Skatteverket
Enhet 6800
171 94 Solna

Tillsyn enligt brottsdatalagen (2018:1177) – Skatteverkets rutiner för hantering av personuppgiftsincidenter

Innehållsförteckning

Datainspektionens beslut

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

1. Skatteverket 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. Skatteverket bör regelbundet kontrollera att rutinerna för hantering av personuppgiftsincidenter följs.

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

4. Skatteverket 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 Skatteverket 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 incidenter enligt brottsdatalagen. I granskningen ingår även att kontrollera om Skatteverket 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 Skatteverket den 4 december 2019 och följdes upp med begäran om komplettering den 4 mars 2020. Myndighetens svar på tillsynsskrivelsen kom in den 27 januari 2020 och kompletteringen inkom den 25 mars 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 beslutet

Datainspektionens granskning

Datainspektionen har i detta tillsynsärende att ta ställning till om Skatteverket har dokumenterade 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 Skatteverket har genomfört

[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.

informations- och utbildningsinsatser 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
Skatteverket har i huvudsak uppgett följande. De personuppgiftsincidenter som upptäcks och rapporteras bygger på att den enskilde chefen och medarbetaren är observanta och har förmåga och kunskap för att kunna identifiera en misstänkt personuppgiftsincident. Samtliga chefer och medarbetare har ett ansvar att rapportera misstänka personuppgiftsincidenter. Information om vad som kan vara en misstänkt personuppgiftsincident har kommunicerats till samtliga chefer och medarbetare på skattebrottsenheten (SBE). Skatteverket uppger vidare att myndigheten har implementerat organisatoriska och tekniska rutiner såsom logguppföljning och behörighetstilldelning. Vad avser tekniska lösningar anges att de centrala datasystemen för handläggarna på skattebrottsenheten är Skatteverkets brottsutredningsstöd (RIF BU) för den brottsutredande verksamheten (förundersökningsverksamheten) och Skatteverkets underrättelseregister (SKUR) för underrättelseverksamheten. RIF BU är byggt och utformat på ett sådant sätt att det har ett flertal tekniska rutiner för att motverka personuppgiftsincidenter. Angående organisatoriska åtgärder framgår att åtkomsten till information och behörigheter styrs genom användning av olika behörighetskontrollsystem och behörighetskort. Behörighetskontrollsystemet har register över samtliga användare och deras behörigheter och transaktioner mot att systemet kontrolleras löpande mot

[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

registret. Dessutom har Skatteverket under 2018-2019 utbildat och informerat medarbetare och chefer inom skattebrottsenheten i dataskyddsfrågor. Samtliga medarbetare har fått information särskilt om bl.a. hur en personuppgiftsincident ska rapporteras och vilket stöd som finns för att rapportera och bedöma personuppgiftsincidenter.

Datainspektionen kan konstatera att Skatteverket 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 Skatteverket 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

Skatteverket har bl.a. uppgett följande. Myndigheten har rutiner/riktlinjer för att rapportera och hantera upptäckta personuppgiftsincidenter. Den chef eller medarbetare som upptäcker en misstänkt personuppgiftincident inom

SBE ska rapportera detta i Skatteverkets Användarstöd eller IT-portalen via en
e-tjänst. SBE har en egen ingång i Användarstöd och IT-portalen som heter ”Personuppgiftsincident enligt brottsdatalagen (SBE)”. Skatteverket har bl.a. lämnat in *Rutin personuppgiftsincidenter* daterad 2019-05-09 samt *Kompletterande intern rutin på SBE för rapportering av personuppgiftsincidenter* daterad 2019-08-13 som kompletterar den förstnämnda rutinen. Skatteverket anger att myndighetens Rutin personuppgiftsincidenter främst är framtagen för dataskyddsförordningen, men tar även hänsyn till BDL och BDF. Skatteverket uppger vidare att myndigheten i maj 2018 fastställde ett stöd för att identifiera, rapportera, bedöma och hantera personuppgiftsincidenter (Rapport 2018-05-18 Dataskyddsförordningen Hantera Personuppgiftsincidenter). Rapporten avsåg att stödja Skatteverkets verksamhet vid personuppgiftsincidenter enligt dataskyddsförordningen samt att stödja verksamheten vid skattebrottsenheten vid personuppgiftsincidenter enligt brottsdatalagen. Skatteverket antog den 26 november 2018 dokumentet Rutin personuppgiftsincidenter (uppdaterat den 9 maj 2019 respektive den 30 december 2019). Skatteverket uppger att det fanns särskilda rutiner/riktlinjer för hantering av personuppgiftsincidenter och ett digitalt hanteringssystem för rapporterade personuppgiftsincidenter på plats när BDL började gälla den 1 augusti 2018.

Med beaktande av de inlämnande handlingarna och vad som framkommit i ärendet konstaterar Datainspektionen att Skatteverket 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 Skatteverket 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
Skatteverket har huvudsakligen uppgett följande. Det är personuppgiftskoordinatorernas (PU-IK) ansvar att rapporteringarna blir diarieförda, handlagda och dokumenterade. Vidare anges att som stöd för handläggning och dokumentation av rapporterade personuppgiftsincidenter finns ett digitalt hanteringssystem där samtliga vidtagna åtgärder dokumenteras. Det finns även stöddokument för diarieföring av personuppgiftsincidenter. Av myndighetens Rutin personuppgiftsincidenter samt av deras Kompletterande interna rutin på SBE för rapportering av personuppgiftsincidenter framgår att alla personuppgiftsincidenter ska dokumenteras. Av dokumentationen ska framgå omständigheterna kring personuppgiftsincidenten, dess effekter och de åtgärder som vidtagits med anledning av den.

Datainspektionen konstaterar att Skatteverket har ett internt IT-system för att rapportera personuppgiftsincidenter. Därutöver framgår av de inlämnade rutinerna att alla personuppgiftsincidenter ska dokumenteras samt att det har preciserats vilka uppgifter som dokumentation ska omfatta. Datainspektionen konstaterar att Skatteverkets rutiner för dokumentation svarar mot kraven i den aktuella bestämmelsen.

Att kunna dokumentera inträffade personuppgiftsincidenter på ett korrekt sätt och därmed motverka risken av att dokumentationen blir bristfällig eller ofullständig är viktigt. Bristfällig dokumentation kan leda till att incidenterna inte hanteras och åtgärdas på ett korrekt sätt, vilket kan få påverkan på integritetsskyddet. Datainspektionen rekommenderar därför, med stöd av 5 kap. 6 § BDL, att Skatteverket 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. [13] 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 Skatteverket uppgett bl.a. följande. Skatteverket har interna utbildningar i dataskydd för medarbetare och chefer. Skatteverket har utbildat och informerat samtliga medarbetare och chefer inom SBE genom att de under 2018-2019 har genomgått Skatteverkets utbildning i dataskyddsfrågor. Under våren/sommaren 2018 har medarbetarna tagit del av utbildningsfilmer producerade av Ekobrottsmyndigheten om dataskyddsreformen inklusive brottsdatalagen. Dessutom har de fått information om dataskyddsförordningen och brottsdatalagen, särskilt kring rapportering av personuppgiftsincidenter. Sektionschefer har även lämnat information till samtliga medarbetare om att personuppgiftsincidenter ska rapporteras, hur man går tillväga för att rapportera samt vad som kan vara en personuppgiftsincident. Samtliga chefer på SBE har fått information från Skatteverkets dataskyddsombud. Varje chef och medarbetare har genomfört en digital grundkurs om dataskyddsförordningen, som omfattar cirka två timmar självstudier.

---

[13] 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 Skatteverket 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 Skatteverket ger de anställda löpande information och återkommande utbildningar i hanteringen av personuppgiftsincidenter och skyldigheten att rapportera dessa.

Detta beslut har fattats av enhetschefen Charlotte Waller Dahlberg efter föredragning av juristen 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:
Skatteverkets 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.