TIETOSUOJAVALTUUTETUN TOIMISTO

Dnr 7767/183/21

15.11.2021

Bästa personuppgiftsansvarig

Dataombudsmannens byrå har noterat att det inom social- och hälsovårdsbranschen finns behov av preciserande anvisningar om anmälan av personuppgiftsincidenter till myndigheten eller till den person som blivit föremål för personuppgiftsincidenter.

Behovet har framkommit till exempel i Recept-tjänstens begäran om utredning som FPA genomförde. Vi har även fäst uppmärksamhet vid att det förekommer aktörspecifika skillnader i identifieringen och behandlingen av personuppgiftsincidenter.

Vi sänder er[1] detta brev för att utöka vetskapen och förståelsen om personuppgiftsincidenter och de lagstadgade skyldigheterna i anslutning till detta. Syftet med brevet är att instruera de personuppgiftsansvariga inom hälso- och sjukvårdsbranschen för att förenhetliga verksamhetsmodellerna för anmälan om personuppgiftsincidenter.

Den personuppgiftsansvariges skyldighet att anmäla personuppgiftsincidenter

I EU:s allmänna dataskyddsförordning föreskrivs om behandlingen av personuppgiftsincidenter samt anmälningsskyldigheterna i anslutning till det. I vissa situationer har den personuppgiftsansvarige skyldighet att anmäla personuppgiftsincidenter som denne upptäckt till myndigheten samt till de personer som är föremål för personuppgiftsincidenten.

Anmäl personuppgiftsincidenter till myndigheten

Den personuppgiftsansvarige ska anmälan personuppgiftsincidenter som denne upptäcker till myndigheten, dvs. till dataombudsmannens byrå, då personuppgiftsincidenten sannolikt orsakar en risk för personernas rättigheter och friheter. Om det är sannolikt att ingen risk är förknippad med personuppgiftsincidenten behöver ingen anmälan göras till myndigheten. Du kan läsa mer om riskbedömningen nedan i punkten Bedöm den risk som personuppgiftsincidenten orsakar den registrerade.

Anmälan ska göras till myndigheten utan oskäligt dröjsmål och i mån av möjlighet inom 72 timmar från att personuppgiftsincidenten har upptäckts. Om anmälan inte görs inom denna tidsfrist ska den personuppgiftsansvarige till dataombudsmannens byrå lämna en förklaring om orsakerna till anmälans försening.

Den personuppgiftsansvarige kan göra anmälan till dataombudsmannens byrå med en elektronisk blankett på vår webbplats. När anmälan görs med den elektroniska

[1]Brevet har sänts till dataskyddsombud och självständiga yrkesidkare inom social- och hälsovårdsbranschen. Kontaktinformation har erhållits ur dataombudsmannens register över dataskyddsombud samt FPA:s kundregister. Ytterligare information om registret över dataskyddsombud: https://tietosuoja.fi/sv/behandling-av-personuppgifter-om-dataskyddsombud

blanketten skickar dataombudsmannens byrå en kvittens som returmeddelande till anmälaren, varav framgår det datum då anmälan gjordes, ärendets diarienummer och den referens som den personuppgiftsansvarige angett för ärendet. Kvittensen kan exempelvis utnyttjas i den adekvata dokumenteringen av personuppgiftsincidenten. Dessutom underlättar ärendets diarienummer som framgår ur kvittensen eventuella kontakter till dataombudsmannens byrå.

En noggrann ifyllnad av blanketten och bedömning av intrång från fall till fall är viktigt. Om inte all information är tillgänglig kan den personuppgiftsansvarige göra anmälan stegvis. Då lämnar den personuppgiftsansvarige först en preliminär anmälan och senare en kompletterande anmälan. Man kan även ge en uppskattning över antalet personer och personuppgifter som är föremål för personuppgiftsincidenten om man inte känner till det exakta antalet.

Anmäl personuppgiftsincidenter till den registrerade

Om personuppgiftsincidenten sannolikt orsakar en hög risk för de personer som är föremål för incidenten ska den personuppgiftsansvarige anmäla personuppgiftsincidenten även till dem. Anmälan ska göras utan oskäligt dröjsmål.

Beslut om anmälan till personer som blivit föremål för en personuppgiftsincident ska göras så snabbt som möjligt för att de registrerades rätt att få information om personuppgiftsincidenten utan oskäligt dröjsmål inte äventyras. Anmälan om en personuppgiftsincident till de registrerade utan dröjsmål hjälper dem att förbereda sig för eventuella följder som incidenten kan orsaka.

Myndigheten kan också ge den personuppgiftsansvarige en separat föreskrift att anmäla personuppgiftsincidenten till den registrerade.

I vissa situationer kan det vara motiverat att anmälan fördröjs. Till exempel om den registrerade har ett svagt hälsotillstånd kan det vara skäl att fördröja anmälan om personuppgiftsincidenten. Den personuppgiftsansvarige har dock skyldighet att påvisa att en sådan situation föreligger. Du kan läsa mer om ansvarsskyldigheten i punkten Dokumentera personuppgiftsincidenter och påvisa att du iakttar dataskyddslagstiftningen.

Anmälan samt kommunikationen i anslutning till den ska vara tydlig och enkel. Den personuppgiftsansvarige ska informera den registrerade bland annat om arten av personuppgiftsincidenten och dess sannolika följder samt de utförda åtgärderna. Dessutom ska den personuppgiftsansvarige ge kontaktinformation till dataskyddsombudet eller någon annan kontaktperson, av vilken den som blivit föremål för en personuppgiftsincident kan få ytterligare information.

I alla situationer behöver den registrerade inte informeras om en personuppgiftsincident. Om händelsen inte sannolikt orsakar någon hög risk för den som blivit föremål för incidenten, behöver det inte anmälas till denne. Andra situationer där anmälan inte krävs har angetts i artikel 34.3 i dataskyddsförordningen.

Bedöm den risk som personuppgiftsincidenten orsakar den registrerade

Den personuppgiftsansvarige ska bedöma hurdan risk som orsakats av personuppgiftsincidenten åt den person som är föremål för incidenten. Myndigheten fäster särskild uppmärksamhet vid den riskbedömning som den

personuppgiftsansvarige gjort, när den behandlar anmälningar om personuppgiftsincidenter.

Risker kan bedömas på tre nivåer:

1. personuppgiftsincidenten orsakar ingen risk för den registrerade,
2. incidenten orsakar sannolikt en **risk** eller
3. incidenten orsakar sannolikt en **hög risk** för den registrerades rättigheter eller friheter.

Personuppgiftsincidenten kan orsaka den registrerade mångahanda skadliga följder. Sådana kan vara exempelvis hälsomässiga skador, ekonomiska förluster, förlorad konfidentialitet för sekretessbelagda personuppgifter, diskriminering, skadat rykte eller att man blir offer för identitetsstöld eller bedrägeri.

När risken i anslutning till personuppgiftsincidenten bedöms ska man beakta hur allvarlig och sannolik den eventuella följden av personuppgiftsincidenten är. Risken är större ju allvarligare följden är för individens del och ju mer sannolikt det är att den förverkligas. Då personuppgiftsincidenten gäller hälsouppgifter föreligger det sannolikt en hög risk, om inte den personuppgiftsansvarige påvisar att risken har reducerats.

Läs praktiska exempel om personuppgiftsincidenter i bilaga 1 (Exempel på personuppgiftsincidenter inom social- och hälsovården).

Vidta korrigerande åtgärder för att stoppa personuppgiftsincidenten

Den personuppgiftsansvarige ska vidta korrigerande åtgärder för att stoppa personuppgiftsincidenten och för att reducera den skada som orsakas de registrerade.

Det är viktigt att den personuppgiftsansvarige genast vidtar korrigerande åtgärder. Exempel på åtgärder är att permanent ta bort uppgifterna så att de inte är tillgängliga för utomstående, korrigera uppgifternas integritet, utföra tekniska åtgärder för att stoppa eller begränsa incidenten, korrigera sårbarheten i systemen, byta ut lösenord och användarnamn, ändra användningsrättigheter, koppla bort datanät samt uppdatera anvisningar och sekretessförbindelser.

Cybersäkerhetscentret har på sin webbplats sammanställt anvisningar och guider för att genomföra dataskyddet.

Dokumentera personuppgiftsincidenter och påvisa att du iakttar dataskyddslagstiftningen

Den personuppgiftsansvarige ska dokumentera personuppgiftsincidenter. Detta innebär att den personuppgiftsansvarige samlar och sparar bland annat uppgifter om personuppgiftsincidenten (såsom dess karaktär och vilka uppgifter det gäller) som behövs för att uppfylla anmälningsskyldigheten, information om effekterna och följderna av incidenten, en riskbedömning samt beslut i anslutning till vidtagna åtgärder och personuppgiftsincidenten.

Det rekommenderas att dokumenteringen förvaras tillräckligt länge så att man vid behov kan återkomma till uppgifterna. Myndigheten ska med hjälp av dokumenteringen kunna kontrollera att dataskyddsförordningen har iakttagits. Även den registrerade ska genom dokumenteringen kunna få ytterligare information om personuppgiftsincidenten i efterskott.

Dokumentering av personuppgiftsincidenter är en del av den personuppgiftsansvariges ansvarsskyldighet. Ansvarsskyldigheten innebär att den personuppgiftsansvarige ska kunna påvisa att denne iakttar dataskyddslagstiftningen (artikel 5.2 i DSF). Ansvarsskyldigheten gäller både de beslut som den personuppgiftsansvarige har fattat och dennes verksamhet.

Här hittar du ytterligare information

- Läs mer om personuppgiftsincidenter på dataombudsmannens byrås webbplats
- Anvisningar om personuppgiftsincidenter av Europeiska dataskyddsstyrelsen:
  - Riktlinjer om anmälan av personuppgiftsincidenter (pdf)
  - Guidelines 01/2021 on examples regarding data breach notification (pdf)[2]

Biträdande dataombudsmannen _____

Dokumentet har undertecknats elektroniskt. Underskriftens riktighet kan vid behov kontrolleras hos registratorskontoret vid dataombudsmannens byrå.

Kontaktinformation till dataombudsmannens byrå

Postadress: PB 800, 00531 Helsingfors

E-post: tietosuoja@om.fi

Telefonväxel: 029 566 6700

Webbplats: www.tietosuoja.fi

[2]Ifrågavarande version av anvisningen har genomgått offentligt hörande inom Europeiska dataskyddsstyrelsen, men anvisningen är inte ännu godkänd.

Bilaga 1: Exempel på personuppgiftsincidenter inom social- och hälsovården

En personuppgiftsincident är en händelse som leder till att personuppgifter förstörs, försvinner, ändras, olovligt lämnas ut eller att någon aktör som inte har rätt att behandla uppgifterna får tag på dem.

Nedan finns exempel sammanställda som stöd för anmälan om personuppgiftsincidenter.

Exemplen är allmänna, och beaktar inte fallspecifika särdrag. Den personuppgiftsansvarige ska därför alltid bedöma ifrågavarande personuppgiftsincident och tröskeln för anmälan från fall till fall.

Exempel	Risk-tröskel	Anmäl till myndigheten	Anmäl till den registrerade	Anmärkningar / rekommendationer
Arbetstagaren har per e-post eller brev skickat en klients/patients hälsoinformation till en felaktig adress (exempelvis plan för missbruksrehabilitering eller intyg för sjukledighet). Informationen har kommit i en utomståendes händer.	Hög risk	✓	✓	En oskyddad e-post ska inte användas för att kommunicera sekretessbelagd information.
På ett möte hade ljudenhetens högtalare vid Bluetooth varit i kontakt med enheterna i rummet bredvid. Detta ledde till att en utomstående hörde samtalet. På mötet behandlades klientens/patientens information. Det är inte	Hög risk	✓	✓	I anvisningar till personalen kan man exempelvis beakta att Bluetooth inte används när mötesenheter kopplas.

känt hur länge den utomstående var del av samtalet.				
Sjukhusets patientuppgifter är otillgängliga i 30 timmar på grund av en nätattack.	Hög risk	✓	✓	Den personuppgiftsansvarige ska ha förmåga att snabbt göra uppgifterna tillgängliga igen när ett fysiskt eller tekniskt fel inträffar.
Den personuppgiftsansvarige har i samband med driftövervakning observerat att enhetens arbetstagare i egenskap av utomstående har behandlat (m.a.o. snokat) en enskild patients/klients uppgifter i eget syfte.	Hög risk	✓	✓	
Arbetstagaren har laddat upp ett foto i sociala medier där även en viss patients uppgifter syns. Med ett bildhanteringsprogram kan patientens uppgifter preciseras, även om bilden är oskarp. Det är inte känt om någon utomstående har laddat ner bilden.	Hög risk	✓	✓	Informationen om den person som är föremål för incidenten ska dokumenteras innan bilden förstörs för genomförande av anmälningsskyldigheten.
En arbetstagare har på parkeringsplatsen tappat bort en klientlista som innehåller information om klienters hälsotillstånd. Arbetstagaren märkte misstaget, men hittade inte listan. Det är inte känt om klientlistan har kommit utomståendes händer.	Hög risk	✓	✓	
En del av patientinformationen som fanns i systemet förstördes slutgiltigt på grund av ett mänskligt misstag. Någon säkerhetskopia fanns inte, och informationen kan inte återbördas.	Hög risk	✓	✓	
En klient (person A) som kom från läkarens mottagning meddelade i receptionen att hen hade fått en	Hög risk	✓	✓	

sjukdagpenningblankett som tillhörde en annan person (person B).				
I specifikationen till en faktura från företagshälsovården hade orsaken till arbetstagarens besök angetts, vilket i onödan avslöjade uppgifter om hälsotillstånd. Arbetsgivarens representant mottog fakturan.	Hög risk	✓	✓	
En arbetstagare vid hemvården hade i misstag lämnat en blankett med en annan klients (B) uppgifter i en klients (A) hem. Klientens (A) anhöriga hade hittat informationen bland sin anhörigas papper.	Hög risk	✓	✓	
En yrkesperson inom hälso- och sjukvården antecknade i misstag informationen om patient A:s medicinallergi i patient B:s uppgifter. I patient A:s uppgifter antecknades alltså inga allergiuppgifter alls. Patient B har inga allergier. En annan yrkesperson inom hälso- och sjukvården (omedveten om A:s allergi) ger i sjukvården till patient A den medicin som A är allergisk mot. A orsakas hälsomässig skada.	Hög risk	✓	✓	Någon anmälan om personuppgiftsincident behöver inte nödvändigtvis göras åt patient B, om någon hög risk inte har uppstått för hen.
Misstanke har väckts om att person A har uppträtt som person B (identitetsstöld), gjort en tidsbokning i dennes namn och kommit till läkarens mottagning. Läkaren har vårdat klienten med de angivna personuppgifterna och har gjort en anteckning i B:s patientuppgifter. Person B har själv tagit kontakt med den personuppgiftsansvarige	Hög risk	✓	✓	Det är skäl att försäkra sig om patientens identitet i samband med varje kontakt.

när hen noterade anteckningar på Mina Kanta-sidor som inte var hens. Den personuppgiftsansvarige raderade de felaktiga uppgifterna ur B:s uppgifter.				
På grund av ett systemfel hade patientens (A) remiss till en åtgärd för ett ögonblick lagrats i fel patients (B) uppgifter. Felet var lokalt och den felaktiga uppgiften överfördes inte till Kanta. Laboratoriet som tog emot remissen var medvetet om felet. Felet samt uppgifternas integritet korrigerades snabbt. Patienten orsakades ingen skada.	Risk	✓		Om patient A inte hade fått komma till åtgärden hade det kunnat vara fråga om en hög risk.
En städare tömde ovarsamt bäddavdelningens sopkärl i fel kärl som den personuppgiftsansvarige innehade. Personalen på avdelningen använde sopkärlet för förvaring av patientpapper som skulle förstöras. Den personuppgiftsansvarige hade inte vetskap om vilka patienters information det var fråga om. Den personuppgiftsansvarige försäkrade sig i samarbete med avfallshanteringen om att uppgifterna förstördes och att informationen inte kom i utomståendes händer.	Risk	✓		Den personuppgiftsansvarige ska i sina processer beakta att patientuppgifter inte ska förvaras i öppna sopkärl, utan de ska förvaras endast i låsta kärl.
En verksamhetsenhet inom hälso- och sjukvården (A) skickade information om ett flertal patienters operativa vård till en annan verksamhetsenhet inom hälso- och sjukvården (B). Syftet med sändningen av informationen var	Risk	✓		

vetenskaplig forskning. Inget avtal var ännu upprättat mellan enheterna, och av patienterna hade man inte skaffat samtycke för deltagande i forskning. Uppgifterna som skickades innehöll inga direkta identifikationsuppgifter, men det var möjligt att identifiera en del av patienterna genom kombination och slutledning utifrån uppgifterna. Uppgifterna nådde endast yrkespersoner inom hälso- och sjukvården som utförde forskningen och som har sekretesskyldighet. Mottagaren förstörde uppgifterna.				
Från ett apotek levererades en beställning innehållande flera patienters mediciner som var avsedd för organisation A till organisation B. Apoteket samarbetar med båda organisationerna. Medicinerna kunde levereras i tid till de rätta patienterna.	Risk	✓		
Till en pålitlig/säker mottagare, som man har en samarbetsrelation till, har fördelats patientuppgifter inom samma avdelning. Mottagaren har en lagstadgad sekretesskyldighet och behandlar informationen i fråga i sina arbetsuppgifter. I situationen finns det ingen orsak att misstänka att uppgifterna har använts eller kommer att behandlas i strid med lagstiftning eller den personuppgiftsansvariges anvisningar.	Ingen risk			De som deltar i vården av en patient eller uppgifter i anslutning till den får behandla patienthandlingar endast i den utsträckning som deras arbetsuppgifter eller ansvar det kräver.

Den personuppgiftsansvariges arbetstagare skickar personuppgifter i en oskyddad e-post. Det finns ingen anledning att misstänka att uppgifterna har kommit utomståendes händer.	Ingen risk			En oskyddad e-post ska inte användas för att kommunicera sekretessbelagd information.
På grund av en systemfunktion har huvudanvändaren haft möjlighet att höja sin användningsrättsnivå till för omfattande, varvid hen skulle ha fått tillgång till onödig information med tanke på sina uppgifter. Den personuppgiftsansvarige kunde genom tekniska åtgärder säkerställa att huvudanvändaren inte höjde sin användningsrättsnivå.	Ingen risk			I patientdatasystem ska det finnas ett system för hantering av användningsrättigheter, med hjälp av vilken användningsrättigheter i enlighet med uppgifterna kan definieras för användare.
Den personuppgiftsansvarige har sparat en hemlig säkerhetskopia av ett arkiv som innehåller klientuppgifter på ett USB-minne. Minnesstickan stjäls i samband med ett inbrott i lokalerna. Informationen är krypterad med en algoritm enligt den senaste tekniken, det finns säkerhetskopior av informationen, den individuella krypteringsnyckeln äventyras inte och informationen kan återbördas i tid.	Ingen risk			
Ett textmeddelande om en tidsbokning hade gått till fel telefonnummer. Meddelandet innehöll inga identifierbara personuppgifter och inte heller hälsoinformation.	Ingen risk			
En arbetstagare vid ett apotek gav kund B ett dokument där kunden A:s namn och	Ingen risk			

personbeteckning kunde ses. Kunden märkte genast det skedda och gav genast tillbaka dokumentet till apotekets arbetstagare.				
Patient A meddelade till hälso- och sjukvården att patientinformation om en annan person (B) hade skrivits in i hens (A) patientinformation. A kan inte på basis av de antecknade uppgifterna sluta sig till vem B är. När saken bekräftades raderades B:s uppgifter ur A:s patientinformation och uppgifterna antecknades i B:s egen patientinformation. Man hann inte göra några avgöranden i anslutning till A:s vård på basis av informationen som gällde person B, och det skedda hade ingen inverkan på B:s vård.	Ingen risk			Man måste se till att man inte i kommunikationen med A avslöjar vem B är. Om A kan identifiera B direkt eller genom att kombinera annan information är risken sannolikt hög, och anmälan till B ska göras. Om man har hunnit göra avgöranden gällande vården för någondera patienten på basis av felaktig information är risken sannolikt hög för denne patients del.