BUDAPEST FŐVÁROS II. KERÜLETI ÖNKORMÁNYZAT
EGÉSZSÉGÜGYI SZOLGÁLATA

1027 Budapest, Kapás u. 22.
Tel: +36/1/488-7500
euszolgig@kapas.hu

IG/2024/802.

ADATVÉDELMI INCIDENS KEZELÉSI SZABÁLYZATA

Hatályos: 2024. augusztus 5.

Készítette: Nádor Rendszerház

Jóváhagyta:

Budapest Főváros II. kerület Önkormányzata Egészségügyi Szolgálata 2

Dr. Stubnya Gusztáv
főigazgató főorvos

A DOKUMENTUM MÓDOSÍTÁSAINAK JEGYZÉKE

A dokumentum következő felülvizsgálatát 2024. augusztus 31-ig el kell végezni.

Verzió	Dátum	Leírás	Hatályba helyező utasítás száma
V1.0		Első verzió, Nádor Rendszerház	
V2.0		Második verzió, Nádor Rendszerház	

TARTALOM

1 Általános rendelkezések 4
1.1 A Szabályzat célja 4
2 Adatvédelmi incidens észlelése és értékelése 4
2.1 Incidensbejelentések 5
2.1.1 Munkatársak által észlelt incidens, vagy fogadott incidens bejelentés 5
2.1.2 Központi kapcsolattartási címre érkezett incidensbejelentés 5
2.1.3 Adatfeldolgozó által észlelt incidens 5
2.1.4 Bejelentő védelme 6
2.2 Adatvédelmi incidensek értékelése 6
3 Az adatvédelmi incidens bejelentése a felügyeleti hatóságnak 6
4 Az érintett tájékoztatása az adatvédelmi incidensről 7
4.1 Kivétel a tájékoztatási kötelezettség alól 7
5 Adatvédelmi incidensek nyilvántartása 7
6 Adatvédelmi incidensek jogkövetkezményei 8

1 Általános rendelkezések

1.1 A Szabályzat célja

A Szabályzat célja, hogy Budapest Főváros II. Kerületi Önkormányzat Egészségügyi Szolgálata (a továbbiakban az Intézmény) adatvédelmi incidenskezelési folyamatát szabályozza. Adatvédelmi incidens előfordulása esetén az Intézmény képes legyen:

a) az adatvédelmi incidensek azonosítására, felderítésére, vagy az ilyen irányú bejelentések fogadására, jogszabályban megállapított határidők betartására;
b) az incidensre adott megfelelő intézkedések megtételére, beleértve a hatóság felé történő bejelentést és szükség esetén az érintettek értesítését;
c) az adatvédelmi incidensek előfordulása nyomán, a megfelelő tanulságok levonására, a további incidensek megelőzésére szolgáló ellenintézkedések bevezetésére.

A Szabályzat személyi hatálya kiterjed az Intézmény, továbbá a szerződött adatfeldolgozóinak alkalmazottjaira, továbbá olyan külső személyekre, akik az Intézmény által kezelt személyes adatokkal valamilyen módon kapcsolatba kerülnek (természetes és jogi személyek, jogi személyiséggel nem rendelkező szervezetek, stb.), beleértve a megbízási szerződéssel, vagy egyéb szerződéssel az Intézmény határozott időre/feladatokra foglalkoztatott külső alkalmazottakat is.

Fogalom meghatározások és rövidítések

„adatvédelmi incidens": a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi;

Kapcsolódó dokumentumok

a) Adatvédelmi szabályzat
b) Adatvédelmi tájékoztatók

Az incidenskezelésben részt vevő személyek és felelősségük:

a) valamennyi dolgozó:
b) incidensek közvetlen észlelése, vagy bejelentés fogadása;
c) területi vezetők (irodavezetők, osztályvezetők):
d) munkatársak képzése és tájékoztatása adatkezelési kötelezettségeik és incidenskezelési feladataik tekintetében;
e) Adatvédelmi tisztviselő:
f) adatvédelmi tevékenység koordinálása;
g) incidens bejelentések fogadása és értékelése, szervezeten belül;
h) szükséges intézkedések, bejelentések és tájékoztatások megtétele.

A kezdeti képzés és az évenkénti képzés megszervezéséért a szakterületi vezetők a felelősek. Az oktatás tantermi vagy e-learning keretek között valósul meg.

2 Adatvédelmi incidens észlelése és értékelése

A Rendelet fogalom meghatározása szerint az adatvédelmi incidens a biztonság olyan sérülése, amely a továbbított, tárolt, vagy más módon kezelt személyes adatok véletlen, vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését, vagy az azokhoz való jogosulatlan hozzáférést eredményezi.

Adatvédelmi incidensről a Szolgálat Intézmény jellemzően az alábbi módokon szerezhet tudomást:

a) munkatársak által észlelt incidens;
b) harmadik fél által bejelentett incidens;
c) érintett(ek) által bejelentett incidens.

Jellemző események, amelyek adatvédelmi incidenst okozhatnak:

a) adathordozó eszközök elvesztése, vagy azok megsemmisülése;
b) adatállomány véletlen, vagy szándékos törlése, megsemmisítése, megváltoztatása;
c) jogosulatlan (idegen, vagy fel nem hatalmazott személy) hozzáférése az adatokhoz (leletek, záró jelentések, stb.), adatmásolás, támadás, szándékos visszaélés;
d) adatok (leletek, záró jelentések, stb.) jogosulatlan átadása, hozzáférés biztosítása jogosulatlan személynek;
e) vírus, vagy hekker támadás az elektronikus információs rendszer ellen, stb.

2.1 Incidens-bejelentések

2.1.1 Munkatársak által észlelt incidens, vagy fogadott incidens bejelentés

Érintettek adatvédelmi incidenst hivatalosan az Adatvédelmi és adatkezelési tájékoztatóban közzétett email címen jelenthetnek be, de előfordulhat, hogy valamelyik munkatárshoz érkezik a bejelentés. A részére jelzett vagy általa észlelt incidensről a tájékoztatást a munkatárs kötelessége, hogy haladéktalanul továbbítsa a szakterület vezetője és az Adatvédelmi tisztviselő részére. Az azonnali továbbítás elengedhetetlen, mivel az adatvédelmi incidensek értékelésére és a szükséges intézkedések megtételére rendkívül rövid idő áll rendelkezésre, mindössze 72 óra (3 nap). A jelentés lényegi részleteit e-mailben kell elküldeni, és a szakterületi vezető felé telefonon meg kell erősíteni a bejelentést.

A bejelentés kötelező elemei:

a) Bejelentő neve
b) Az incidensről való tudomásszerzés módja (saját megállapítás, vagy bejelentés)
c) Az adatvédelmi incidens jellege, beleértve – ha lehetséges – az érintettek kategóriái és hozzávetőleges száma, valamint az incidenssel érintett adatok kategóriái és hozzávetőleges száma.

2.1.2 Központi kapcsolattartási címre érkezett incidens-bejelentés

A központi kapcsolattartási címre érkezett incidens bejelentést közvetlenül a Titkárság és az Adatvédelmi tisztviselő számára kell eljuttatni. A rövid határidő miatt, házon kívüli elfoglaltsága esetén, telefonon is értesíteni kell a Főigazgató főorvost.

A bejelentést tevő munkatárs felelősségre akkor vonható, ha jelentéséről bebizonyosodik, hogy szándékosan valótlan tartalommal bírt. Egyéb esetben a munkatárssal szemben semmiféle hátrányos elbánás nem alkalmazható.

A bejelentést tevő munkatársat a Főigazgató főorvos munkáltatói dicséretben részesítheti.

2.1.3 Adatfeldolgozó által észlelt incidens

Az Intézménnyel szerződött adatfeldolgozó az adatvédelmi incidenst, az arról való tudomásszerzését követően indokolatlan késedelem nélkül bejelenti az Intézmény Finanszírozási és Kontrolling Koordinátori vezetőnek, a Titkárság és az Adatvédelmi tisztviselője részére.

2.1.4 Bejelentő védelme

A bejelentő személy kérheti nevének elhallgatását és adatainak zárt kezelését. Ebben az esetben ezeket csak az Intézmény vezetési jogkörének gyakorlása miatt a Főigazgató főorvos ismerhet meg. Az adatokat zárt borítékban, páncélszekrényben kell tárolni.

2.2 Adatvédelmi incidensek értékelése

Az Adatvédelmi tisztviselő irányítja az incidensről szóló jelentés kivizsgálását. A vizsgálat során

a) meg kell állapítani az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát;
b) fel kell mérni az adatvédelmi incidensből eredő, valószínűsíthető következményeket.

Ki kell vizsgálni az incidens valószínű okát, azonnali intézkedéseket kell hozni, illetve hosszabb távú intézkedési tervet kell kidolgozni az incidens hatásainak csökkentésére, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

Az adatvédelmi tisztviselő a kivizsgálás során:

a) összegyűjti az adatokat, információkat, meghallgatja az érintetteteket;
b) értékeli a kapott információkat
c) jóváhagyásra előkészíti intézkedési tervet – feladat, felelős, határidő megjelöléssel
d) az incidensről incidenskezelési nyilvántartást vezet;
e) az intézkedési tervet szükség esetén egyezteti a felügyelő hatósággal;
f) nyomon követi a felügyelő hatóság által is elfogadott intézkedési terv megvalósulását amennyiben szükséges, egyeztetéseket, megbeszéléseket hív össze;

Az incidens okának feltárása után belső képzéseket kell tartani a további adatvédelmi incidensek megelőzése érdekében.

Az incidens kivizsgálásában az üggyel szemben elfogult személy nem vonható be.

Az incidens bejelentést nem kell kivizsgálni, ha ugyanazon incidens kivizsgálása már folyamatban van. Azonban a bejelentést nyilvántartásba kell venni.

3 Az adatvédelmi incidens bejelentése a felügyeleti hatóságnak

Az adatvédelmi incidenst indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, az Intézmény Adatvédelmi tisztviselője jelenti be az illetékes felügyeleti hatóságnak, kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. A bejelentéshez készített dokumentációk a Főigazgató főorvosnak jóvá kell hagynia. Jóváhagyása nélkül az incidens nem jelenthető be.

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

A hatóság felé továbbított bejelentésben legalább:

a) ismertetni kell az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát;
b) közölni kell az Intézmény további tájékoztatást nyújtó kapcsolattartójának nevét és elérhetőségeit;
c) ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket;

d) 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.

Ha és amennyiben nem lehetséges az információkat egyidejűleg közölni, azok további indokolatlan késedelem nélkül később részletekben is közölhetők.

4 Az érintett tájékoztatása az adatvédelmi incidensről

Az érintett(ek)et az adatvédelmi incidensről indokolatlan késedelem nélkül tájékoztatni kell, ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve.

Az érintett részére adott tájékoztatásban világosan és közérthetően ismertetni kell az adatvédelmi incidens jellegét és közölni kell legalább az előző fejezet b), c) és d) pontjában említett információkat és intézkedéseket.

Az érintettek tájékoztatóját az Adatvédelmi tisztviselő készíti elő, és a tájékoztatás a Főigazgató főorvos jóváhagyásával történhet meg.

4.1 Kivétel a tájékoztatási kötelezettség alól

Nem kell az érintetteket tájékoztatni, ha a következő feltételek bármelyike teljesül:

a) az adatkezelő megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre és ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében alkalmazták, különösen azokat az intézkedéseket – mint például a titkosítás alkalmazása –, amelyek a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik az adatokat;
b) az adatkezelő az adatvédelmi incidenst követően olyan további intézkedéseket tett, amelyek biztosítják, hogy az érintett jogaira és szabadságaira jelentett, az (1) bekezdésben említett magas kockázat a továbbiakban valószínűsíthetően nem valósul meg;
c) a tájékoztatás aránytalan erőfeszítést tenne szükségessé. Ilyen esetekben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, vagy olyan hasonló intézkedést kell hozni, amely biztosítja az érintettek hasonlóan hatékony tájékoztatását.

Ha az adatkezelő még nem értesítette az érintettet az adatvédelmi incidensről, a felügyeleti hatóság, miután mérlegelte, hogy az adatvédelmi incidens valószínűsíthetően magas kockázattal jár-e, elrendelheti az érintett tájékoztatását, vagy megállapíthatja az előző, a), b) vagy c) pontban említett feltételek valamelyikének teljesülését.

5 Adatvédelmi incidensek nyilvántartása

Az Intézmény nyilvántartja az adatvédelmi incidenseket, feltüntetve az adatvédelmi incidenshez kapcsolódó tényeket, annak hatásait és az orvoslására tett intézkedéseket. E nyilvántartás lehetővé teszi, hogy a felügyeleti hatóság ellenőrizze a Rendelet incidenskezelésről szóló cikk követelményeinek való megfelelést.

A nyilvántartás vezetéséért az Adatvédelmi tisztviselő felelős.

6 Adatvédelmi incidensek jogkövetkezményei

Amennyiben dolgozó szándékos vagy gondatlan tevékenysége miatt következik be adatvédelmi incidens a Főigazgató főorvos dönt az adatvédelmi incidenssel kapcsolatos jogkövetkezmény kezdeményezéséről figyelembe véve a munkajogi szabályokat, illetve a Ptk. és Btk. rendelkezéseit.

Adatvédelmi incidens jogkövetkezményeként a dolgozóval szemben

a) jogi jellegű (szabálysértési vagy bűntető eljárás kezdeményezése, akár kártérítési eljárás indítása);
b) munkajogi (figyelmeztetés, felmondás);
c) pénzügyi jellegű (pénzbeli juttatás, kifizetés részben vagy egészben történő felfüggesztése, visszakövetelése, behajtása)

felelőségre vonást kezdeményezhető.

Az adatvédelmi incidens következményeként elrendelheti a belső szabályozás felülvizsgálatát, szükség szerinti módosítása és a szabályozás betartásának fokozott ellenőrzését.