Ikt. sz.: 2645/2021

Zuglói Család- és Gyermekjóléti Központ incidenskezelési szabályzata

Hatályos

2020. 07. 15.

1. Általános rendelkezések

A Szabályzat célja

A Szabályzat célja, hogy a Zuglói Család-és Gyermekjóléti Központ (a továbbiakban: ZCSK/szervezet) adatvédelmi incidenskezelési folyamatát szabályozza. Adatvédelmi incidens előfordulása esetén a szervezet képes legyen:

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

2. A szabályzat személyi hatálya

A személyi hatálya kiterjed a ZCSK, a szerződött adatfeldolgozók alkalmazottaira, továbbá olyan külső személyekre, akik a szervezet 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 a határozott időre/feladatokra foglalkoztatott külső alkalmazottakat is.

3. Fogalom meghatározások és rövidítések

Adatvédelmi incidens: A természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK Rendelet hatályon kívül helyezéséről szóló az Európai Parlament és Tanács (EU) 2016/679 Rendelete (a továbbiakban: GDPR) 4. cikk 12. pontja szerint 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.

Az incidenskezelésben részt vevő személyek és felelősségük:

- Valamennyi munkatárs: incidensek közvetlen észlelése vagy bejelentés fogadása.
- A szervezet vezetője és a belső adatvédelmi felelős: az adatvédelmi tevékenység koordinálása; képzés megszervezése, incidens bejelentések fogadása és értékelése a szervezeten belül; szükséges intézkedések, bejelentések és tájékoztatások megtétele.

A kezdeti képzés és az évenkénti képzés megszervezéséért az adatvédelmi felelős felel Budapest Főváros XIV. Kerület Zuglói Polgármesteri Hivatal adatvédelmi tisztviselőjével előre egyeztetve és vele együttműködve. Az oktatás személyes vagy e-learning keretek között valósul meg.

A GDPR követelmények 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 Hivatal jellemzően az alábbi módokon szerezhet tudomást:

- munkatársak által észlelt incidens
- harmadik fél által bejelentett incidens
- érintett(ek) által bejelentett incidens

Jellemző események, amelyek adatvédelmi incidenst okozhatnak:

- adathordozó eszközök elvesztése vagy azok megsemmisülése
- adatállomány véletlen vagy szándékos törlése, megsemmisítése, megváltoztatása
- jogosulatlan (idegen vagy fel nem hatalmazott személy) hozzáférése az adatokhoz, adatmásolás
- támadás, szándékos visszaélés
- adatok jogosulatlan átadása, hozzáférés biztosítása jogosulatlan személynek
- vírus vagy hacker támadás az elektronikus információs rendszer ellen

4. Incidensbejelentések

a) Munkatársak által észlelt incidens, vagy fogadott incidens bejelentés esetén az incidensek hivatalos bejelentési csatornája az adatvédelmi felelős email címe, illetve az adatvédelmi tisztviselő email címe. Amelyik munkatárs adatvédelmi incidensről szerez tudomást, ebben az esetben a munkatárs kötelessége, hogy a kapott tájékoztatást haladéktalanul továbbítsa az szerv vezetője, az adatvédelmi felelős illetve az adatvédelmi tisztviselő részére.

Az azonnali továbbítás elengedhetetlen, mivel az adatvédelmi incidensek értékelésére és a szükséges intézkedések megtételére a GDPR 33. cikk (1) bekezdése szerint rendkívül rövid idő áll rendelkezésre, **mindössze 72 óra** (3 nap). A jelentés lényegi részleteit emailben kell elküldeni, s az erre szolgáló belső telefonszámon is meg kell erősíteni a bejelentést.

A bejelentés kötelező elemei:

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

b) Adatfeldolgozó által észlelt incidens

A ZCSK-val szerződött adatfeldolgozó az adatvédelmi incidenst, az arról való tudomásszerzését követően indokolatlan késedelem nélkül bejelenti a ZCSK által a szerződésben kijelölt kapcsolattartójának és a belső adatvédelmi felelősnek.

5. Adatvédelmi incidensek értékelése

A szervezet vezetője vagy a belső adatvédelmi felelős irányítja az incidensről szóló jelentés kivizsgálását, melyről az adatvédelmi tisztviselőt is tájékoztatnia kell, amennyiben úgy ítélik meg, hogy az incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságára nézve.

A vizsgálat során 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; 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 felelős 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.

6. 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, a szervezet belső adatvédelmi felelőse bejelenti az illetékes felügyeleti hatóságnak, kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve.

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 a további tájékoztatást nyújtó kapcsolattartó 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.

7. 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 felelős készíti elő, és a tájékoztatás a szervezet vezetőjének jóváhagyásával történhet meg.

Kivétel a tájékoztatási kötelezettség alól, azaz 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.

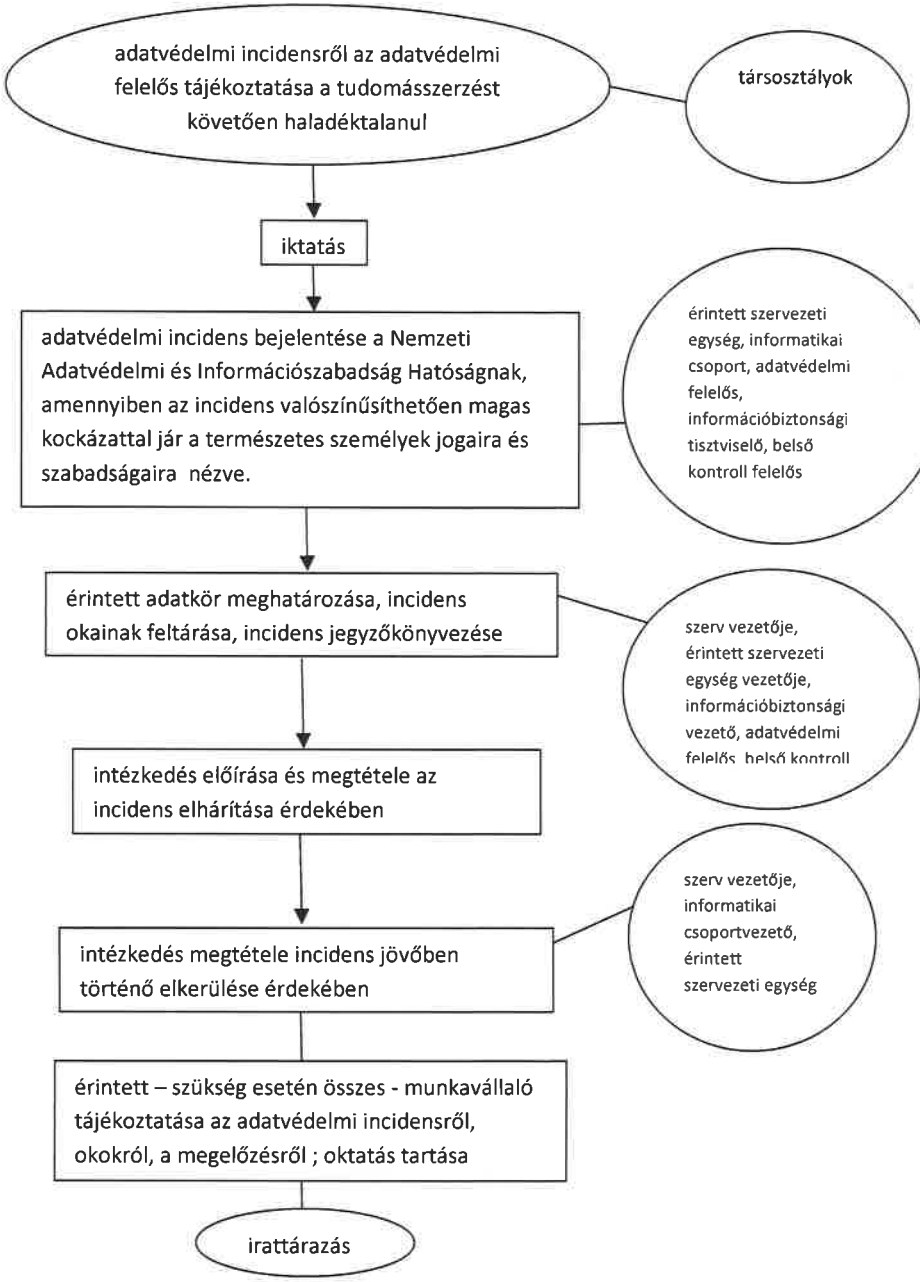
8. Adatvédelmi incidensek nyilvántartása

A szervezet 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.

9. Adatvédelmi incidensek jogkövetkezményei

Amennyiben a munkatárs szándékos vagy gondatlan tevékenysége miatt következik be adatvédelmi incidens a szervezet vezetője 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) felelősségre vonást kezdeményezhető. Az adatvédelmi incidens következményeként elrendelheti a belső szabályozás felülvizsgálatát, szükség szerinti módosítása és a szabályozás betartásának fokozott ellenőrzését.

ADATVÉDELMI INCIDENS DOKUMENTÁLÁSA, KEZELÉSE



DOKUMENTUM	FELELŐS
e-mail, papír alapú bejelentés	adminisztrátor
	intézmény vezetője, adatvédelmi felelős
jegyzőkönyv	adatvédelmi felelős
	szerv vezetője, érintett szervezeti egység vezetője, informatikai csoportvezető, információbiztonsági vezető, adatvédelmi felelős, belső kontroll felelős
	szerv vezetője, érintett szervezeti egység vezetője, informatikai csoportvezető adatvédelmi felelős, információbiztonsági vezető adminisztrátor

A Zuglói Család-és Gyermekjóléti Központ incidens kezelési szabályzata 2020. 07. 15.-től hatályos.

Budapest, 2020. július 15.

Varga Sándor

igazgató