Eljárásrend

adatvédelmi incidensek kezelésére

EESZT-hez csatlakozott egészségügyi szolgáltatók részére

EESZT
Elektronikus
Egészségügyi
Szolgáltatási Tér

ORSZÁGOS
KÓRHÁZI
FŐIGAZGATÓSÁG

Tartalom

I. Eljárásrend kialakításának szükségessége

Az Elektronikus Egészségügyi Szolgáltatás Tér (a továbbiakban: EESZT, Tér) rendszerrel kapcsolatban az adatkezelő jogszabály alapján az Országos Kórházi Főigazgatóság (a továbbiakban: OKFŐ), azonban saját adatkezelésük vonatkozásában a csatlakozott adatkezelők mint egészségügyi szolgáltatók szintén önálló adatkezelőnek minősülnek. Az OKFŐ adatkezelőként való megjelölése az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény (Eüak.) 38. § (3) bekezdés c) pontjában kapott felhatalmazás alapján, az Országos Kórházi Főigazgatóság feladatairól szóló 516/2020. (XI. 25.) Korm. rendelet 7. § (4)-(6) bekezdésein alapul, amelyek az EESZT működtetőjeként, az EESZT-hez kapcsolódó önrendelkezési nyilvántartás vezetőjeként és az EESZT-ben használt kapcsolati kódot kezelő szervként az Országos Kórházi Főigazgatóságot jelölte ki.

Az EESZT az egészségügyi ágazatban hatékony és biztonságos információáramlást valósít meg, így az EESZT önállóan és az egészségügyi ellátóhálózat informatikai rendszereihez csatlakozva tölti be központi szerepét. Az EESZT-be történő adatszolgáltatást az EESZT-hez csatlakozott egészségügyi szolgáltató adatkezelők végzik. A csatlakozott adatkezelő fogalmát az Elektronikus Egészségügyi Szolgáltatási Térrel kapcsolatos részletes szabályokról szóló 39/2016. (XII. 21.) EMMI rendelet (a továbbiakban: EESZT rendelet) 1. § 2. pontja tartalmazza, e szerint csatlakozott adatkezelő az Eüak. 35/B. § (1) és (2) bekezdésében meghatározott, a csatlakozást informatikai rendszer útján megvalósító adatkezelő. Az adatküldés az általuk használt medikai rendszerek EESZT-hez való integrált működésével történik. Az EESZT-ben tárolt adatok **tehát meglévő adatok továbbításával kerülnek a Térbe, így azok tartalmáért az adatszolgáltatást végző egészségügyi szolgáltató tartozik felelősséggel. Ily módon az egészségügyi szolgáltatók az EESZT működésétől függetlenül adatkezelőnek minősülnek az egészségügyi szolgáltatás nyújtása során az egészségügyi intézményben keletkező betegadatok tekintetében.**

Az OKFŐ és az egészségügyi szolgáltatók önálló adatkezelőként történő minősítése alapjaiban határozza meg az adatvédelemmel kapcsolatos jogszabályi kötelezettségek betartásáért való felelősség rendszerét – többek között – az adatvédelmi incidensek kezelése területén.

Jelen eljárásrend célja, hogy az egészségügyi szolgáltatók részére megfelelő eszközként szolgáljon az adatvédelmi incidensek azonosításában, vizsgálatában, majd szükség esetén a Nemzeti Adatvédelmi Információszabadság Hatóság (a továbbiakban: NAIH, Hatóság, felügyeleti hatóság) részére történő bejelentésében és az érintettek tájékoztatásában is.

Tekintettel az EESZT központi szerepére, az EESZT működtetője kiemelt figyelmet fordít az érintett egészségügyi szolgáltatókkal való együttműködésre az adatvédelmi incidensek észlelése, kivizsgálása és bejelentése tekintetében. Ennek megfelelően olyan hatékony eljárásrend került kialakításra, amely ösztönzi az egészségügyi szolgáltatókat az incidensgyanúk megfelelő kivizsgálására és incidensbejelentési kötelezettségének teljesítésére.

II. Adatvédelmi incidens fogalma

A GDPR 4. cikk 12. pontja alapján az adatvédelmi incidens a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, módosítását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi. Az adatvédelmi incidens egyfajta biztonsági incidens, amikor a személyes adatok biztonsága sérül. A különbség a biztonsági incidens és az adatvédelmi incidens között, hogy lényegét tekintve minden adatvédelmi incidens biztonsági incidens, azonban nem feltétlenül minősül mindegyik biztonsági incidens adatvédelmi incidensnek, tekintettel arra, hogy a biztonsági incidens nem kizárólag személyes adatokra korlátozódik. Nem minősül például adatvédelmi incidensnek, ha a személyes adatok tervezett rendszerkarbantartás miatt nem hozzáférhetők.

Az adatvédelmi incidens egyes fogalmi elemeinek részletezése:

Személyes adatnak minősül a GDPR 4. cikk 1. pontja értelmében az azonosított vagy azonosítható természetes személyre („érintett”) vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható. Személyes adat tehát például bármely természetes személyazonosító adat, TAJ-szám vagy más azonosító szám, bármely egészségügyi adat vagy ellátáshoz kapcsolódó adat, amely természetes személyhez köthető, vagy abból a személy kilétére következtetni lehet.

A személyes adatok „*megsemmisítése*” alatt értendő az az eset, amikor az adatok egyáltalán nem, vagy az adatkezelő számára nem használható formában léteznek. A „*károsodás*” az az eset, amikor a személyes adatok módosultak, sérültek, vagy már nem hiánytalanok. A személyes adatok „*elvesztése*” úgy értelmezendő, hogy az adatok még léteznek, de az adatkezelő már nem rendelkezik felettük, nem fér hozzájuk, vagy azok nincsenek a birtokában. Végezetül pedig *jogosulatlan vagy jogellenes* adatkezelésnek minősülhet a személyes adatok közlése vagy *hozzáférhetővé tétele* arra jogosulatlan címzettek számára, illetve bármilyen egyéb, az általános adatvédelmi rendeletbe ütköző adatkezelés.

Fontos azonban hangsúlyozni, hogy egy adatkör téves rögzítése önmagában nem feltétlenül minősül adatvédelmi incidensnek, hiszen az adatok téves rögzítéséből fakadó jogosulatlan adat megismerés kizárólag akkor minősül adatvédelmi incidensnek, ha az adatokat megismerő személy olyan adatokat ismer meg, - téves rögzítésből adódóan- amely adatok alapján más személyt azonosítani tud. Tehát az adatvédelmi incidens - a fentebb hivatkozott GDPR 4. cikk 12. pontja értelmében – személyes adatokat érint és egy információ akkor minősül személyes adatnak, ha a GDPR 4. cikk 1. pontja szerinti fogalmi elemek – így a személy azonosíthatósága is – megvalósulnak. Ellenkező esetben az esemény nem minősül adatvédelmi incidensnek. Erre jó példaként szolgálhat az az eset, amikor az ellátáson részt nem vett személy egy olyan beutalót, vagy eReceptet lát a felületén, amelyen – tévesen – a saját adatai szerepelnek, emellett azonban pusztán olyan információk, mint egy gyógyszer neve, vagy az intézmény neve, ahová a beutaló szól, akkor az eset egyértelműen nem adatvédelmi incidens, mivel nem tudja azonosítani, hogy a gyógyszer kinek lett felírva, ki lett beutalva az adott intézménybe. Ugyanezen megítélés alá esik azon eset, ha tévesen egy olyan EHR dokumentum lett feltöltve, amely az ellátás adatait tartalmazza; a panaszokat, diagnózist, alkalmazott kezelést – ebben az esetben sem tudja megállapítani a személy, hogy kinek a panaszait, kinek a diagnózisát, kinek a részére előírt kezelésre vonatkozó adatait látja.

Az itt ismertetett esetekkel szemben azonban előfordulnak olyan esetek is, amikor a feltöltött dokumentumon szerepel, hogy kihez tartozik, ilyen eset lehet pl. egy orvosi lelet. Ha a feltöltött leleten szerepel az ellátáson részt vett személy neve és egyéb adatai, akkor a téves feltöltés adatvédelmi incidenst valósít meg, melyet ez esetben – a kockázatot mérlegelve – az adatkezelőnek be kell jelentenie a Hatóságnak.

Az EESZT-t érintő néhány gyakorlati eset szemléltetését az *1. sz. mellékletben* található tájékoztató tartalmazza.

III. Felelősségi körök elhatárolása az EESZT-t érintő adatvédelmi incidensek tekintetében

Az egészségügyről szóló 1997. évi CLIV. törvény 136. §-a az EESZT működésétől teljesen függetlenül előírja az egészségügyi szolgáltatók számára az egészségügyi dokumentáció vezetésének kötelezettségét. Ezen adatok az ellátást végző egészségügyi szolgáltató saját rendszerében kerülnek tárolásra az EESZT-től teljesen függetlenül, törvény által előírt ideig pedig megőrzésre kerülnek az egészségügyi szolgáltató által – **az egészségügyi szolgáltató tehát a nála keletkezett adatok tekintetében önálló adatkezelőnek minősül**.

Ezek az egészségügyi szolgáltatónál eleve meglévő adatok és dokumentumok kerülnek a jogszabály által meghatározott körben feltöltésre az EESZT-be, tehát csupán az EESZT-be történő adatfeltöltési kötelezettség miatt nem szükséges többlet adatot igényelni a pácienstől. **Az OKFŐ mint az EESZT működtetője a Térben tárolt adatok vonatkozásában szintén önálló adatkezelőnek minősül.**

Tekintettel arra, hogy az OKFŐ és az egészségügyi szolgáltatók egyaránt önálló adatkezelők, így az adatvédelmi incidensekkel kapcsolatos felelősségek az alábbiak szerint különíthetőek el egyértelműen egymástól.

1. Az adatot rögzítő egészségügyi szolgáltató felelőssége

Mivel az EESZT-be kerülő adatok a csatlakozott egészségügyi szolgáltatók informatikai rendszeréből kerülnek továbbításra az EESZT-be, **az adatvédelmi incidensek kivizsgálása elsődlegesen az adatot feltöltő egészségügyi szolgáltató feladata**.

A gyakorlatban megvalósuló **legtipikusabb eset**, amikor az állampolgár mint érintett által az EESZT felé bejelentett incidensgyanús eset nem az EESZT működésében bekövetkezett zavar következtében áll elő, hanem az adatok feltöltését végző **egészségügyi intézmény** EESZT kompatibilis medikai programjában történő **téves adatrögzítése** miatt (tipikusan például a beteg TAJ-számának elütése miatt) alakul ki.

A fentiek alapján az EESZT-ben tárolt adatok meglévő adatok továbbításával kerülnek a Térbe, így azok tartalmáért az adatszolgáltatást végző egészségügyi szolgáltató tartozik felelősséggel. Ilyen esetekben **az egészségügyi szolgáltató feladata annak teljeskörű kivizsgálása**, hogy a téves rögzítésből fakadóan az ellátásban ténylegesen részt vett személy megismer-e olyan adatokat, amelyek nem rá vonatkoznak, azaz ebben a vonatkozásban bekövetkezik-e adatvédelmi incidens. E vizsgálat teljeskörűsége érdekében kérjük az egészségügyi szolgáltatóktól a **teljes ellátási esemény kivizsgálását**: ha a bejelentés például csak eRecepttel volt kapcsolatos, abban az esetben is terjedjen ki a vizsgálat a további tényezőre, hogy az ellátási esemény során keletkezett-e többi (pl.: EHR

dokumentum, eKat bejegyzés, eBeutaló, stb...) bejegyzés, és hogy ezen események között megismerhetővé váltak-e személyes adatok a bejelentő részére.

Az EESZT-nek továbbá nincs rálátása, sem hatásköre arra vonatkozóan, hogy az ellátásban ténylegesen részt vett személy az ellátás során kapott-e és ha igen, milyen típusú dokumentumot kapott kézhez, továbbá, hogy e dokumentum személyes adatokat tartalmaz-e, és ha igen kinek és milyen személyes adatait tartalmazza. Az előzőek alapján az OKFŐ felelősségét kizárja különösen a felírási igazolások kiadása kapcsán mind papír alapú, mind elektronikus felírási igazolások vonatkozásában.

A hibás adatrögzítésből eredő, például jogosulatlan adatmegismerés esetén az adatot rögzítő egészségügyi szolgáltató felelős, így adatkezelőként az ő felelőssége a GDPR által meghatározott adatvédelmi incidensekkel kapcsolatos kötelezettségek teljesítése. Az adatvédelmi incidens kivizsgálása, elhárítása és – adott esetben – a felügyeleti hatósághoz történő bejelentése ilyen esetben tehát az egészségügyi szolgáltató mint adatkezelő feladata.

Az adatvédelmi incidens elhárítása érdekében a rendszerbe hibásan felvett adatok törlésére és módosítására minden esetben az az egészségügyi szolgáltató jogosult és köteles, amely az adatot számítógépes rendszerébe hibásan rögzítette. Az EESZT együttműködési hatáskörében eljárva ilyenkor csak átirányítani képes a hibát az egészségügyi szolgáltatókhoz, a hibát az EESZT sem törölni, sem módosítani nem jogosult.

Az adatot rögzítő **egészségügyi szolgáltató felelős mindazon adatvédelmi incidensért** is, amely saját érdekkörében (felelősségi körében) merül fel, így ezek **kivizsgálása és elhárítása** körében az egészségügyi szolgáltató köteles megtenni a IV. pontban ismertetett szükséges lépéseket.

2. OKFŐ mint az EESZT működtetőjének felelőssége

Felmerülhet olyan adatvédelmi incidens is, amely az **EESZT nem üzemszerű működése** folytán következik be, amely esetben az **OKFŐ felelőssége** kerül megállapításra. Amennyiben a IV. pontban meghatározott eljárás eredményeként az egészségügyi szolgáltató alappal feltételezi az EESZT hibás működéséből fakadó adatvédelmi incidens megtörténtét, az erre utaló körülmények részletes leírásával **haladéktalanul értesíteni köteles** az EESZT üzemeltetést, amelyet követően az OKFŐ mint adatkezelő megteszi a GDPR által előírt szükséges lépéseket.

Az OKFŐ tehát kizárólag abban az esetben végzi el az adatvédelmi incidens kivizsgálását, amennyiben az az EESZT rendszer működése kapcsán keletkezett hibából fakad.

Összefoglalva *tehát mind az OKFŐ, mind az egészségügyi szolgáltatók önálló adatkezelőnek minősülnek. Ennél fogva a GDPR által az adatvédelmi incidensek esetére előírt kötelezettségeket és felelősséget az az adatkezelő köteles viselni, amelynek hibájából az adatvédelmi incidens bekövetkezett.*

IV. Az egészségügyi szolgáltatók EESZT-t érintő adatvédelmi incidensgyanú esetén követendő eljárásrendje

A következőkben áttekintést adunk az egészségügyi szolgáltató teendőiről, amennyiben adatvédelmi incidens gyanús eseményt észlel.

1. Az adatvédelmi incidens észlelése, a felelős adatkezelő kilétének megállapítása

Az adatvédelmi incidens beazonosításához szükséges első lépés az **incidens vagy incidens gyanú észlelése** (maga észleli vagy egyéb szerv tájékoztatja róla). Ezt követően a szolgáltató minden esetben köteles **megvizsgálni, hogy az adatvédelmi incidens saját, vagy az OKFŐ érdekkörében (felelősségi körében) merült-e fel**. E kérdés eldöntéséhez az alábbi szempontok mérlegelése szükséges:

1.1 A GDPR fogalomrendszerében az adatvédelmi incidens megvalósulásának feltétele a biztonság sérülése, így először az egészségügyi szolgáltatónak azt kell vizsgálnia, hogy saját érdekkörében merült-e fel az incidens (pl. téves adatrögzítés) illetve az általa alkalmazott egészségügyi szoftverrel kapcsolatban áll-e fenn hiba, avagy ezek hiányában feltételezi, hogy az EESZT működéséből fakadó hiba történhetett, vagyis, hogy az EESZT rendeltetésszerűen működött-e.

A kérdés vizsgálata azért kulcsfontosságú, mert például egy téves rögzítés esetében az EESZT működtetője nincs abban a helyzetben, hogy megállapítsa, valóban téves adatrögzítés történt-e, vagy hogy a beteg valóban nem járt a rendelésen, továbbá az adatok orvosszakmai szempontú vizsgálatára sem rendelkezik hatáskörrel - ezzel összefüggésben az OKFŐ tehát nem tudja vizsgálni az adatvédelmi incidens megvalósulását, illetve megállapítani annak kockázati mértékét. Emellett nem tud technikai védelmi és szervezési intézkedést sem végrehajtani az incidens haladéktalan megállapítása, sem az érintettek sürgős értesítése érdekében. Az OKFŐ csupán arra rendelkezik hatáskörrel, hogy a hozzá bejelentett feltételezett incidensről indokolatlan késedelem nélkül értesítse az egészségügyi szolgáltatót mint adatkezelőt, a szükséges további lépéseket az egészségügyi szolgáltatónak szükséges megtennie.

Ez a gyakorlatban a következőket jelenti:

– **Az adatvédelmi incidens észlelése**

Az adatvédelmi incidensről, vagy az incidens gyanújáról való értesülés többféleképpen is megtörténhet: az egészségügyi szolgáltató **maga észleli** az incidenst (például az betegellátó személy munkavégzés közben észleli az incidenst), vagy **az adatfeldolgozó, az érintett, harmadik személy, az OKFŐ, esetleg a Hatóság jelenti** az incidenst az egészségügyi szolgáltatónak**.**

A kialakult gyakorlatban gyakran előforduló eset, hogy az érintett személy EESZT-ben szereplő hibás adataival kapcsolatos tájékoztatást az OKFŐ-től kéri. Az OKFŐ ilyen esetben **továbbítja az adatvédelmi incidens gyanúját az érintett adatot rögzítő egészségügyi szolgáltató felé**, tekintettel arra, hogy a kérdéses adat az egészségügyi szolgáltatónál keletkezett. Az OKFŐ ilyen esetekben nem végzi el az esemény vizsgálatát, majd

értékelését, hiszen a IV. pontban írtak alapján az értékelésre, valamint a **szükséges lépések megtételére az érintett szolgáltató köteles.**

– **Vezető értesítése**

Bármelyik esetről is legyen szó, fontos, hogy incidens észlelését követően azonnal értesíteni kell a megfelelő vezetési szinten lévő személyt (például kórházak esetében az intézmény vezetőjét, magánszolgáltatók esetében a vezető tisztségviselőt valamint az adatvédelmi tisztviselőt), hogy az incidenst kezelni és szükség szerint jelenteni lehessen a NAIH, illetve az érintettek részére.

– **Az incidens körülményeinek kivizsgálása, az incidens megállapítása**

Ezt követően az egészségügyi szolgáltatónak ki kell vizsgálnia az incidens körülményeit. Amikor az adatkezelő először értesül esetleges adatvédelmi incidensről, vagy saját maga észlel adatvédelmi vagy biztonsági incidenst, rövid vizsgálatot folytat annak megállapítása érdekében, hogy valóban érintettek-e személyes adatok és hogy az adott esemény az adatvédelmi incidens kategóriába esik-e (lásd III. 1. pontban írtaknál). *E vizsgálat ideje alatt nem tekinthető úgy, hogy az adatkezelő „tudomására" jutott az adatvédelmi incidens.* Ugyanakkor az első vizsgálatot minél előbb meg kell kezdeni, és észszerű bizonyossággal meg kell állapítani, hogy történt-e incidens.

1.2 Amennyiben az egészségügyi szolgáltató az adatvédelmi incidens gyanú kivizsgálásakor azt észleli, hogy az adatvédelmi incidens az általa használt medikai rendszer hibájából fakad, haladéktalanul értesíti a medikai rendszer szállítóját, amely kivizsgálja az esetet.

Amennyiben az egészségügyi szolgáltató az adatvédelmi incidens gyanú kivizsgálásakor azt észleli, hogy az adatvédelmi incidens nem az egészségügyi szolgáltatónál és nem is a medikai rendszer miatt keletkezett, hanem az EESZT nem üzemszerű működéséből fakad, az erre utaló körülmények részletes leírásával haladéktalanul értesíti OKFŐ-t az adatvedelem.eeszt@okfo.gov.hu e-mail címen keresztül. Ebben az esetben az eljárás az OKFŐ általi kivizsgálással folytatódik.

1.3 Amennyiben megállapítást nyert, hogy az incidens az egészségügyi szolgáltató érdekkörében keletkezett, az egészségügyi szolgáltatónak, mint adatkezelőnek meg kell bizonyosodnia arról, hogy az összes megfelelő technológiai védelmi és szervezési intézkedés végrehajtásra került-e, egyrészt az adatvédelmi incidens haladéktalan megállapítása, másrészt a felügyeleti hatóságnak történő bejelentés, illetve szükség esetén az érintett sürgős értesítése érdekében.

Azt, hogy az **értesítésre indokolatlan késedelem nélkül került-e sor**, különösen az adatvédelmi incidens jellegének és súlyosságának felmérése, valamint az adatvédelmi incidens érintettre gyakorolt következményeinek, illetve hátrányos hatásainak felmérése útján lehet megállapítani.

2. A kockázatok felmérése

Az incidens megállapítását követően fel kell mérni az incidens következtében az egyéneket érintő kockázatokat és egyúttal tájékoztatni kell a szervezet érintett részlegeit (amennyiben van ilyen). A

kockázat felmérésének két lényeges oka van: az egyénekre gyakorolt hatás valószínűségének és lehetséges súlyosságának ismeretében az adatkezelő egyrészről könnyebben tud hatékony intézkedéseket hozni az incidens elhárítására és kezelésére, másrészt gördülékenyebben meg tudja állapítani, hogy kell-e a NAIH részére bejelentést tenni, és az érintett egyéneket értesíteni. A kockázat felmérés eredményeként az adatkezelő képes annak megállapítására, hogy *az incidens valószínűsíthetően kockázattal jár-e az egyének jogaira és szabadságaira nézve*, ugyanis ilyen esetben a Hatóság részére jelenteni kell az incidenst. Az érintettek incidensről való tájékoztatása pedig akkor válik szükségessé, *ha az incidens valószínűsíthetően magas kockázattal jár az egyének jogaira és szabadságaira nézve*. Ilyen kockázat akkor merül fel, ha az incidens fizikai, vagyoni vagy nem vagyoni károkat okozhatnak azoknak az érintetteknek, akiknek adatait az incidens érinti. E károk közé tartozik például a hátrányos megkülönböztetés, a személyazonosság-lopás vagy a személyazonossággal való visszaélés, a pénzügyi veszteség és a jó hírnév sérelme. Amennyiben az incidens különleges adatokra, többek között genetikai adatokra, egészségügyi adatokra is kiterjed, akkor az ilyen károk valószínűleg bekövetkeznek. A kockázat felmérésekor az érintett jogait és szabadságait érintő kockázat valószínűségét és súlyosságát kell meghatározni, mivel egy tényleges adatvédelmi incidens esetén már bekövetkezett az esemény, így teljes mértékben az incidens egyénekre gyakorolt hatásából eredő kockázat felmérésére kerül a hangsúly. A kockázatok felmérése az adatkezelés jellegének, hatókörének, körülményeinek és céljainak függvényében történik. A felmérés eredményeként a kockázatot olyan objektív értékelés alapján kell felmérni, amelynek során megállapíthatóvá válik az, hogy az adatkezelési műveletek i) kockázattal, illetve ii) nagy kockázattal járnak-e.

Az értékelés során ajánlott megvizsgálni az alábbi szempontokat:

2.1. Az incidens jellege: A megtörtént incidens jellege befolyásolhatja az egyéneket érintő kockázat mértékét.

2.2 A személyes adatok jellege, érzékenysége és mennyisége: Általánosságban elmondható, hogy minél érzékenyebbek az érintettek személyes adatok, annál nagyobb a kár bekövetkeztének kockázata. Ugyanakkor figyelembe kell venni az érintettről rendelkezésre álló további személyes adatokat is, vagyis az összes személyes adatot együttesen kell értékelni. Az egészségügyi adatokat, személyazonosító okmányokat vagy pénzügyi adatokat, például hitelkártya adatokat érintő incidensek önmagukban is mind kárt okozhatnak, együttesen azonban személyazonosság-lopáshoz vezethetnek. A személyes adatok együttesen érzékenyebbnek tekinthetők, mint külön-külön. Ehhez hasonlóan kis mennyiségű, fokozottan érzékeny személyes adatnak jelentős hatása lehet az egyénre, és egy nagy mennyiségű személyes adat pedig még szélesebb részét fedheti fel az egyénnek.

2.3 Az egyének könnyű azonosíthatósága: Az előző ponthoz szorosan kapcsolódó fontos, mérlegelendő tényező, hogy a veszélyeztetett személyes adatokhoz hozzáférő fél mennyire könnyen tudja azonosítani az egyes egyéneket, vagy egyének azonosítása céljából más információkkal összeegyeztetni az adatokat.

2.4 Az egyéneket érintő következmények súlyossága: Az incidensben érintett személyes adatok jellegétől függően, például különleges kategóriájú adatok esetében különösen súlyosak lehetnek az egyéneket fenyegető lehetséges károk, különösen akkor, ha az incidens személyazonosság-lopáshoz, személyazonossággal való visszaéléshez vezethet.

2.5 Az egyén sajátosságai: Az incidens érintheti gyermekek vagy más olyan, kiszolgáltatott helyzetben lévő egyének személyes adatait, akik ennek következtében nagyobb veszélybe kerülhetnek. Az egyénnel kapcsolatosan más olyan tényezők is felmerülhetnek, amelyek befolyásolják az incidens rájuk gyakorolt hatását.

2.6 Az adatkezelő sajátosságai: Az adatkezelő és tevékenységei jellege és szerepe befolyásolhatják az incidens következtében az egyéneket érintő kockázat mértékét. Például az egészségügyi szervezetek különleges kategóriájú személyes adatokat dolgoznak fel, következésképpen e személyes adataik megsértése esetén nagyobb fenyegetés éri az egyéneket, mint ha egy hírlevél listája kerülne nyilvánosságra.

2.7 Az érintett egyének száma: Az incidens érinthet csak egy, néhány, több ezer vagy akár még több személyt. Általánosságban elmondható, hogy minél nagyobb az érintett egyének száma, annál nagyobb hatást gyakorol az incidens.

2.8 Általános szempontok: Következésképpen a valószínűsíthetően az incidens miatt felmerülő kockázat felmérésekor az adatkezelőnek együttesen kell mérlegelnie az egyének jogaira és szabadságaira esetlegesen gyakorolt hatás súlyosságát és bekövetkezésének valószínűségét. Egyértelmű, hogy amikor az incidens súlyosabb következményekkel jár, a kockázat is magasabb, és ehhez hasonlóan, amikor nagyobb ezek bekövetkezésének valószínűsége, akkor a kockázat is fokozódik.

Amennyiben az adatkezelő mérlegelése körében megállapította, hogy az adatvédelmi incidens valószínűsíthetően kockázattal, vagy valószínűsíthetően magas kockázattal ját a természetes személyek jogaira és szabadságaira nézve az adatkezelőnek bejelentést kell tennie, illetve tájékoztatást kell adnia következő pontban kifejtettek szerint. Ammenyiben a kritériumok értékelése közben az adatkezelőnek kétsége merülne fel, a biztonság kedvéért javasoljuk bejelentést/tájékoztatást szintén megtenni.

3. Az OKFŐ tájékoztatása

3.1 Amennyiben az egészségügyi szolgáltatót **nem az OKFŐ tájékoztatta** az adatvédelmi incidensről vagy annak gyanújáról, kizárólag akkor köteles az OKFŐ-t értesíteni a kivizsgálás eredményéről, amennyiben az incidens okaként az EESZT nem üzemszerű működését állapította meg.

3.2 Amennyiben az egészségügyi szolgáltatót **az OKFŐ tájékoztatta** az adatvédelmi incidensről vagy annak gyanújáról, az eset kivizsgálását követően haladéktalanul értesíti az OKFŐ-t a vizsgálat eredményéről, részleteiről, valamint az incidens elhárítása érdekében tett intézkedésekről. A tájékoztatást az egészségügyi szolgáltató minden esetben e-mailben, az adatvedelem.eeszt@okfo.gov.hu e-mail címre küldött levélben köteles megtenni.

4. Az érintett tájékoztatása

Amennyiben a vizsgálat és a kockázatok felmérése arra az eredményre jutott, hogy az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatkezelő indokolatlan késedelem nélkül tájékoztatja az érintetteket az adatvédelmi incidensről.

A tájékoztatásban világosan és közérthetően

4.1 ismertetni kell az adatvédelmi incidens jellegét,

4.2 és közölni kell legalább az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;

4.3 ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket;

4.4 ismertetni kell az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

Az érintettet nem kell az előző pontban említettek szerint tájékoztatni, ha az alábbi feltételek bármelyike teljesül:

4.5 az adatkezelő az incidens bekövetkezése előtt megfelelő technikai és szervezési intézkedéseket alkalmazott személyes adatok védelme érdekében, ideértve különösen azokat az intézkedéseket, amelyek a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik az adatokat.

4.6 az adatkezelő rögtön az incidenst követően intézkedéseket tett annak biztosítása érdekében, hogy az egyének jogaira és szabadságaira jelentett magas kockázat a továbbiakban valószínűsíthetően ne valósuljon meg. Az eset körülményeitől függően például előfordulhat, hogy az adatkezelő azonnal azonosította azt az egyént, aki még azelőtt hozzáfért a személyes adatokhoz, mielőtt bármit lehetett volna velük kezdeni, és intézkedéseket hozhatott vele szemben. Ekkor is kellő figyelmet kell fordítani a titoksértés lehetséges következményeire, szintén az érintett adatok jellegétől függően.

4.7 az egyénekkel való kapcsolatfelvétel aránytalan erőfeszítést tenne szükségessé, talán azért, mert elérhetőségi adataik az incidens következtében elvesztek, vagy eleve nem is voltak ismertek. Például egy dokumentumok tárolására szolgáló raktárat elönt az árvíz, és a személyes adatokat tartalmazó dokumentumokat kizárólag papíralapon tárolták. Az adatkezelőnek ilyenkor nyilvánosan közzétett információk útján kell tájékoztatnia az egyéneket, vagy olyan hasonló intézkedést kell hoznia, amely biztosítja a hasonlóan hatékony tájékoztatásukat. Amennyiben aránytalan erőfeszítésre lenne szükség, olyan technikai megoldások is alkalmazhatók, amelyekkel igény szerint válik hozzáférhetővé az incidenssel kapcsolatos tájékoztatás. Ez azoknál az egyéneknél bizonyulhat hasznosnak, akiket az incidens érintett, de az adatkezelő nem tud más módon kapcsolatba lépni velük.

Az Érintettek tájékoztatása ennek megfelelően közvetlenül, vagy nyilvánosan közzétett (például honlapon keresztül közzétett) információk útján valósulhat meg.

5. Az incidens elhárítása

Az adatkezelőnek egyúttal gondoskodnia kell az incidens elhárításáról, majd a normál működés helyreállításról. E körben mindig az adott incidens sajátosságainak megfelelően kell eljárni.

Az OKFŐ az egészségügyi szolgáltató kérésére közreműködik a komplexebb incidensek tisztázásában, a lehetséges mértékben támogatja az egészségügyi szolgáltatót a kivizsgálásban és – adott esetben – elhárításában.

6. Az adatvédelmi incidens nyilvántartása

Az incidens alakulásáról az egészségügyi szolgáltató, mint adatkezelő nyilvántartást vezet. Az adatvédelmi incidens nyilvántartásban fel kell tüntetni:

6.1 az adatvédelmi incidenshez kapcsolódó tényeket,

6.2 annak hatásait és

6.3 az orvoslására tett intézkedéseket.

Az incidens nyilvántartás célja, hogy a felügyeleti hatóság ellenőrizze az adatvédelmi követelményeknek való megfelelést. Az adatvédelmi incidens nyilvántartás minden esetben vezetni szükséges, ahol az incidens személyes adatokat érintett. Ebből adódóan itt nem kerül eltérő megítélés alá az az incidens, amely valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve attól az incidenstől, amely (magas) kockázattal jár a természetes személyek jogaira és szabadságaira nézve.

7. Incidens bejelentése a Hatóságnak

A bejelentést akkor kell megtenni a NAIH részére, ha az adatvédelmi incidens valószínűsíthetően kockázattal jár a természetes személyek jogaira és szabadságaira nézve, amelyet az egészségügyi szolgáltató a IV. fejezet 2. pontjában kifejtett kockázat felmérése körében ismertetett tényezők alapján mérlegelt. Ebben az esetben az incidensről történő tudomásszerzéstől számított 72 órán belül bejelentést kell tenni a NAIH részére.

Akkor tekinthető úgy, hogy az incidens az adatkezelő „tudomására" jutott, amikor az adatkezelő észszerű bizonyossággal **meggyőződött** arról, hogy olyan biztonsági incidens történt, amelynek következtében a személyes adatok veszélybe kerültek. A meggyőződéssel, megbizonyosodással kapcsolatban a GDPR (87) preambulum-bekezdése megköveteli, hogy az adatkezelő az összes megfelelő technikai védelmi és szervezési intézkedést végrehajtsa, egyrészt az incidens haladéktalan megállapítása, másrészt a felügyeleti hatóságnak történő bejelentés és az érintettek sürgős értesítése érdekében.

A Hatóságnak történő bejelentésben:

7.1 ismertetni kell az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát;

7.2 közölni kell az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;

7.3 ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket;

7.4 ismertetni kell az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

A bejelentést a NAIH honlapján található Adatvédelmi Incidensbejelentő Rendszeren keresztül az adatkezelő bármikor megteheti. Az Adatvédelmi Incidensbejelentő Rendszer a https://www.naih.hu/adatvedelmi-incidensbejelent--rendszer.html linken keresztül érhető el. Amennyiben valamely okból kifolyólag nem lehetséges az információkat egyidejűleg közölni a

Hatósággal – például az adatkezelőnek további vizsgálatot kell lefolytatnia az incidens szempontjából lényeges összes tény megállapítása céljából - azok további indokolatlan késedelem nélkül később, részletekben is közölhetők.

Ha a bejelentés nem történik meg 72 órán belül, akkor mellékelni kell hozzá a késedelem igazolására szolgáló indokokat is.

Az ünnepnapok, szünnapok esetén 1-2 nap késedelem elfogadható, de minden esetben haladéktalanul vagy legalábbis indokolatlan késedelem nélkül szükséges megtenni az intézkedéseket. A határidő esetleges elmulasztása esetén a NAIH az eset összes körülményét mérlegeli, és csak indokolt esetben állapít meg jogsértést. Ennek körében a Hatóság figyelembe veszi az incidens súlyosságát és késedelem mértékét és indokát is.

A NAIH-nál történő bejelentés csak abban az esetben mellőzhető, ha a vizsgálat és a kockázatok felmérése arra az eredményre jutott, hogy az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve.

V. Adatfeldolgozók kötelezettségei az adatvédelmi incidens kapcsán

A GDPR 28. cikk (3) bekezdés alapján az adatkezelő (jelen eljárásrend szempontjából az egészségügyi szolgáltató és az OKFŐ) köteles gondoskodni az alkalmazott adatfeldolgozójával érvényes és hatályos adatfeldolgozói megállapodás megkötéséről. Az adatfeldolgozói megállapodásnak az általánosan meghatározott követelményeken kívül, **az incidensek megelőzése, illetve kezelése vonatkozásában** adatkezelő által kötött **adatfeldolgozási megállapodásában javasolt kitérni az alábbi feltételekre is**:

1. Az adatfeldolgozó a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével a GDPR 32. cikk (1) bekezdés szerinti megfelelő technikai és szervezési intézkedéseket hajt végre annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja**.**
2. Amennyiben adatvédelmi incidens következik be, az adatfeldolgozó köteles haladéktalanul intézkedni az incidens elhárítása és a kár megelőzése érdekében. Az adatfeldolgozó az incidens tudomására jutásától számítva indokolatlan késedelem nélkül köteles tájékoztatni az adatkezelőt.
3. Amennyiben a személyes adatokkal kapcsolatos incidens nem esetileg bekövetkezett véges esemény, hanem folyamatosan fennáll, akkor a személyes adatok védelme érdekében az adatkezelő az adatfeldolgozással érintett szolgáltatást nyújtását felfüggeszti.
4. Az incidensről szóló tájékoztatást az adatfeldolgozó írásban köteles megtenni az adatkezelő felé. A bejelentésnek legalább a következő adatokat kell tartalmaznia:

   4.1 az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát;

4.2 a további tájékoztatást nyújtó azon kapcsolattartó nevét és elérhetőségeit, akit az incidens hatósági bejelentése esetén a hatóság az esetleges vizsgálat során közvetlenül elérhet;

4.3 az adatvédelmi incidensből eredő, valószínűsíthető következményeket.

4.4 az Adatfeldolgozó által az adatvédelmi incidens orvoslására tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

Az adatkezelő az adatfeldolgozó értesítése alapján dönt az incidens soron kívüli vizsgálatáról továbbá ehhez kapcsolódóan az adatfeldolgozásnak az incidens hatókörét meghaladó ellenőrzéséről is dönthet. A döntésben köteles az adatkezelő kijelölni a vizsgálatot, és kapcsolódó ellenőrzés esetén az azt végző személyeket. A vizsgálatról készített jelentés 1 példányát az adatkezelő átadja az adatfeldolgozónak.

Adatkezelő a vizsgálat alapján dönt az incidens elhárításához és a jövőben való bekövetkezés megelőzéséhez szükséges intézkedésekről, amelyet az adatfeldolgozó köteles végrehajtani.

Jelen eljárásrend 2021. július 28-án lép hatályba és visszavonásig érvényes.

VI. Mellékletek

1. számú melléklet: Tájékoztató adatvédelmi incidensek kezelésére EESZT-hez csatlakozott egészségügyi szolgáltatók részére

2. számú melléklet: Folyamatábra a bejelentési kötelezettségekről a WP250 állásfoglalása alapján

TÁJÉKOZTATÓ

adatvédelmi incidensek kezelésére

EESZT-hez csatlakozott egészségügyi szolgáltatók részére

EESZT
Elektronikus
Egészségügyi
Szolgáltatási Tér

ORSZÁGOS
KÓRHÁZI
FŐIGAZGATÓSÁG

Tartalom

A tájékoztató célja

Jelen tájékoztató az EESZT-hez csatlakozott egészségügyi szolgáltatók részére kiadott **adatvédelmi incidensek kezeléséről szóló eljárásrend mellékletét képezi**. Példálózó jelleggel tartalmaz néhány olyan adatvédelmi incidenst, amelyek esetén az EESZT rendszer érintettsége megállapítható lehet. Fontos kiemelni, hogy a felsorolt esetkörök nem fedik le a lehetséges adatvédelmi incidensek teljes körét. **Adatvédelmi incidens bekövetkezését minden esetben a hatályos adatvédelmi szabályok alapján egyedileg szükséges mérlegelni. A felmerült esetek teljeskörű kivizsgálásához az adatvédelmi incidensek beazonosításához szükséges támpontokat részletesen az adatvédelmi incidensek kezeléséről szóló eljárásrend tartalmazza.**

Az Országos Kórházi Főigazgatóság (a továbbiakban: OKFŐ) mint az EESZT működtetője a tájékoztató útján gyakorlati iránymutatást kíván adni az EESZT-hez csatlakozott egészségügyi szolgáltatók számára, segítve ezzel az adatvédelmi incidensek felismerését és megfelelő kezelését. Jelen tájékoztató nem terjed ki a felmerült adatvédelmi incidensekkel kapcsolatos részletes eljárási szabályokra, azokat a fent említett eljárásrend tartalmazza.

Adatvédelmi incidensek a gyakorlatban

Az egészségügyi szolgáltatóknak **minden esetben teljeskörűen ki kell vizsgálniuk** a felmerült problémát az eljárásrendben meghatározott szempontok szerint annak megállapítása érdekében, hogy **valóban történt-e adatvédelmi incidens.**

1. Helytelen TAJ-szám használatából eredő incidensek

- **Bekövetkezett adatvédelmi incidensre utaló jelek:**
  - a bejelentő olyan ellátási eseményt lát a Lakossági Portál felületén, amelyen nem vett részt
  - a bejelentő más személy eReceptjét is látja saját eReceptjei között a Lakossági Portál felületen
  - a bejelentő más személy eBeutalóját is látja saját eBeutalói között a Lakossági Portál felületen
  - a bejelentő olyan EHR dokumentumot lát a saját Lakossági Portál felületén, amely nem hozzá tartozik
- **Az adatvédelmi incidens lehetséges okai:**
  - TAJ-szám elütése
  - TAJ-szám visszaellenőrzésének hiánya
  - TAJ-szám helyett a páciens nevére vagy születési dátumára történő keresés, így azonos nevű vagy születési dátummal rendelkező más személy TAJ-számára történő rögzítés
  - EESZT nem üzemszerű működése

Figyelem! A téves adatrögzítés önmagában nem feltétlenül jelenti adatvédelmi incidens bekövetkezését. Amennyiben az érintettre vonatkozó, tehát **más személyhez *nem* köthető** hibás adatról érkezik bejelentés (pl. rossz vércsoport került rögzítésre, helytelen gyógyszer felírása az érintett nevére, a zárójelentésben helytelen megállapítások szerepelnek, stb.), akkor **nem beszélhetünk adatvédelmi incidensről**.

Erre jó példaként szolgálhat az az eset, amikor az ellátáson részt nem vett személy egy olyan beutalót, vagy eReceptet lát a felületén, amelyen – tévesen – a saját adatai szerepelnek, emellett azonban pusztán olyan információk látszanak, mint egy gyógyszer neve, vagy az intézmény neve, ahová a beutaló szól, akkor az eset egyértelműen *nem adatvédelmi incidens, mivel nem tudja azonosítani, hogy a gyógyszer kinek lett felírva, ki lett beutalva az adott intézménybe*. Ugyanezen megítélés alá esik azon eset, ha az Ön nevével és adataival ellátva tévesen egy olyan EHR dokumentum lett feltöltve, amely az ellátás adatait tartalmazza; a panaszokat, diagnózist, alkalmazott kezelést (de egyéb, más személyre vonatkozó személyazonosító adatot nem) – ebben az esetben sem tudja megállapítani a személy, hogy kinek a panaszait, kinek a diagnózisát, kinek a részére előírt kezelésre vonatkozó adatait látja.

Ilyen esetben az adatvédelmi hatóságnak (NAIH) történő **bejelentésre nincs szükség**, ám **az adatok helyesbítését el szükséges végezni** abban az esetben is, ha ezirányú kérelem nem érkezik. A hibás adatok helyesbítésére orvos-szakmai mérlegelés után kizárólag az az egészségügyi szolgáltató jogosult, amely az adatot rögzítette az EESZT-ben.

Az itt ismertetett esetekkel szemben azonban előfordulnak olyan esetek is, amikor a feltöltött **dokumentumon/bejegyzésben szerepel, hogy kihez tartozik**, ilyen eset lehet pl. egy orvosi lelet. Ha a feltöltött leleten szerepel az ellátáson részt vett személy neve és egyéb személyazonosító adatai, akkor

a **téves feltöltés adatvédelmi incidenst valósít meg**, ez esetben azt – a kockázatot mérlegelve – az adatkezelőnek **be kell jelenteni a Hatóságnak** és az eljárásrendben foglaltak szerint megtenni a **szükséges intézkedéseket**, helyesbítést.

- **Okozott adatvédelmi problémák ismertetése:**
  - jogosulatlan adathozzáférés (a bejelentő, valamint bármely más, jogosultsággal nem rendelkező személy által)
- **Az adatvédelmi incidens kezelése körében kötelezően eljáró szerv:**
  - Az adatfeltöltést végző egészségügyi szolgáltató
  - EESZT nem üzemszerű működése esetén: Az egészségügyi szolgáltató köteles haladéktalanul értesíteni OKFŐ-t az EESZT oldali hibára utaló körülmények részletes leírásával.

2. Az adatfeltöltést végző egészségügyi szolgáltató EESZT kompatibilis medikai programjában EESZT intézményi törzsadatbázis nem megfelelő használata

- **Bekövetkezett adatvédelmi incidensre utaló jelek:**
  - a medikai program eBeutaló kiállítása esetén nem a kívánt ellátást nyújtó szolgáltatót jeleníti meg
  - az érintett nem a megfelelő intézményhez kiállított eBeutalót látja a Lakossági Portál felületen
- **Az adatvédelmi incidens lehetséges okai:**
  - a medikai rendszer hibája
  - az eBeutalót kiállító orvos nem körültekintően használta a medikai program törzsadatbázisát (rossz szolgáltatót választott ki)
  - EESZT nem üzemszerű működése
- **Okozott adatvédelmi problémák ismertetése:**
  - jogosulatlan adathozzáférés (az ellátást nyújtóként tévesen bejelölt szolgáltató részéről történő adatmegismerés)
- **Az adatvédelmi incidens kezelése körében kötelezően eljáró szerv:**
  - a medikai rendszer hibája esetén: medikai rendszer szállítója
  - rossz szolgáltató kiválasztása esetén: a hibát vétő egészségügyi szolgáltató, a helytelenül kiválasztott ellátást nyújtó szolgáltató tájékoztatási kötelezettsége mellett amennyiben a hibát a kiválasztott szolgáltató észlelte
  - EESZT nem üzemszerű működése esetén: Az egészségügyi szolgáltató köteles haladéktalanul értesíteni OKFŐ-t az EESZT oldali hibára utaló körülmények részletes leírásával.

3. A bejelentő EESZT-ben tárolt adatai között nem szerepelnek olyan adatok, amelyek megőrzési időn belül keletkeztek

- **Bekövetkezett adatvédelmi incidensre utaló jelek:**
  - pl. a bejelentő 2018-ban rögzített ellátási eseménye 2020-ban nem található meg az EESZT rendszerben

- **Az adatvédelmi incidens lehetséges okai:**
  - egészségügyi szolgáltató vagy az általa használt medikai rendszer hibás működése
  - az EESZT nem üzemszerű működése
- **Okozott adatvédelmi problémák ismertetése:**
  - adatok véletlen vagy jogellenes megsemmisítése/elvesztése
- **Az adatvédelmi incidens kezelése körében kötelezően eljáró szerv:**
  - egészségügyi szolgáltató vagy az általa használt medikai rendszer hibás működése esetén az egészségügyi szolgáltató vagy a hibásan működő medikai rendszer szállítója
    - EESZT nem üzemszerű működése esetén: Az egészségügyi szolgáltató köteles haladéktalanul értesíteni OKFŐ-t az EESZT oldali hibára utaló körülmények részletes leírásával.

Figyelem! Nem minősül adatvédelmi incidensnek, ha egy ellátásról szóló információk nem kerülnek feltöltésre az EESZT-be az egészségügyi szolgáltató adatszolgáltatási kötelezettsége ellenére. Ebben az esetben az egészségügyi szolgáltató jogsértő magatartást tanúsít.

Figyelem! Nem minősül adatvédelmi incidensnek, ha az adatot az egészségügyi szolgáltató orvos-szakmai szempontból megfontolt döntése miatt törölte (pl. tévedésből felvitt adat esetén).

Figyelem! Hiányzó adatok hátterében az is állhat, hogy az egészségügyi szolgáltató hibás TAJ-számra rögzítette a dokumentumot/bejegyzést és az nem került korrigálásra. Az ilyen típusú eseményt az 1. pont szerint („Helytelen TAJ-szám használatából eredő incidensek") szükséges megítélni és kezelni.

4. Digitális önrendelkezésben megadott tiltó rendelkezések ellenére adatmegismerési lehetőség nyitott az orvos számára

- **Bekövetkezett adatvédelmi incidensre utaló jelek:**
  - az ellátó orvos tiltó rendelkezések beállítása ellenére látja a páciens EESZT-ben tárolt adatait
- **Az adatvédelmi incidens lehetséges okai:**
  - medikai rendszer hibás működése
  - az EESZT nem üzemszerű működése
- **Okozott adatvédelmi problémák ismertetése:**
  - jogosulatlan adathozzáférés
- **Az adatvédelmi incidens kezelése körében kötelezően eljáró szerv:**
  - a medikai rendszer hibája esetén: medikai rendszer szállítója
    - EESZT nem üzemszerű működése esetén: Az egészségügyi szolgáltató köteles haladéktalanul értesíteni OKFŐ-t az EESZT oldali hibára utaló körülmények részletes leírásával.

Figyelem! Nem minősül adatvédelmi incidensnek a páciens által 24 órára adott egyedi engedély alapján történő adatmegismerés. A páciens EESZT-ben tárolt egészségügyi adataihoz és dokumentumaihoz meghatározott naptári napra a digitális önrendelkezési korlátozásai ellenére hozzáférést adhat kezelőorvosa számára.

Break glass funkció jogellenes alkalmazása

Az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény (a továbbiakban Eüak.) 10. § (4) bekezdése szerint sürgős szükség esetén a kezelést végző orvos által ismert, a gyógykezeléssel összefüggésbe hozható minden egészségügyi és személyazonosító adat továbbítható.

Ezt az EESZT-ben az **ún. break glass (azaz „üvegtörés") funkció** biztosítja, amelyet használva a kezelést végző orvos **indokolt ellátási esetben feloldhatja a digitális önrendelkezési nyilatkozatban szereplő alapértelmezett és beállított korlátozásokat**, ezzel az összes rendelkezést felülírja, így **egyetlen lekérdezés erejéig** hozzáférhet olyan adatokhoz, amelyekhez egyébként nem lenne jogosultsága. A hozzáférés teljesítése után a rendszer visszatér a beállított alapállapothoz.

Fontos azonban tisztázni a funkció használatának peremfeltételeit, hiszen ez egy igencsak limitáltan igénybe vehető lehetőség, amelynek **túlzott használata akár büntetőjogi szankciót** is vonhat maga után, így minden esetben kiemelt körültekintéssel kell eljárni a szükségesség megítélésekor.

A sürgős szükség fennállását csak és kizárólag az orvos képes megítélni az adott helyzet alapján, így ő tartozik felelősséggel azért, hogy **a Break glass funkciót csak és kizárólag kivételes és indokolt esetben vegye igénybe.** Mivel a fenti körülmények egzakt meghatározása az egyes helyzetek sajátosságai miatt nem lehetséges, az orvosnak kell eldöntenie, hogy valóban nem áll-e rendelkezésre egyéb módszer a szükséges betegadatokhoz való hozzáféréshez, vagy alakulhat-e ki olyan súlyos, életveszélyes helyzet, ami miatt elengedhetetlen a funkció használata.

Az EESZT vonatkozó felületén az orvosnak jelölnie kell az adott időpontban fennálló, az Eüak. 12. § (3) bekezdése szerinti sürgős szükség helyzetét és azt, hogy ez alapján kér adatot az EESZT-ből. Ez a **bejelentés az orvos nyilatkozatának minősül** a sürgős szükség fennállása tekintetében, az erre vonatkozó **valótlan állításnak akár büntetőjogi következményei is lehetnek**. A rendszerből a Break glass funkció használatát tanúsító adatok visszakereshetők**.**

Gyakran ismételt kérdések

1. Mi minősül adatvédelmi incidensnek?

A GDPR 4. cikk 12. pontja alapján az adatvédelmi incidens a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, módosítását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi.

2. Mi a különbség biztonsági incidens és adatvédelmi incidens között?

Az adatvédelmi incidens egyfajta biztonsági incidens, amikor a személyes adatok biztonsága sérül. A különbség a biztonsági incidens és az adatvédelmi incidens között, hogy lényegét tekintve minden adatvédelmi incidens biztonsági incidens, azonban nem feltétlenül minősül mindegyik biztonsági incidens adatvédelmi incidensnek, tekintettel arra, hogy a biztonsági incidens nem kizárólag személyes adatokra korlátozódik.

3. Hogyan szerez tudomást az egészségügyi szolgáltató adatvédelmi incidens bekövetkezéséről?

Az adatvédelmi incidensről, vagy az incidensgyanújáról való *értesülés többféleképpen is megtörténhet:* az egészségügyi szolgáltató maga szerez tudomást az incidensről (például az betegellátó személy munkavégzés közben észleli az incidenst), vagy az adatfeldolgozó, az érintett, harmadik személy, az OKFŐ esetleg a Hatóság jelenti az incidenst az egészségügyi szolgáltatónak. Ezt követően az egészségügyi szolgáltató által lefolytatott kivizsgálás eredményeként állapítható meg, hogy történt-e adatvédelmi incidens.

Akkor tekinthető úgy, hogy az incidens az adatkezelő „tudomására" jutott, amikor az adatkezelő észszerű bizonyossággal meggyőződött arról, hogy olyan biztonsági incidens történt, amelynek következtében a személyes adatok veszélybe kerültek. A meggyőződéssel, megbizonyosodással kapcsolatban a GDPR (87) preambulum-bekezdése megköveteli, hogy az adatkezelő az összes megfelelő technikai védelmi és szervezési intézkedést végrehajtsa, egyrészt az incidens haladéktalan megállapítása, másrészt a felügyeleti hatóságnak történő bejelentés és az érintettek sürgős értesítése érdekében.

4. Amennyiben az egészségügyi szolgáltatóhoz az EESZT-t érintő adatvédelmi incidens bejelentés érkezik, a szolgáltatónak tájékoztatnia kell erről az OKFŐ-t?

Amennyiben az egészségügyi szolgáltatót **nem az OKFŐ tájékoztatta** az adatvédelmi incidensről vagy annak gyanújáról, kizárólag akkor köteles az OKFŐ-t értesíteni a kivizsgálás eredményéről, amennyiben az incidens okaként az EESZT nem üzemszerű működését állapította meg.

Amennyiben az egészségügyi szolgáltatót **az OKFŐ tájékoztatta** az adatvédelmi incidensről vagy annak gyanújáról, az eset kivizsgálását követően haladéktalanul értesíti az OKFŐ-t a vizsgálat eredményéről, részleteiről, valamint az incidens elhárítása érdekében tett intézkedésekről. A tájékoztatást az egészségügyi szolgáltató minden esetben e-mailben, az adatvedelem.eeszt@okfo.gov.hu e-mail címre küldött levélben köteles megtenni.

5. Az egészségügyi szolgáltató részéről ki az, aki adatvédelmi incidens bejelentés esetén eljár?

Az incidens észlelését követően azonnal értesíteni kell a megfelelő vezetési szinten lévő felettest (például kórházak esetében az intézmény vezetőjét, magánszolgáltatók esetében a vezető tisztségviselőt és az adatvédelmi tisztviselőt).

6. Amennyiben az egészségügyi szolgáltató adatvédelmi incidenst észlel vagy bejelentést kap, mi a teendője?

Az eljárás részletes szabályait az EESZT-hez csatlakozott egészségügyi szolgáltatók részére kiadott, adatvédelmi incidensek kezeléséről szóló eljárásrend tartalmazza.

7. Az EESZT-t érintő adatvédelmi incidens gyanú esetén miért nem az OKFŐ mint az EESZT üzemeltetője vizsgálja ki az esetet?

Az EESZT-be történő adatszolgáltatást az EESZT-hez csatlakozott egészségügyi szolgáltató adatkezelők végzik; az adatküldés az általuk használt medikai rendszerek EESZT-hez való integrált működésével történik. Az EESZT-ben tárolt adatok tehát meglévő adatok továbbításával kerülnek a Térbe, így azok tartalmáért az adatszolgáltatást végző egészségügyi szolgáltató tartozik felelősséggel. Ezért elsődlegesen az adatot feltöltő egészségügyi szolgáltató feladata az adatvédelmi incidens gyanú kivizsgálása. Amennyiben saját érdekkörén belül nem találja az incidenshez vezető biztonsági sérülést, az OKFŐ megvizsgálja, hogy az EESZT üzemszerű működése fennállt-e az incidens bekövetkezésének időpontjában.

8. Az EESZT-t érintő adatvédelmi incidens esetén miért nem az OKFŐ mint az EESZT üzemeltetője köteles az incidenst orvosolni?

Mivel az EESZT-be kerülő adatok a csatlakozott egészségügyi szolgáltatók informatikai rendszeréből kerülnek továbbításra az EESZT-be, *az adatvédelmi incidensek kivizsgálása elsődlegesen az adatot feltöltő egészségügyi szolgáltató feladata.*

Abban az esetben tehát, ha az incidens nem az EESZT üzemszerű működésének hiánya miatt következett be, az adatvédelmi incidenst az az adatkezelő köteles orvosolni, amelynél az adatvédelmi incidenst előidéző biztonsági sérülés bekövetkezett.

9. Minden esetben szükséges az adatvédelmi incidenst bejelenteni a hatóságnak (NAIH)?

Nem, a bejelentést akkor kell megtenni a NAIH részére, ha adatvédelmi incidens következett be és az adatvédelmi incidens valószínűsíthetően kockázattal jár a természetes személyek jogaira és szabadságaira nézve, amelyet az egészségügyi szolgáltató a kockázat felmérése körében ismertetett tényezők alapján mérlegelt.

10. Az esetleges incidensek bejelentése esetén a rendkívül szűk határidő hogyan alkalmazandó pl. egy hosszabb ünnep esetén?

A GDPR által megfogalmazott eljárásrend szerint, az incidensről való tudomásszerzést követő 72 órán belül, de legalábbis indokolatlan késedelem nélkül, az incidens tényét a Hatóság (NAIH) felé be kell jelenteni. Az ünnepnapok, szünnapok esetén 1-2 nap késedelem elfogadható, de minden esetben haladéktalanul vagy legalábbis indokolatlan késedelem nélkül szükséges megtenni az intézkedéseket. A határidő esetleges elmulasztása esetén a NAIH az eset összes körülményét mérlegeli, és csak indokolt esetben állapít meg jogsértést. Ennek körében a Hatóság figyelembe veszi az incidens súlyosságát és késedelem mértékét és indokát is.

2. számú melléklet: **Folyamatábra a bejelentési kötelezettségekről**