Fővárosi Állat- és Növénykert **8/2021. számú szabályzat**

ADATVÉDELMI INCIDENS KEZELÉSI SZABÁLYZAT

Verzió	Dátum	Módosította/létrehozta	Módosítás
1.0.	2019. március 12.	dr. Karai Klára	Első verzió
2.0	2021. május 10.	Pósáné dr. Pécsi Szilvia	Felülvizsgálat

1. BEVEZETÉS

A Fővárosi Állat- és Növénykert, mint Adatkezelő (a továbbiakban: Adatkezelő/FÁNK) a jelen szabályzatban határozza meg az általa végzett személyes adatok kezelésével kapcsolatos adatvédelmi incidens során követendő eljárásrendet, az adatvédelmi incidens kezelését és nyilvántartását.

Az Adatkezelő az adatkezelési tevékenységét úgy végzi, hogy az megfeleljen az Európai Parlament és Tanács 2016/679. számú Általános Adatvédelmi Rendeletének, ismert elnevezéssel: a GDPR-nek, amely alapvetően szabályozza a természetes személyeknek a személyes adatok kezelése tekintetében történő védelmét és az ilyen adatok szabad áramlását.

1.1. A Szabályzat célja

A Szabályzat célja azoknak a belső szabályoknak és intézkedéseknek a megismertetése munkavállalókkal, megbízottakkal, amelyek az Adatkezelő (vagy Adatfeldolgozó) által a bekövetkezett adatvédelmi incidensek esetén végrehajtandók az incidensek hatásának csökkentésére, bekövetkezési okának feltárására és további incidensek elkerülésére, valamint az incidensek által leállított folyamatok minél előbbi újraindítására.

1.2. A Szabályzat hatálya: kikre és milyen tevékenységekre terjed ki a szabályozás

Jelen Szabályzat hatálya kiterjed

- az Adatkezelő és/vagy Adatfeldolgozó minden (belső és külsős) munkavállalóira, megbízottaira és egyéb közreműködőre, mint az adatvédelmi esemény vagy incidens észlelésekor az azonnali jelentési kötelezettség betartására;
- az Adatkezelő vagy Adatfeldolgozó adatvédelemért felelős tisztviselője/munkatársa számára az incidenskezelési folyamatban meghatározott feladatai végrehajtására;
- az incidenskezelés szakmai elemzésében és megoldásában, kezelésében részt vevők feladataik végrehajtásában.

1.3. Alapvető biztonsági szempontok

A személyes adatok kezelését oly módon kell végezni, hogy a megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szemben védelmet is ideértve.

A megfelelő technikai és szervezési intézkedéseket kell végrehajtani, a kezelt személyes adatokat érintő kockázat mértékének megfelelő szintű adatbiztonság garantálása érdekében. Ennek során figyelembe kell venni a tudomány és technológia állását és a megvalósítás költségeit, továbbá az adatkezelés jellegét, hatókörét, körülményeit és céljait, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázatot.

2. ADATVÉDELMI INCIDENS FOGALMA, FAJTÁI ÉS ÉRTÉKELÉSE

2.1. Adatvédelmi incidensnek minősül 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.

A személyes adat megsemmisítése azt jelent, hogy a személyes adat már nem létezik, legalábbis nincs meg olyan formátumban, amelyben az adatkezelő számára bármilyen módon felhasználható lenne,

A személyes adatok elvesztéséről akkor beszélhetünk, ha a személyes adat továbbra is létezik, de az adatkezelő nem fér hozzá, nincs a birtokában.

A személyes adatok megváltoztatásáról akkor beszélhetünk, ha a személyes adat állapotában, tartalmában, illetve megjelenésében módosulás történik.

Jogosulatlan közlés akkor következik be, ha arra illetéktelen személyekkel a személyes adatot megosztják.

Míg jogosulatlan hozzáférésről akkor beszélhetünk, ha illetéktelen személy képes a személyes adatot megismerni.

Személyes adat károsodásáról akkor beszélünk, ha az eredeti adatállományt megváltoztatták, az nem teljes.

Az adatvédelmi incidensek során a fenti fogalmak ismerete és elhatárolása jelentőséggel bír, hiszen az incidensek vizsgálatában, kockázati besorolásában szerepet játszanak.

2.2. Adatvédelmi incidensnek minősülnek például:

- Személyes adatok dokumentumon, hordozható eszközön, adathordozón vagy informatikai rendszeren (pl. levelezéssel) történő illegális továbbítása.
- Illetéktelen hozzáférések személyes adatokat kezelő informatikai rendszerhez vagy alkalmazáshoz (pl. jelenlegi vagy volt alkalmazott vétlen vagy tudatos közreműködése által, vagy biztonsági lyuk kihasználásával).
- Személyes adatokat tartalmazó adatbázis részének vagy egészének sérülése vagy elvesztése.
- Az informatikai rendszer részének vagy egészének használhatatlanná válása vírus vagy egyéb rosszindulatú szoftver által.

2.3. A gyakorlatban tipikusan előforduló incidenstípusok és az elvárt kockázatcsökkentő intézkedések

2.3.1. Téves címzés miatti félrepostázás, téves címzett részére küldött elektronikus levél

Az Adatkezelőnek ilyenkor mindent meg kell tennie, hogy a téves címzett birtokába jutott, személyes adatokat tartalmazó dokumentumot, üzenetet megsemmisítse/törölje. Továbbá gondoskodni kell arról, hogy a tényleges címzett is megkapja az üzenetet, valamint amennyiben például az érintett személyes adatok jellege alapján az incidens kockázatát valószínűsíthetően magasnak értékeli az Adatkezelő, tájékoztatnia kell sz incidensről az érintettet.

2.3.2. Hacker támadás következtében kiszivárgott adatok

Ilyen esetben fontos az incidens által érintett adatok mihamarabbi azonosítása, az informatikai biztonsági rendszer felülvizsgálata. Amennyiben a támadás emberi tényező kihasználásával történt, az elhárítás folyamatából kihagyhatatlan a munkavállalók oktatása. Abban az esetben, ha informatikai hibából adódott a sérülékenység, a teljes rendszer felülvizsgálata lehet indokolt. Ilyenkor minden esetben az információbiztonsági szabályzat felülvizsgálatát el kell végezni.

2.3.3. Ellopott/elveszett számítástechnikai eszközök, telefonok

Ezekben az esetekben kiemelt szerepet játszik az, hogy az Adatkezelő az incidenst megelőzően megfelelő figyelmet biztosított-e az eszközök védelmének (jelszó, titkosítás), amellyel megakadályozható, hogy az adott eszközön tárolt adatokat ismeretlen személyek megismerhessék. Távoli hozzáférés esetén utólag is elképzelhető az adatok eszközről való törlése. Fontos, hogy az incidensről való tudomásszerzést követően azonnal azonosítani kell, hogy az adott kliens milyen adatokhoz, szerverekhez, meghajtókhoz fért hozzá, és milyen jogosultság került kiosztásra számára, azokat azonnal meg kell vonni tőle, az érintett szervereket, meghajtók elérését vissza kell vonni, illetve a hozzáférést meg kell változtatni.

2.4. Egy adatvédelmi incidens után a feltárt hiányosságokat kiértékelve indokolt lehet a belső folyamatok felülvizsgálata, további szűrők, ellenőrzések beiktatása a munkafolyamatba, illetve a munkavállalók adatvédelmi tudatosságának növelése.

2.5. Az adatvédelmi incidens fajtái

Az adatvédelmi incidensek az alábbi három ismert információbiztonsági elv szerint kategorizálhatók:

- **bizalmassági incidens**: személyes adatok jogellenes, felhatalmazás nélküli vagy véletlen közlése vagy az azokhoz való jogosulatlan hozzáférés (például, ha egy hacker védett tartalmat és jelszavakat szerez meg egy website-ról);
- **integritási/sértetlenségi incidens**: személyes adatok jogellenes vagy véletlen megváltoztatása (például az adatbázis olyan módon történő feltörése, hogy a hacker személyes adatokat töröl belőle);
- **elérhetőségi/hozzáférhetőségi incidens:** személyes adatok véletlen vagy jogellenes megsemmisítése, a személyes adatokhoz való hozzáférés véletlen vagy jogellenes elvesztése (például egy laptopot ellopnak, és nincs back-up az adatokról, zsarolóvírus).

2.6. Osztályozás alapján az alábbi négy kategóriába sorolhatók az adatvédelmi incidensek:

- **Alacsony kockázat**: a természetes személyekre lényegében nincs kihatással az incidens vagy az részükre csupán kisebb kellemetlenséget okoz, amelyet gond nélkül meg tudnak oldani (pl. újra meg kell adniuk információt, idegeskedést okoz az incidens stb.);
- **Közepes kockázat**: a természetes személyek jelentős kellemetlenségeket tapasztalhatnak, amelyeket nehézségek árán meg tudnak oldani (extra költségek, szorongás, stressz, bizonyos szolgáltatásokhoz nem férnek hozzá, nem értik mi történik stb.);
- **Magas kockázat**: a természetes személyek jelentős következményekkel szembesülhetnek az incidens kapcsán, amelyeket képesek lehetnek leküzdeni, azonban csak komoly nehézségek árán (vagyoni veszteség, bank általi fekete listára helyezés, tulajdonban bekövetkező kár, állás elvesztése, egészségi állapot romlása stb.);
- **Nagyon magas kockázat**: a természetes személyek jelentős vagy akár visszafordíthatatlan következményekkel szembesülhetnek, amelyeket adott esetben nem képesek leküzdeni (pénzügyi nehézségek, úgy, mint például jelentős adósság vagy munkaképtelenség, hosszútávú pszichés vagy testi betegség, halál stb.).

2.7. További szempontok az adatvédelmi incidens megítélésében

A természetes személyek jogait és szabadságait érintő – változó valószínűségű és súlyosságú – kockázatok származhatnak a személyes adatok kezeléséből, amelyek fizikai, vagyoni vagy nem vagyoni károkhoz vezethetnek. A GDPR (75)-(76) preambulumbekezdései segítségül szolgálthatnak annak megítélésében, hogy mi tekinthető kockázatnak a természetes személyek jogaira és szabadságaira nézve (például személyazonosság-lopás, személyazonossággal való visszaélés, diszkrimináció, pénzügyi veszteség, jóhírnév sérelme, a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülése, gazdasági vagy szociális hátrány).

Az adatvédelmi incidens értékelése során négy adat kategóriát különböztethetünk meg, úgy, mint egyszerű, viselkedési, pénzügyi és érzékeny adat. Az incidenssel érintett adatok típusán felül, az adatok száma, az adatkezelő és a természetes személyek sajátos jellemzői és az adatok jellege figyelembe veendő és értékelendő tényezők.

További két tényezőt kell még figyelembe venni, amelyek, jóllehet közvetlenül nem jelennek meg de a végső értékelés szempontjából fontosak. Ezek a következők: az érintettek száma meghaladja-e a százat és az incidenssel érintett adatok értelmezhetőek-e / olvashatóak-e. Például, ha erős titkosítást használtak az adatok védelméhez és a titkosító kulcs érintetlen, akkor ez jelentősen csökkenteni tudja az incidens hátrányos következményeit.

3. ADATVÉDELMI INCIDENS ÉSZLELÉSE, KEZELÉSE

3.1. Adatvédelmi incidens észlelésekor az azt észlelő személy köteles azonnal **tájékoztatni** közvetlen munkahelyi vezetőjét, az Informatikai csoportvezetőt, valamint az adatvédelmi tisztviselőt. Munkahelyi vezető akadályoztatása (távollét, betegség stb.) esetén a szervezeti rend szerinti helyettes vagy helyettesítő vezető megkeresése szükséges. A bejelentés tartalmazza a bejelentő nevét, elérhetőségét, szervezeti egységét és az észlelt incidens megnevezését.

3.2. Az adatvédelmi tisztviselőnek a bejelentés megérkezését követően haladéktalanul megkezdi az **adatvédelmi incidens kivizsgálást és értékelését**, valamint szükség esetén a Nemzeti Adatvédelmi és Információszabadság Hatóság felé megteszi a bejelentést.

3.2.1. Adatvédelmi incidens esetén az adatvédelmi tisztviselő és az informatikai csoportvezető haladéktalanul megvizsgálja a bejelentést, ennek során azonosítani kell az incidenst, el kell dönteniük, hogy valódi incidensről vagy téves riasztásról van szó. Minden egyes adatvédelmi incidenst ki kell értékelni, azaz az elemzést esetről esetre szükséges elvégezni, kockázati besorolása az adatvédelmi incidensnek. Meg kell vizsgálni és meg kell állapítani:

- az incidens bekövetkezésének helyét és időpontját,
- az incidens leírását, körülményeit, hatásait,
- az incidens típusát, fajtáját,
- az incidens során érintett adatok körét (jellege, érzékenysége), számosságát,
- az incidenssel érintett személyek körét, mennyire könnyen azonosítható az adatvédelmi incidenssel érintett természetes személy, és az érintett személyek számát,
- az adatvédelmi incidenssel érintett személyre nézve fennálló következmények valószínűsége és súlyossága,
- az adatkezelő és tevékenysége jellemzőit,
- az incidens elhárítása érdekében megtett intézkedések leírását,
- a kár megelőzése, elhárítása, csökkentése érdekében tett intézkedések leírását.

3.2.2. Adatvédelmi incidens észlelésekor az adatvédelmi tisztviselő és az informatikai csoportvezető haladéktalanul tájékoztatja a FÁNK főigazgatóját.

3.3. Amennyiben az Adatkezelő a kezelt személyes adatok vonatkozásában Adatfeldolgozó, akkor az észlelést (bejelentést) követően a lehető leghamarább, indokolatlan késedelem nélkül az incidenst az adott személyes adatok vonatkozásában jelenteni kell az Adatkezelőnek.

3.4. Amennyiben az Adatkezelő a kezelt személyes adatok vonatkozásában Adatkezelő, akkor az észlelést (bejelentést) követően a lehető leghamarább, indokolatlan késedelem nélkül, de legkésőbb 72 órán belül az **incidenst jelenteni kell a Nemzeti Adatvédelmi és Információszabadság Hatóságnak** (továbbiakban: NAIH/Hatóságnak), kivéve, ha az adatvédelmi incidens nem érint személyes adatokat, valószínűsíthetően nem jár kockázattal, nincs különféle, jelentős hátrányos hatásai a természetes személyek jogaira és szabadságára nézve. A bejelentést a NAIH honlapján (https://naih.hu/adatvedelmi-incidensbejelento-rendszer) elektronikusan vagy papír alapon kell megtenni.

A NAIH-nak történő incidens bejelentésnek minimum a következő adatokat kell tartalmaznia:

- az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát,
- az incidenssel érintett adatok kategóriáit és hozzávetőleges számát,
- az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit,
- az adatvédelmi incidensből eredő, valószínűsíthető következményeket,
- az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

Amennyiben az adatkezelési incidens első bejelentésekor még az incidensre és annak megoldására vonatkozó összes adat még nem áll rendelkezésre, úgy az első bejelentéskor a rendelkezésre álló adatokat kell bejelenteni, valamint a többi adatot azok rendelkezésre állásának ütemében, de indokolatlan késedelem nélkül pótlólag kell a Hatóságnak bejelenteni.

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

3.5. Amennyiben az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatkezelőnek indokolatlan késedelem nélkül, világos és közérthető megfogalmazásban, közvetlenül **tájékoztatni kell az érintettet** az adatvédelmi incidensről.

3.5.1. Az Adatkezelő általi érintetteknek történő incidens bejelentésnek minimum a következő adatokat kell tartalmaznia:

- az adatvédelmi incidens jellegét,
- az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit,
- az adatvédelmi incidensből eredő, valószínűsíthető következményeket,
- az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

Arról is tájékoztatni kell az érintettet, hogy hogyan tud védekezni a lehetséges hátrányos következményekkel szemben. (Pl.: ha a jelszót lopnak el, akkor a jelszó megváltoztatásának szükségességéről.)

Azonban amennyiben a tájékoztatás aránytalan erőfeszítést tenne szükségessé, az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, vagy olyan hasonló intézkedést kell hozni, amely biztosítja az érintettek hasonlóan hatékony tájékoztatását.

3.5.2. Nem kell az érintettet tájékoztatni, ha olyan technikai, szervezési, védelmi intézkedéseket hajtott végre az Adatkezelő az érintett adatokra vonatkozóan, amelyek megakadályozzák az illetéktelen személyek számára való hozzáférést az adatokhoz vagy megakadályozzák az adatok értelmezhetőségét. Továbbá, ha az adatvédelmi incidenst követően olyan intézkedések történtek, amelyek biztosítják, hogy a feltárt adatkezelési kockázat valószínűsíthetően nem valósul meg.

3.6. Amennyiben az incidens informatikai eszközzel, erőforrással kapcsolatban hozható, akkor az informatikai csoportvezető, a rendszergazda és az adatvédelmi tisztviselő további feladatai:

3.6.1. A bejelentett adatvédelmi incidens nyugtázása, az incidenssel kapcsolatos további adatok, információk begyűjtése.

3.6.2. Adatvédelmi incidens hatásának vagy potenciális hatásának elemzése, meghatározása a FÁNK, illetve az érintettek jogai szempontjából.

3.6.3. Szükség esetén azonnali eszkalálás, válságkezelési terv elindítása.

3.6.4. A megtámadott információs rendszer, szolgáltatás és/vagy hálózat elkülönítésének és lekapcsolásának lehetővé tétele.

3.6.5. Az üzleti szempontból kritikus szolgáltatások, rendszerek helyes működésének biztosítása.

3.6.6. A kapcsolódó folyamatok / tevékenységek felelőseinek értesítése az incidensről.

3.6.7. Az incidens hatását, és az incidenskezelés módját, lépéseit meghatározó szakértői team összehívása. Feladatuk az incidenssel kapcsolatos minden információ felderítése, bizonyítékok további gyűjtése, majd a szükséges technikai és szervezési intézkedések meghatározása és foganatosítása.

3.6.8. A feltárt eredmények naplózása, dokumentálása az Adatvédelmi incidensek nyilvántartásában.

3.6.9. Az adatvédelmi incidens kiértékelésének eredményéről tájékoztatni kell a Főigazgatót szükség esetén a Hatóságot.

4. ADATVÉDELMI INCIDENS NYILVÁNTARTÁSA

Az adatvédelmi incidensről nyilvántartást kell vezetni, amely tartalmazza:

- az érintett személyes adatok köre,
- az adatvédelmi incidenssel érintettek körét és számát,
- az adatvédelmi incidens időpontja,
- az adatvédelmi incidens körülményeit, hatásait,
- az adatvédelmi incidens orvoslására megtett intézkedéseket,
- az adatkezelést előíró jogszabályban meghatározott egyéb adat.

A nyilvántartásban szereplő adatvédelmi incidensre vonatkozó adatok megőrzési ideje:

- személyes adatokat érintő incidens esetében 5 év,
- különleges adatokat érintő incidens esetén 20 év.

A nyilvántartásban adatvédelmi incidenssel érintett személy személyes adata nem szerepelhet. Az adatvédelmi incidens nyilvántartását az adatvédelmi tisztviselő, távollétében az informatikai csoportvezető vezeti.

5. TECHNIKAI ÉS SZERVEZÉSI INTÉZKEDÉSEK

Az adatkezelő a tudomány és technológia állása, a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és célja, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja.

A szükséges és megfelelő, komplex információbiztonsági szintet a következő intézkedések/szabályozó eszközök biztosítják a bizalmasság, sértetlenség és rendelkezésre állás tekintetében:

- komplex fizikai védelmi intézkedések,

- komplex adminisztratív és technikai védelmi intézkedések és szabályozók (informatikai biztonsági stratégia és politika, informatikai biztonsági szabályzat, belső adatvédelmi szabályzat),

- folyamatos kockázat feltárás és elemzés eredménye alapján a mindenkori védelmi intézkedések zárt, teljes körű, folytonos és a kockázattal arányos beavatkozási rendszere,

- a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítása, integritása, rendelkezésre állása és ellenálló képessége,

- az adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedések hatékonyságának rendszeres tesztelése, felmérése és értékelése,

- megfelelő erőforrás biztosítása,

- személyi biztonsági intézkedések,

- képzés, tudatosítás

6. ZÁRÓ RENDELKEZÉS

Jelen Szabályzat 2021. május 10. napján lép hatályba, ezzel egyidejűleg a 2019. március 12. napján hatályba lépett Adatvédelmi incidens kezelésének szabályzata hatályát veszti.

Mellékletek:

1. számú Adatvédelmi incidens nyilvántartás

Budapest, 2021. május 10.

Szabó Roland

operatív igazgató

1. számú melléklet

Fővárosi Állat- és Növénykert

ADATVÉDELMI INCIDENS NYILVÁNTARTÁS

Belső felelős: Adatvédelmi tisztviselő, Informatikai csoportvezető

Ssz.	Érintett személyek (köre, száma)	Incidenssel érintett személyes adatok	Incidens leírása, jellege, oka	Incidens időpontja	Incidens mértéke, hatása, következményei	Intézkedés