksamhetens ”normala” nätverks

trafikmönster hjälper till att identifiera sådant som avviker från den normala trafikbilden gentemot exempelvis servrar, applikationer eller datafiler. Organisatoriska åtgärder kan exempelvis vara antagande av interna strategier för dataskydd som avser interna regler, riktlinjer, rutiner och olika typer av styrdokument och policydokument.[10] Riktlinjer och regler för hantering av personuppgifter, rutiner för incidenthantering och logguppföljning[11] utgör exempel på sådana strategier. Periodisk uppföljning av tilldelade behörigheter är ett annat exempel på organisatoriska åtgärder. I en behörig myndighet ska det finnas rutiner för tilldelning, förändring, borttagning och regelbunden kontroll av behörigheter.[12] Information till och utbildning av personal om de regler och rutiner för incidenthantering som ska följas är också exempel på sådana åtgärder.

Datainspektionens bedömning
Ekobrottsmyndigheten har i huvudsak uppgett följande. Myndigheten behandlar personuppgifter i brottsbekämpande syfte främst i verksamhetssystem, programvaror och lagringsytor som tillhandahålls av Polismyndigheten och Åklagarmyndigheten. I Ekobrottsmyndighetens brottsutredande verksamhet används Polismyndighetens verksamhetsstöd Durtvå[13] och i deras åklagarverksamhet används Åklagarmyndighetens verksamhetsstöd Cåbra.[14] Detta innebär att dessa två myndigheter är personuppgiftsbiträden till Ekobrottsmyndigheten. Ekobrottsmyndigheten har i personuppgiftsbiträdesavtal med Åklagarmyndigheten säkerställt att rutiner för att upptäcka incidenter finns på plats. Det har vidare framkommit att biträdesavtalet med Polismyndigheten avseende IT-systemet Durtvå vid tidpunkten för Ekobrottsmyndighetens svar ännu inte var färdigställt.

Vidare har Ekobrottsmyndigheten angett att Åklagarmyndigheten regelbundet utför loggningar i sina system samt att Polismyndighetens IT-miljö kontinuerligt säkerhetsövervakas i syfte att förebygga, upptäcka och förhindra exempelvis it-attacker, driftstörningar och spridning av skadlig kod. Därigenom kan allvarligare personuppgiftsincidenter upptäckas. Om

[10] Brottsdatalag – Delbetänkande av Utredningen om 2016 års dataskyddsdirektiv Stockholm 2017, SOU 2017:29 s. 302
[11] Behöriga myndigheter ska se till att det finns rutiner för logguppföljning, se prop. 2017/18:232 s. 455 f.
[12] 3 kap. 6 § BDL och kompletterande bestämmelser i 3 kap. 6 § BDF
[13] Datoriserad utredningsrutin med tvångsmedelshantering
[14] Centralt system för åklagarväsendets brottmålshantering

det finns anledning till närmare utredning av användaraktiviteter kan loggutdrag användas. Beträffande Ekobrottsmyndighetens egen IT-infrastruktur uppges att den övervakas och loggas regelbundet bl.a. för att personuppgiftsincidenter ska kunna upptäckas. Därutöver har myndigheten en policy för hantering av säkerhetsloggar i IT-system vid Ekobrottsmyndigheten (EBM A-2012/0135). Angående organisatoriska åtgärder har Ekobrottsmyndigheten tagit fram rutiner för behörighetstilldelning gällande Åklagarmyndigheten, och behörigheter följs upp och rensas löpande. Ekobrottsmyndigheten har även genomfört utbildnings- och informationsinsatser om den nya dataskyddsregleringen för sin personal. I dessa har ingått information om personuppgiftsincidenter och om rapporteringsskyldighet. Syftet har varit att medvetandegöra personalen och i och med det öka benägenheten att anmäla incidenter.

Som framgår av utredningen är Polismyndigheten och Åklagarmyndigheten personuppgiftsbiträde till Ekobrottsmyndigheten avseende IT-systemen Durtvå respektive Cåbra. Datainspektionen vill understryka att det åligger Ekobrottsmyndigheten, i egenskap av personuppgiftsansvarige, att försäkra sig att personuppgiftsbiträdena vidtar lämpliga säkerhetsåtgärder för att skydda de personuppgifter som Ekobrottsmyndigheten ansvarar för.

Datainspektionen kan konstatera att Ekobrottsmyndigheten har rutiner för att upptäcka personuppgiftsincidenter på plats.

Skyldigheten att vidta säkerhetsåtgärder för att upptäcka personuppgiftsincidenter är inte knuten till en viss tidpunkt utan åtgärderna ska kontinuerligt ses över och vid behov förändras. För att Ekobrottsmyndigheten ska kunna upprätthålla tillräcklig skyddsnivå av personuppgifter över tid rekommenderar Datainspektionen, med stöd av 5 kap. 6 § BDL, att myndigheten regelbundet utvärderar effektiviteten hos de vidtagna säkerhetsåtgärderna för att upptäcka personuppgiftsincidenter och att myndigheten vid behov uppdaterar dessa.

Rutiner för hantering av personuppgiftsincidenter

För att kunna leva upp till kraven på organisatoriska åtgärder i 3 kap. 8 § BDL ska den personuppgiftsansvarige ha dokumenterade interna rutiner som beskriver vilken process som ska följas när en incident har upptäckts eller inträffat, inbegripet hur incidenten ska begränsas, hanteras och återställas, samt hur riskbedömningen ska gå till och hur incidenten ska anmälas internt

och till Datainspektionen. Av rutinerna ska framgå bl.a. vad en personuppgiftsincident är/kan vara, när en incident behöver anmälas, och till vem, vad som ska dokumenteras, ansvarsfördelningen samt vilken information som bör tillhandahållas inom ramen för anmälan till Datainspektionen.

Datainspektionens kontroll av rutiner för att hantera personuppgiftsincidenter avser tiden från brottsdatalagens ikraftträdande dvs. den 1 augusti 2018.

Datainspektionens bedömning
Ekobrottsmyndigheten har bl.a. uppgett följande. Myndigheten har, sedan ett antal år tillbaka, dokumenterade rutiner för incidenthantering. Vidare har myndigheten uppgett att den under hösten 2018 identifierade ett behov av att tydliggöra vad som gäller för hantering av personuppgiftsincidenter, varför ett arbete med att ta fram riktlinjer för detta påbörjades. Arbetet slutfördes genom att myndigheten den 18 september 2019 beslutade om nya riktlinjer för hantering av personuppgiftsincidenter - EBMR-A 2019:3. Till riktlinjen hör *även Rutin vid förlust av fysisk datamedia samt felskickad e-post, steg för steg* samt *Rutin vid IT-incidenter som omfattar personuppgifter, steg för steg.* Ekobrottsmyndigheten har även lämnat in dokumentation gällande myndighetens tidigare rutiner och om incidentrapporteringssystem (Key Concept), som visar att dessa också omfattade rapportering av personuppgiftsincidenter.

Med beaktande av de inlämnande handlingarna och vad som framkommit i ärendet konstaterar Datainspektionen att Ekobrottsmyndigheten från tidpunkten då brottsdatalagen trädde ikraft har haft och har rutiner för att hantera personuppgiftsincidenter på plats.

Att kunna hantera upptäckta personuppgiftsincidenter på ett korrekt sätt och motverka dess effekter och risker för de registrerades personliga integritet är viktigt. Datainspektionen rekommenderar därför, med stöd av 5 kap. 6 § BDL, att Ekobrottsmyndigheten regelbundet kontrollerar att rutinerna för hantering av personuppgiftsincidenter följs.

Rutiner för dokumentation av personuppgiftsincidenter
En förutsättning för att Datainspektionen ska kunna kontrollera efterlevnaden av dokumentationskravet av incidenter i 3 kap. 14 § BDF är att

dokumentationen omfattar vissa uppgifter som alltid bör ingå. Dokumentationen ska omfatta alla detaljer kring incidenten, inbegripet dess orsaker, vad som skedde och de personuppgifter som berördes. Den ska även innehålla incidentens konsekvenser och de korrigerande åtgärder som den personuppgiftsansvarige vidtagit.

Datainspektionens bedömning
Ekobrottsmyndigheten har huvudsakligen uppgett följande. Myndigheten använder incidenthanteringssystemet Key Concept för intern rapportering av bl.a. personuppgiftsincidenter. Myndighetens dataskyddsombud är mottagare av de interna anmälningarna av incidenter i systemet och är den som avgör om incidenterna ska anmälas till Datainspektionen. En incident som anmäls till Datainspektionen diarieförs även i diarieföringssystemet Cårall. Ekobrottsmyndigheten har tagit fram en riktlinje för hantering av personuppgiftsincidenter samt ett frågeformulär för detta ändamål.

Datainspektionen konstaterar att Ekobrottsmyndigheten har ett IT-system för att bl.a. rapportera incidenter som rör personuppgifter. Därutöver framgår av myndighetens nya riktlinjer för hantering av personuppgiftsincidenter att alla incidenter ska dokumenteras samt vilka uppgifter som dokumentationen ska omfatta. Datainspektionen konstaterar att Ekobrottsmyndighetens rutiner för dokumentation svarar mot kraven i den aktuella bestämmelsen.

Datainspektionen noterar dock att myndigheten i sitt svarsyttrande framfört att det under 2018-2019 har identifierats 15 incidenter internt samt att dokumentationen av dessa i vissa fall har varit bristfällig. Detta kan enligt Datainspektionens mening tyda på att det finns en okunskap hos anställda om vad som ska dokumenteras. Datainspektionen rekommenderar därför, med stöd av 5 kap. 6 § BDL, att Ekobrottsmyndigheten genomför regelbundna kontroller av den interna dokumentationen av personuppgiftsincidenter.

Information och utbildning kring personuppgiftsincidenter

Personalen är en viktig resurs i säkerhetsarbetet. Det räcker inte bara med interna rutiner, regler eller styrdokument om användarna inte följer dem. Alla användare måste förstå att hantering av personuppgifter ska ske på ett rättssäkert sätt samt att det är allvarligare att inte rapportera en incident än

att rapportera t.ex. ett misstag eller ett fel. Det krävs därför att alla användare får en adekvat utbildning och tydlig information om dataskydd.

Den personuppgiftsansvarige ska informera och utbilda sin personal i frågor om dataskydd inbegripet hantering av personuppgiftsincidenter. Av Datainspektionens rapportserie *Anmälda Personuppgiftsincidenter* under perioden 2018-2019 framgår att den mänskliga faktorn utgör den vanligaste orsaken till anmälda personuppgiftsincidenter.[15] Dessa består i huvudsak av individer som, medvetet eller omedvetet, inte följer interna rutiner vid behandling av personuppgifter eller begått ett misstag vid hantering av personuppgifter. Omkring hälften av de incidenter som beror på den mänskliga faktorn handlar om felskickade brev och e-postmeddelanden. Detta understryker enligt Datainspektionens mening betydelsen av att interna rutiner och tekniska säkerhetsåtgärder behöver kompletteras med löpande utbildning, information och andra åtgärder för att öka kunskap och medvetenhet hos medarbetarna.

Datainspektionens bedömning
På frågan om på vilket sätt information och utbildning om incidenter ges till anställda har Ekobrottsmyndigheten uppgett bl.a. följande. Information och utbildning har getts i form av e-utbildning, information på intranät och informationsinsatser i samband med att den nya dataskyddsregleringen trädde ikraft. De nya riktlinjerna för hantering av personuppgiftsincidenter har implementerats och informationsinsatser om detta har genomförts. Rutiner och regler för hantering av e-post och för andra informationsbärare har tagits fram. Därutöver har myndigheten reviderat *Riktlinjen Ekobrottsmyndighetens informationssäkerhet – policy och ansvar* (EBMR-A 2015-3) för att tydliggöra varje medarbetarens ansvar för att rapportera brister och incidenter. I riktlinjen anges vilket ansvar medarbetare och befattningshavare har för myndighetens informationssäkerhet. Vidare har olika vägledande dokument som har bäring på hanteringen av personuppgiftsincidenter tagits fram, t.ex. Ekobrottsmyndighetens vägledning för säker hantering av information. Dessa finns publicerade på myndighetens intranät.

---

[15] Rapport 2019:1, rapport 2019:3 och rapport 2020:2. Liknande slutsatser har MSB dragit i sin årsrapport för allvarliga IT-incidenter, dvs. att de flesta av incidenterna beror på mänskliga misstag, se https://www.msb.se/sv/aktuellt/nyheter/2020/april/arsrapporten-for-allvarliga-it-incidenter-2019-ar-slappt/

Mot bakgrund av vad som framgår av utredningen anser Datainspektionen att Ekobrottsmyndigheten har visat att myndigheten har gett information och utbildning om hantering av personuppgiftsincidenter till sina medarbetare.

För att upprätthålla kompetensen och säkerställa att ny personal får utbildning är det viktigt med återkommande information och utbildning till de anställda och inhyrd personal. Datainspektionen rekommenderar, med stöd av 5 kap. 6 § BDL, att Ekobrottsmyndigheten ger de anställda löpande information och återkommande utbildningar i hanteringen av personuppgiftsincidenter och skyldigheten att rapportera dessa.

Övrigt

Av utredningen i ärendet har det framkommit att det vid tidpunkten för Ekobrottsmyndighetens svar pågick en förhandling med Polismyndigheten i syfte att upprätta ett personuppgiftsbiträdesavtal avseende IT-systemet Durtvå. Förekomsten av ett sådant biträdesavtal omfattas inte av denna tillsyn och därför vidtar Datainspektionen inte någon åtgärd i detta avseende.

Detta beslut har fattats av enhetschefen Charlotte Waller Dahlberg efter föredragning av Maria Angelica Westerberg. Vid den slutliga handläggningen av ärendet har även IT-säkerhetsspecialisten Ulrika Sundling och juristen Jonas Agnvall medverkat.

Charlotte Waller Dahlberg, 2020-12-17 (Det här är en elektronisk signatur)

Kopia för kännedom till:
Ekobrottsmyndighetens dataskyddsombud

Hur man överklagar

Om ni vill överklaga beslutet ska ni skriva till Datainspektionen. Ange i skrivelsen vilket beslut ni överklagar och den ändring som ni begär. Överklagandet ska ha kommit in till Datainspektionen senast tre veckor från den dag beslutet meddelades. Om överklagandet har kommit in i rätt tid sänder Datainspektionen det vidare till Förvaltningsrätten i Stockholm för prövning.

Ni kan e-posta överklagandet till Datainspektionen om det inte innehåller några integritetskänsliga personuppgifter eller uppgifter som kan omfattas av sekretess. Myndighetens kontaktuppgifter framgår av beslutets första sida.