INCIDENSKEZELÉSI SZABÁLYZAT

Magyar Igazságügyi Szakértői Kamara

2.0 verzió

2022 április

Tartalomjegyzék

I. Incidenskezelése és nyilvántartása

A Magyar Igazságügyi Szakértői Kamara (a továbbiakban: Adatkezelő) az Európai Parlament és a Tanács 2016. április 27-i (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (továbbiakban: GDPR), valamint az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) alapján a tevékenysége során zajló incidenskezelés rendjét az alábbiak szerint határozza meg.

A GDPR értelmében azadatvédelmi incidens alatt a biztonság olyan sérülését értjük, 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.

II. Az Incidenskezelési Szabályzat hatálya

<u>A Szabályzat személyi hatálya</u>
A Szabályzat személyi hatálya kiterjed az Adatkezelővel jogviszonyban álló minden foglalkoztatottra, illetve munkavégzésre irányuló egyéb jogviszonyban álló (alvállalkozók, beszállítók, foglalkoztatásra pályázók, ügyfelek, szerződéses partnerek) természetes személyre, valamint a gazdasági társaságmegbízásából szerződés alapján adatfeldolgozói feladatokat ellátó partnerére.

<u>A Szabályzat tárgyi hatálya</u>
A Szabályzat tárgyi hatálya kiterjed az Adatkezelővel folytatott valamennyi papír alapú és elektronikus adatkezelésre.

<u>A szabályzat időbeli hatálya</u>
Módosításig, illetve visszavonásig.

III. Adatvédelmi tisztviselő tevékenységének szabályai

Az Adatkezelő adatvédelmi tisztviselője megbízási jogviszonyban látja el az adatvédelemmel kapcsolatos feladatait. Az Adatkezelő biztosítja, hogy az adatvédelmi tisztviselő a személyes adatok védelmével kapcsolatos összes ügyben megfelelő módon és időben bekapcsolódjon, az adatkezelési folyamatokra rálásson.

<u>Az adatvédelmi tisztviselő feladatai</u>

- Az adatvédelmi tisztviselő tájékoztat és szakmai tanácsot ad az Adatkezelő vagy az Adatfeldolgozó, továbbá az adatkezelést végző alkalmazottak részére a GDPR, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezések szerinti kötelezettségeikkel kapcsolatban.

- Ellenőrzi a GDPR-nak, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezéseknek, továbbá az Adatkezelő vagy az Adatfeldolgozó személyes adatok védelmével kapcsolatos belső szabályainak való megfelelést, ideértve a feladatkörök kijelölését, az adatkezelési műveletekben vevő személyzet tudatosság-növelését, képzésének- és a kapcsolódó auditok megszervezését.
- Szükség szerint szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomon követi a hatásvizsgálatnak a GDPR35. cikke szerinti elvégzését.
- Együttműködik a felügyeleti hatósággal az adatkezeléssel összefüggő ügyekben – ideértve a GDPR36. cikkében említett előzetes konzultációt is – kapcsolattartó pontként szolgál a felügyeleti hatóság felé, valamint adott esetben bármely egyéb kérdésben konzultációt folytat vele.

Az adatvédelmi tisztviselő – e megbízatása vonatkozásában - feladatait az adatkezelési műveletekhez fűződő kockázat megfelelő figyelembevételével, az adatkezelés jellegére, hatókörére, körülményére és céljára is tekintettel végzi. Adatvédelemmel összefüggő feladataiban véleményezési és javaslattételi joga van, felelőssége kizárólag erre irányul.

IV. Adatvédelmi incidens nyilvántartás vezetése

Az adatkezelő a rendelet 33. cikk (5) bekezdésnek megfelelően tartja nyilván az incidenseket. A nyilvántartás minden mezője a felügyeleti hatóság (NAIH) online bejelentőjének megfelelő struktúrában kerül nyilvántartásra. Az adatkezelő 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 az e cikk követelményeinek való megfelelést.”

Nyilvántartás nyilvántartott adatai:

0. Adatvédelmi incidens jelentése

- Bejelentés típusa
- A korábban bejelentett incidens azonosítója
- A korábbi bejelentés időpontja

1. A bejelentő adatai

1.1 Kapcsolati

- A bejelentő adatkezelő cégjegyzékszáma
- A bejelentő adatkezelő adószáma (magánszemély bejelentése esetén nem kell)
- Szervezet száma
- A bejelentő adatkezelő elnevezése
- Az incidenssel érintett igazgatási/szervezeti egység megnevezése és elérhetőségei
- A bejelentő adatkezelő címe és egyéb elérhetőségei
- A bejelentő természetes személy neve és beosztása
- A bejelentő természetes személy elérhetőségei
- Az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó neve és beosztása
- Az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó email elérhetősége
- Az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó telefonszáma

- Az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó levelezési címe
- Az adatkezelő az alábbiak közül melyik szektorba tartozik

1.2 Az adatkezelőn kívüli felek részvétele az adatvédelmi incidenssel érintett szolgáltatásban

- Az adatkezelőn kívül részt vesz-e más személy/szervezet az adatvédelmi incidenssel érintett adatkezelés folyamatában?
- Az adatkezelőn kívüli fél megnevezése és minősége

2. Időpontok

- Adatvédelmi incidens időpontja
- Adatvédelmi incidens kezdő időpontja
- Adatvédelmi incidens záró időpontja
- Az adatvédelmi incidens továbbra is fennáll
- Az incidensről való tudomásszerzés időpontja
- Az incidens észlelésének módja
- Az adatfeldolgozó általi értesítés időpontja
- A késedelmes tájékoztatás indokai
- Egyéb megjegyzések az incidens időpontját érintően

3. Az adatvédelmi incidensről

- Bizalmas jelleg
- Integritás
- Rendelkezésre állás
- Adatvédelmi incidens jellege (több válasz is elfogadható)
- Egyéb megjegyzés az adatvédelmi incidens részletes leírásához
- Adatvédelmi incidens okai (több válasz is elfogadható)
- Adatvédelmi incidens egyéb okainak leírása

4. Az adatvédelmi incidenssel érintett személyes adatok

4.1 Személyes adatok

- Személyazonossághoz kapcsolódó adatok
- Személyi szám
- Elérhetőségi adatok
- Azonosító adatok
- Gazdasági, pénzügyi adatok
- Képfelvétel
- Hangfelvétel
- Hivatalos okmányok
- Helymeghatározó adatok
- Biometrikus adatok
- Büntetett előélettel, bűncselekményekkel vagy büntetéssel, intézkedéssel kapcsolatos adatok

4.2 Különleges adatok

- Faji eredetre, nemzetiséghez tartozásra vonatkozó adatok
- Politikai véleményre vonatkozó adatok

- Vallásos vagy más világnézeti meggyőződésre vonatkozó adatok
- Érdek-képviseleti szervezeti tagságra vonatkozó adatok
- Szexuális életre vonatkozó adatok
- Egészségügyi adatok
- Genetikai adatok
- Még nem ismert
- Egyéb
- Az egyéb személyes adatok leírása
- Az adatvédelmi incidenssel érintett személyes adatok becsült száma

5. Az érintettek

- Alkalmazottak
- Felhasználók
- Feliratkozók
- Diákok
- Katonai állomány tagjai
- Ügyfelek (jelenlegi és potenciális)
- Páciensek
- Kiskorúak
- Kiszolgáltatott személyek
- Hatósági eljárás vagy intézkedés alá vont, vagy azok által érintett személyek
- Még nem ismert
- Egyéb
- Az egyéb leírása
- Az incidenssel érintett adatalanyok részletes leírása
- Az adatvédelmi incidenssel érintettek becsült száma

6. Az incidens ELŐTT alkalmazott intézkedések

- Az adatvédelmi incidens előtt alkalmazott intézkedések leírása

7. Következmények

7.1 Bizalmas jelleg sérülése

- Szélesebb körű hozzáférés, mint ami szükséges, vagy amihez az érintett hozzájárult
- Az adat összekapcsolhatóvá vált az érintett egyéb adatával
- Az adatot más célokból történő, tisztességtelen módon történő kezelése lehetséges
- Egyéb
- Az egyéb bizalmas jelleget érintő következmény leírása

7.2 Intergritás sérülése

- Az adat módosíthatóvá vált annak ellenére, hogy archivált elavult adat volt
- Az adatot valószínűsíthetően módosították egyébként pontos adatokra, és azokat eltérő célokra használhatták
- Egyéb
- Az egyéb integritást érintő következmény leírása

7.3 Rendelkezésre állás sérülése

- Az érintettek számára történő kritikus szolgáltatásnyújtás képességének elvesztése
- Az érintettek számára történő kritikus szolgáltatásnyújtás képességének módosulása
- Egyéb
- Az egyéb rendelkezésre állást érintő következmény leírása

7.4 Az érintetteket ért fizikai, anyagi vagy nem vagyoni károk, vagy egyéb jelentős következmények

- Az incidens valószínűsíthető hatásai az érintettekre
- Az egyéb valószínűsíthető hatások leírása
- A valószínűsíthető következmények súlyossága

8. Megtett intézkedések

8.1 Érintettek tájékoztatása

- Érintettek tájékoztatása
- Tájékoztatás időpontja („a" válasz esetén)
- Tájékoztatás tervezett időpontja („b" válasz esetén)
- A tájékoztatás tervezett időpontja még nincs eldöntve („b" válasz esetén
- Tájékoztatás hiányának indokai („c" válasz esetén)
- Intézkedések leírása, amelyek alapján az érintettek tájékoztatására nem került sor („c" válasz esetén)
- Tájékoztatott érintettek száma („a" válasz esetén)
- Az érintett tájékoztatásának formája („a" válasz esetén)
- Az érintetteknek szóló tájékoztatás tartalma („a" válasz esetén)
- Nyilvánosan közzétett információk, vagy hasonló intézkedés („c" illetve „III" válasz esetén)

8.2 Az adatvédelmi incidens orvoslására tett intézkedések

- Az adatkezelő által az adatvédelmi incidens orvoslására tett intézkedések

8.3 Egyéb bejelentések

- A vezető hatóságnak bejelentett határokon átnyúló adatvédelmi incidens
- Az EU felügyeleti hatóságok listája, amelyeket az adatvédelmi incidens érinthet (több válasz is elfogadható)
- Az adatkezelő bejelentette-e, vagy be fogja-e jelenteni az adatvédelmi incidenst közvetlenül más tagállam felügyeleti hatóságának?
- Az EU felügyeleti hatóságok listája, amelyeknek az adatkezelő közvetlenül bejelentette-e, vagy be fogja-e jelenteni az adatvédelmi incidenst (több válasz is elfogadható)
- Bejelentette-, vagy be fogja-e jelenteni az adatkezelő az adatvédelmi incidenst másik EGT-tagállam olyan adatkezelőjének, amely részére az incidenssel érintett adatokat korábban továbbította, vagy amely adatkezelő az incidenssel érintett adatokat részére átadta?
- Azon más EGT-tagállami adatkezelő megnevezése és elérhetőségei, amelynek az incidenst bejelentette vagy be fogja jelenteni.
- Bejelentette-e, vagy be fogja-e jelenteni az adatkezelő az adatvédelmi incidenst EU-n kívüli adatvédelmi hatóságnak?
- Az EU-n kívüli felügyeleti hatóságok listája, amelyeknek az adatvédelmi incidenst bejelentette, vagy be fogja jelenteni az adatkezelő

- Bejelentette-, vagy be fogja-e jelenteni az adatkezelő az adatvédelmi incidenst egyéb EU-s hatóságnak egyéb jogszabály alapján fennálló kötelezettség alapján? (NIS Irányelv, eIDAS Rendelet)?
- Egyéb EU hatóságok listája, amelyeknek az adatvédelmi incidenst bejelentette vagy be fogja jelenteni az adatkezelő.

V. Adatvédelmi incidens során alkalmazandó eljárásrend

- Az Adatkezelő (illetve az adatkezelővel munkavégzésre irányuló jogviszonyban álló személy), Adatfeldolgozó által észlelt vagy saját hatáskörükben megállapított adatvédelmi, információ biztonsági incidens esetében azonnal tájékoztatja adatvédelemért felelős személyt.
- Azadatvédelemért felelős személy a számára jelzett, vagy saját hatáskörükben megállapított adatvédelmi incidens felderítése és súlyosságának megállapítása érdekében a következők szerint köteles eljárni:
    - megállapítja az incidens jellegét (elektronikus adatokat, papír alapú adatokat, elektronikus és papír alapú adatokat is érint-e)
    - eldönti az incidens kezelésének megkezdése során tájékoztatandó személyek összetételét
    - tájékoztatja az Adatkezelő ügyvezetőjét a bevonásukig meghozott intézkedéseiről, és a tervezett további lépésekről.

Az adatvédelemért felelős személynek a felderítés során az alábbi kategóriák valamelyikébe kell az adatvédelmi incidenst sorolni:

- **Alacsony szintű adatvédelmi incidens**: a személyes adatok elhanyagolható körének jogosulatlan továbbítása, megváltoztatása, nyilvánosságra hozatala, szándékolt, vagy véletlen törlése vagy megsemmisítése, vagy más jogellenes adatkezelési eset esetén.
- **Közepes szintű adatvédelmi incidens**: a személyes adatok csekély körének megváltoztatása, jogosulatlan továbbítása, nyilvánosságra hozatala, szándékolt, vagy véletlen törlése vagy megsemmisítése, vagy más jogellenes adatkezelési eset esetén.
- **Magas szintű adatvédelmi incidens**:
    - a személyes adatok széles körének jogosulatlan megváltoztatása, továbbítása, nyilvánosságra hozatala, szándékolt, vagy véletlen törlése, megsemmisítése, vagy más jogellenes adatkezelési eset esetén, illetve
    - az adatok körétől függetlenül minden olyan eset, amikor az incidensnek az érintettre hátrányos hatása valószínűsíthető, vagy a hátrányos következmény bekövetkezés mértéke biztos.

<u>Alacsony szintű adatvédelmi incidens esetén követendő eljárás</u>

Az adatvédelemért felelős személy haladéktalanul, de legkésőbb 12 órán belül megteszi az alábbi lépéseket:

- amennyiben az incidens informatikai rendszert is érint, az érintett rendszer rendszergazdájával meghatározza az adatvédelmi incidens kezelésének módját és felhívja az intézkedésre jogosult személyt az incidens kezelésére,

- amennyiben az incidens informatikai rendszert nem érint, meghatározza az adatvédelmi incidens kezelésének módját és felhívja az intézkedésre jogosult személyt az incidens kezelésére,
- rögzíti az adatvédelmi incidenst az incidensek nyilvántartásába,
- tájékoztatja az Adatkezelő ügyvezetőjét az incidens kezelés során megtett intézkedésekről és elvégzett nyilvántartási bejegyzésekről.

Közepes szintű adatvédelmi incidens esetén követendő eljárás

- Az adatvédelemért felelős (adatvédelmi tisztviselő) személy haladéktalanul, de legkésőbb 12 órán belül munkacsoportot összehívását kezdeményezi, amelyben részt vesz
  - *az Adatkezelő ügyvezetője, vagy az általa delegált személy,*
  - *az incidens által érintett terület vezetője/felelőse,*
  - *szükség esetén az incidens által érintett adatfeldolgozó kijelölt munkatársa,*
  - *informatikai rendszert vagy információbiztonsági kérdést is érintő esetekben azinformatikai biztonságért felelős személy (rendszergazda)*
- a munkacsoport meghatározza az adatvédelmi incidens kezelésének módját, dönt a felügyeleti hatóság felé történő bejelentésről.
- tájékoztatja az intézkedésre jogosult személyt/személyeket az incidens kezelése során elvégzendő feladatairól, a visszacsatolás határidejéről,
- az adatvédelemért felelős személy rögzíti az adatvédelmi incidenst az incidensek nyilvántartásában.

Magas szintű adatvédelmi incidens esetén

- Az adatvédelemért felelős(adatvédelmi tisztviselő) személy haladéktalanul, de legkésőbb 12 órán belül munkacsoport összehívását kezdeményezi, amelyben részt vesz
  - *az Adatkezelő ügyvezetője, vagy az általa delegált személy,*
  - *az incidens által érintett terület vezetője/felelőse,*
  - *szükség esetén az incidens által érintett adatfeldolgozó kijelölt munkatársa,*
  - *informatikai rendszert vagy információbiztonsági kérdést is érintő esetekben az informatikai biztonságért felelős személy (rendszergazda)*
- a munkacsoport meghatározza az adatvédelmi incidens kezelésének módját
- amennyiben szükséges, meghatározza az érintettek értesítésének módját, az értesítés tartalmát és gondoskodik az érintettek haladéktalan értesítéséről.
- tájékoztatja az intézkedésre jogosult személyt/személyeket a munkacsoport által meghozott döntésekről és az incidens kezelése során elvégzendő feladatairól, a visszacsatolás határidejéről,
- az adatvédelemért felelős személy rögzíti az adatvédelmi incidenst az incidensek nyilvántartásában.
- az adatvédelmi tisztviselő jóváhagyásával megtörténik a felügyeleti hatóság tájékoztatása az online bejelentőrendszeren keresztül.
- az adatvédelmi tisztviselő felveszi a kapcsolatot a felügyeleti hatósággal, konzultációt folytat a megtett intézkedésekről és további teendőkről.

Az incidenskezelés (GDPR-ben meghatározott) általános protokollja

Ha az Adatkezelő tudomására jut az adatvédelmi incidens, indokolatlan késedelem nélkül, - ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott - bejelenteni köteles azt az illetékes felügyeleti hatóságnál, kivéve, ha az elszámoltathatóság elvével összhangban bizonyítani tudja, hogy az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Ha a bejelentés 72 órán belül nem tehető meg, a bejelentésben meg kell jelölni a késedelem okát, az előírt információkat pedig – további indokolatlan késedelem nélkül – részletekben is közölni lehet.

Az adatvédelmi incidensről szóló bejelentésben:
A bejelentés tartalmát az incidens nyilvántartás rögzíti, többek között:
- ismertetni kell az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát;
- közölni kell az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;
- ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket;
- 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.

VI. Az adatvédelmi incidensek típusai

a) Bizalmasságiincidensek

A személyes adatok véletlen vagy felhatalmazás nélküli közlése, vagy az ezekhez valóhozzáférés.

- Személyes adatokat tartalmazó postai vagy elektronikus küldeményeknek nem a címzett részére történő megküldése;
- Személyes adatokat kezelő informatikai eszközök közötti váltás (pl.: adatmigráció miatt a korábbi adatok hozzáférhetetlensége);
- A személyes adatok nem megfelelő megsemmisítése (pl.: a személyes adatokat tartalmazó adattárolók, illetve papír alapú dokumentumok anélkül kerülnek illetéktelen személy részére továbbításra, vagy megsemmisítésre, hogy a személyes adatok vissza nem állítható módon törlésre kerülnének);
- A munkaviszony megszűnése kapcsán felmerülő incidensek (pl.: a kilépő munkavállaló személyes adatainak a munkaviszony megszűnését követően történő, cél nélküli kezelése);
- Az informatikai rendszer külső támadása okozta adatvédelmi incidensek (pl.: hackertámadás);
- Vírusok, vagy egyéb biztonság elleni támadások az informatikai eszközrendszereken, vagy hálózatokon;
- Bizalmas adatok (pl.: üzleti titok, banktitok) illetéktelen személy számára történő hozzáférhetővé tétele, vagy bizalmas adatokat tartalmazó dokumentumok bárki által hozzáférhető helyen hagyása (pl.: fénymásolóban hagyott dokumentumok)
- Nem megfelelő jogosultsági, hozzáférési beállítások, amelyek következtében az adatokat hozzáférési joggal nem rendelkező felhasználók is kezelhetik;
- A fizikai biztonság sérelme (pl.: zárt biztonsági szobába, vagy irattárba történő behatolás)

- Az informatikai eszközök őrizetlenül hagyása (pl.: a felhasználói fiók zárolása nélkül történő távozás a munkaállomásról, amelynek következtében a felhasználó számítógépén tárolt adatokhoz bárki hozzáférhet);

b) Sértetlenséggel kapcsolatos incidens

A személyes adatok véletlen vagy jogtalanmegváltoztatása.

- Az informatikai rendszer külső támadása okozta adatvédelmi incidensek (pl.: hackertámadás);
- Vírusok, vagy egyéb biztonság elleni támadások az informatikai eszközrendszereken, vagy hálózatokon;
- Papír alapú adatkezelés tekintetében az eredeti bizonyító erővel rendelkező dokumentumok elvesztése;
- Papír alapú adatkezelés tekintetében az eredeti bizonyító erővel rendelkező dokumentumok megsemmisülése, sérülése;

c) Hozzáférhetőséggel kapcsolatos incidens

A személyes adatok véletlen, vagy jogtalan megsemmisítése, elvesztése.

- Számítógépes eszközök (ideértve a hordozható, vagy egyéb eszközöket), adattárolás céljára szolgáló eszközök, valamint a személyes adatot tartalmazó papír alapú dokumentumok elvesztése;
- Az informatikai rendszer külső támadása okozta adatvédelmi incidensek (pl.: hackertámadás);
- Vírusok, vagy egyéb biztonság elleni támadások az informatikai eszközrendszereken, vagy hálózatokon;
- Bizalmas adatok (pl.: üzleti titok, banktitok) illetéktelen személy számára történő hozzáférhetővé tétele, vagy bizalmas adatokat tartalmazó dokumentumok bárki által hozzáférhető helyen hagyása (pl.: fénymásolóban hagyott dokumentumok)

VII. Az incidens-nyilvántartásba bevezetendő incidensek

Általános:

- Olyan eszközök elvesztése, ellopása (laptop, mobiltelefon, pendrive, cd, dvd, egyéb adathordozó), amelyeken ügyfél adatok, személyes adatok találhatóak.
- Ha valaki papíralapú dokumentumokat veszít el.
- Ha olyan driverre kerül adat feltöltésre, amelynek a szervere harmadik országban lehet.

Postai és e-postai küldemények:

- Ha egy adott érintettnek küldött postai küldeményben/elektronikus levélben egy másik ügy iratai belekerülnek (pl. ügyintéző összefogta, véletlenül rossz mellékletet csatol).
- A felszólító levél más személy – nem a címezett – adatait tartalmazza.
- Ha valaki személyes adatokat küld harmadik országbeli és nem EU irányelvek alapján működő szerverre (pl. yahoo.com), kivéve, ha a címzett konkrétan ide kéri, de akkor is csak és kizárólag az kérheti, akié a személyes adat.
- Ha valaki tömeges személyes adatot továbbít tömörítetlen formában.

Tájékoztatás:

- Ügyintézői hibából, vagy a telefonáló személy rosszhiszemű magatartása miatt nem az adott ügyben jogosult személy kerül tájékoztatásra az ügy adatairól telefonon, személyesen, hanem megfelelő meghatalmazással nem rendelkező másik személy (pl. családtag, ismerős).
- Ha névazonosság áll fenn, és születési hely, -idő, anyja neve adatok hiányában történt beazonosítás, de később kiderül, hogy nem az érintettel, hanem az ugyanolyan nevű más személlyel egyeztetett/kezdte meg az egyeztetést a munkatárs.
- Harmadik fél – meghatalmazás nélkül, vagy nem megfelelő azonosítással – járt el (többször) az érintett nevében, (akár az ügyfél tudomásával).

Informatikai adatvédelmi incidens:

- Vírustámadás érte a felhasználót.
- Ha az Adatkezelő szándékától és akaratától függetlenül megváltozott a weboldal akár formai, akár tartalmi elemet tekintve.
- Ha olyan adattároló ment tönkre, amelyen személyes adat volt.
- Arra jogosulatlan fért hozzá a tárolt személyes adatokhoz.
- Ha a weboldal vagy az adatbázis elérhetetlensége meghaladja az egyórát (a szolgáltatói oldalon).
- Ha az adatok sérültek, vagy törlődtek és mentésből történő visszatölt következett be.

VIII. Hatálybalépés

Jelen szabályzat az aláírás napján lép hatályba.

A jelen szabályzatban nem szabályozott kérdések tekintetében a GDPR és az Infotv. rendelkezései az irányadóak.

Budapest, 2022. április 30.

Dr. Borka Zoltán
főtitkár