ADATKEZELÉSI SZABÁLYZAT

Ficsor Zoltán igazságügyi szakértő (4NSIC Szakértői Iroda Kft.)

Készítette: Ficsor Zoltán

Tartalomjegyzék

Az Európai Parlament és a Tanács (EU) 2016/679 Rendelete, az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) alapján az igazságügyi szakértő tevékenysége során zajló adatkezelés rendjéről

Adatkezelési szabályzat célja

Adatvédelmi Szabályzatának (a továbbiakban: Szabályzat) célja, hogy

- meghatározza a természetes személyként végzett igazságügyi szakértői tevékenység által kezelt adatok adatkezelés céljait és az egyes céloknak megfelelően rendelje a célokhoz az adatkezelés jogalapját és az egyes adatok kezelésének időkorlátait. Megbízható alapja legyen a természetes személyek tájékoztató anyagainak, illetve biztosítsa a természetes személyek jogait a róluk tárolt adatok tekintetében,
- az igazságügyi szakértői tevékenységhez kapcsolódó feladatok teljesítéséhez, valamint a nyilvántartások vezetéséhez kapcsolódóan meghatározza a *természetes személynél alkalmazandó* irat és adatkezelés rendjét,
- biztosítsa az Uniós adatvédelmi rendelet (a továbbiakban: GDPR), valamint a tagállami jogi szabályozás, így az Alaptörvényben, az Infotv.-ben meghatározott érintetti, adatkezelői, adatfeldolgozói, címzetti jogokat és kötelezettségeket.

Általános szabályok

A szabályzat személyi hatálya

A mikrogazdasági társaságként végzett igazságügyi szakértői tevékenységből eredő adatkezelésekre.

A szabályzat tárgyi hatálya

A szabályzat tárgyi hatálya kiterjed a igazságügyi szakértői tevékenység*nél* folytatott valamennyi papír alapú és elektronikus adatkezelésre.

A szabályzat időbeli hatálya

Visszavonásig.

Értelmező fogalom-meghatározások

Személyes adat: 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;
Adatkezelés: a személyes adatokon, vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége;
Az adatkezelés korlátozása: a tárolt személyes adatok megjelölése jövőbeli kezelésük korlátozása céljából;
Adatkezelő: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza; ha az adatkezelés céljait és eszközeit az uniós vagy a tagállami jog határozza meg, az adatkezelőt vagy az adatkezelő kijelölésére vonatkozó különös szempontokat az uniós vagy a tagállami jog is meghatározhatja;
Adatfeldolgozó: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel;
Címzett: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, akivel, vagy amellyel a személyes adatot közlik, függetlenül attól, hogy harmadik fél-e;
Az érintett hozzájárulása: az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez;
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;
Felügyeleti hatóság: egy tagállam által a GDPR 51. cikknek megfelelően létrehozott független közhatalmi szerv;
Érintett felügyeleti hatóság: az a felügyeleti hatóság, amelyet a személyes adatok kezelése a következő okok valamelyike alapján érint:

1. a) az adatkezelő vagy az adatfeldolgozó az említett felügyeleti hatóság tagállamának területén rendelkezik tevékenységi hellyel;
2. b) az adatkezelés jelentős mértékben érinti vagy valószínűsíthetően jelentős mértékben érinti a felügyeleti hatóság tagállamában lakóhellyel rendelkező érintetteket; vagy
3. c) panaszt nyújtottak be az említett felügyeleti hatósághoz.

Általános elvek

Elszámoltathatóság
A természetes személyként végzett igazságügyi szakértő, mint adatkezelő a felelős a GDPR 5. cikk 1. bekezdésben meghatározott elvek megvalósulásáért, mint adatkezelőnek, képesnek kell lennie a megfelelés igazolására.

Jogszerűség, tisztességes eljárás és átláthatóság
A személyes adatok kezelését jogszerűen és tisztességesen, valamint az érintettek számára átláthatóan kell végezni, biztosítva az érintetti jogok gyakorlásának zökkenőmentes megvalósulását.

Célhoz kötöttség
A személyes adatok gyűjtése tekintetében csak meghatározott, egyértelmű és jogszerű céllal tárol adatokat, és nem kezel adatokat a célokkal nem összeegyeztethető módon.

Adattakarékosság
Csak a célok eléréséhez szükséges és feltétlenül szükséges adatokat kezeli.

Pontosság
A tárolt adatoknak az észszerűség határain belül pontosnak, naprakésznek kell lenni.

Korlátozott tárolhatóság
A személyes adattárolást a szaktörvénynek megfelelő ideig kezeli és tárolja

Integritás, bizalmasság
Az Adatkezelő biztosítja a személyes adatok megfelelő biztonságos tárolását és kezelését, ugyanakkor gátolja a jogosulatlan vagy jogellenes kezelést, a véletlen elvesztést, vagy megsemmisítést.

Jogalapok

Hozzájárulás
Az érintett a hozzájárulását adta személyes adatainak egy, vagy több konkrét célból történő kezeléséhez.

Szerződésen alapuló
Az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél, vagy az a szerződés megkötését megelőzően, az érintett kérésére történő lépések megtételéhez szükséges.

Jogi szabályozásra visszavezethető

Az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges, az ez alapján tárolt személyes adatok tárolására, kezelésére vonatkozóan a jogi környezet változását a szabályozásban követni kell, és szükség esetén a jogalap változásról az érintetteket tájékoztatja az adatkezelő.

Adatkezelő vagy harmadik fél jogos érdeke
Az adatkezelés az adatkezelő, vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei, vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé, különösen, ha az érintett gyermek.

Érintettek jogai:
Az igazságügyi szakértő *biztosítja az Érintettnek, hogy az általa* kezelt Érintetti adataival kapcsolatban élhessen az Uniós rendeletben és a tagállami szabályozásban meghatározott jogaival.

Hozzájárulás (visszavonás)
Amennyiben bármely érintett esetében a hozzájárulás jogalapján az érintett élni kíván a visszavonás, vagy ismételt hozzájárulás jogával, biztosítani kell.

Hozzáférés joga (betekintés)
Az igazságügyi szakértő biztosítja az általa kezelt adataihoz az Érintett hozzáférjen. Az elektronikus tájékoztatás ingyenes, ha a tájékoztatást kérő az adott naptári évben azonos adatkezelésre vonatkozó tájékoztatási kérelmet még nem nyújtott be. Minden egyéb esetben a ráfordítással arányos költségtérítést állapíthat meg az adatkezelő.

Helyesbítés joga, és kötelezettsége
Az érintett tájékoztatást kérhet az igazságügyi szakértőtől az érintett kérheti a személyes adatainak helyesbítését.

Törlés, felejtés joga
Az érintett kérheti adatainak törlését, felejtését, a jogszabályi környezetben meghatározott feltételek fennállásának kötelező adatkezelés előírásait kivéve.

Adatkezelés korlátozásának joga
Az érintett kérheti kezelt adatainak adatkezelési korlátozását a jogszabályi környezetben meghatározott feltételek fennállásának esetében, kötelező adatkezelés előírásait kivéve. Ebben az esetben az adatok tárolása továbbra is fenn ál, de az adatkezelés nem valósulhat meg.

Adathordozhatóság joga
Egy példány ingyenes, de az adatkezelő felmerült költséget felszámolhat.

Tiltakozás joga

Az érintett jogainak gyakorlása tekintetében csak a közérdekű feladat kezelése és az adatkezelő által jogos érdekké minősített jogalappal rendelkező adatkezelés (továbbítása) ellen élhet tiltakozással.

Érintettek tájékoztatása

Az érintettet az adatkezelés megkezdése előtt tájékoztatni kell az Infotv. 20.§-ában foglaltak szerint. Ez a tájékoztatás egyénileg írásban, valamint az igazságügyi szakértő honlapján található „adatkezelés" menüpontban elhelyezett tájékoztató formájában is megtehető.

Az igazságügyi szakértő tevékenységével összefüggő adatkezelési folyamatai

Szakértő kirendelésének folyamata

Az igazságügyi szakértőt felkérheti magánszemély, jogi személy, illetve a különböző hatóságok is kirendelhetik. A kirendelés vagy megrendelés célja a felkérésben rögzített kérdés, illetve kérdések megválaszolása. A kirendelés vagy megrendelés során az ügy szempontjából lényeges dokumentumokat adnak át a szakértő részére, ezek között azonban személyes adatok is szerepelhetnek (név, cím, születési hely, születési idő, telefonszám, e-mail cím, személyi azonosító, személyi igazolvány szám, jogosítvány száma, súly, magasság). Az átadott adatokat a szakértő bizalmasan kezeli, azokat harmadik fél számára nem adja át.

Az adatkezelés célja: A kirendelés teljesítése

Az adatkezelés jogalapja Jogszabály

Adattárolási idő: Az igazságügyi szakértőkről szóló 2016. évi XXIX. törvény (a továbbiakban: Szaktv.) alapján a szakértő a tevékenysége során általa kezelt személyes adatokat – ha törvény másképp nem rendelkezik – a kirendelés befejezését vagy megbízás teljesítését követően haladéktalanul zárolja. Az adattárolási idő a befejezett kirendelést vagy megbízást követően, a zárolástól számított tíz év.

Tárolás helye: Informatikai tároló eszközök, papír alapú tárolás, mindkettő

Szakértő megbízásának folyamata

Az igazságügyi szakértőt felkérheti magánszemély, jogi személy, illetve a különböző hatóságok is kirendelhetik. A kirendelés vagy megrendelés célja a felkérésben rögzített kérdés, illetve kérdések megválaszolása. A kirendelés vagy megrendelés során az ügy szempontjából lényeges dokumentumokat adnak át a szakértő részére, ezek között azonban személyes adatok is szerepelhetnek (név, cím, születési hely, születési idő, telefonszám, e-mail cím, személyi azonosító,

személyi igazolvány szám, jogosítvány száma, súly, magasság). Az átadott adatokat a szakértő bizalmasan kezeli, azokat harmadik fél számára nem adja át.
Az adatkezelés célja: A megbízás teljesítése
Az adatkezelés jogalapja Jogszabály
Adattárolási idő: Az igazságügyi szakértőkről szóló 2016. évi XXIX. törvény (a továbbiakban: Szaktv.) alapján a szakértő a tevékenysége során általa kezelt személyes adatokat – ha törvény másképp nem rendelkezik – a kirendelés befejezését vagy megbízás teljesítését követően haladéktalanul zárolja. Az adattárolási idő a befejezett kirendelést vagy megbízást követően, a zárolástól számított tíz év.
Tárolás helye: Informatikai tároló eszközök, papír alapú tárolás, mindkettő

A szakértői feladatok ellátása során kezelt adatok osztályozása

Ez az osztályozás meghatározza, hogy az adatfeldolgozás folyamán melyek a rá vonatkozó biztonsági szintek és az alkalmazandó biztonsági szabályok:

1. B első Info r máció : Általános információ, ha nem tartalmaz a B vagy C osztályba tartozó
2. Bizalmas Információ: Megbízóra vonatkozó adat, ügyfélre vonatkozó adat, harmadik félre vonatkozó adat.
3. Korlátozott hozzáférésű információ: Személyi adatok, érzékeny információk. A korlátozott hozzáférésű információkhoz a lehető legkevesebb személynek lehet hozzáférése a

Adatbiztonsági előírások

Fizikai és környezeti biztonság

A fizikai behatások jogi következményekhez, bizalom- és szakmai hitelvesztéshez vezethetnek a megbízó, az érintett és az igazságügyi szakértő vonatkozásában egyaránt. Ezeket elsődlegesen természeti események vagy emberi közrehatás okozza és eredményük lehet az, hogy a kezelt adatokhoz jogosulatlanul hozzá lehet férni, vagy az, hogy az szakértői információk elérhetetlenek lesznek.

A fizikai és környezeti biztonsági intézkedéseknek alkalmasnak kell lenniük a lopásból, jogosulatlan hozzáférésből, hőmérsékletből, tűzből, füstből, vízből, rázkódásból, terrorcselekményekből, vandalizmusból, áramkimaradásból, kémiai anyagokból vagy robbanószerekből eredő kockázatok hatékony megelőzésére, feltárására és csökkentésére.
Az okokra és lehetséges elkövetőkre példák:
Jogosulatlan belépés

- Berendezések vagy dokumentumok károsítása, vandalizmus vagy lopás
- Érzékeny vagy érintetti információk másolása vagy megtekintése
- Érzékeny berendezések és információk módosítása
- Érzékeny információk nyilvánosságra hozása
- Adatkezelési erőforrásokkal való visszaélés

A lehetséges elkövetők:

- Korábbi munkavállalók
- Érdekelt vagy tájékozott külső személyek, mint pl. versenytársak, tolvajok, szervezett bűnözés és hackerek
- Egy gondatlan elkövető

Információbiztonsági szempontból a következő létesítmények védendők, többek között:

- Szerverek
- Telekommunikációs berendezések
- Áramforrások
- Mobil eszközök
- Helyi hálózatok
- Adattárolók
- Irattárolási helyszínek

Érzékeny adathordozók kezelése és szállítása

Megfelelő ellenőrző mechanizmusokat kell alkalmazni a számítógépeken, lemezeken és más berendezésen vagy adathordozókon tárolt érzékeny információhoz való hozzáférés megelőzésére, vagy ezek elvesztésének megakadályozására (pl. papír alapú dokumentumok, tárolóeszközök, USB memóriák, CD/DVD stb.), hogy megelőzhető legyen a belső, bizalmas vagy korlátozott hozzáférésű információk nyilvánosságra kerülése.

- Minden adathordozót, amely adatot tartalmaz, fizikailag meg kell semmisíteni vagy olvashatatlanná kell tenni, mielőtt leselejtezésre kerülne.
- A belső, bizalmas vagy korlátozott hozzáférésű információkat tartalmazó papír alapú dokumentumokat meg kell semmisíteni, amikor a tárolási idő lejárt.
- A belső, bizalmas vagy korlátozott hozzáférésű információkat tartalmazó CD-t/DVD-t fizikailag meg kell semmisíteni, amikor a tárolási idő lejárt.
- A hibás flash memóriás eszközöket, mint az USB memóriákat és memóriakártáykat fizikailag meg kell semmisíteni.

Vírusvédelem védelem

Az ártalmas szoftverek és az eszközök ártalmas felhasználása ellen további biztonsági ellenőrzéseket kell bevezetni.

Az átadott munkaállomásokat, laptopokat és szervereket egy elismert vírusirtó legújabb verziójával kell ellátni, és automatikus frissítéseket kell beállítani az vírusirtó

- A vírus meghatározásokat azonnal frissíteni kell a publikációt követően.
- A vírusirtó szoftvert úgy kell beállítani, hogy a gépeket és a teljes rendszert valós időben ellenőrizze rendszeresen, a tervezett időpontokban.

Fájltovábbítási szabályok

Az érzékeny adatokat tartalmazó fájlok megosztása nem biztonságos kommunikációs csatornákon kiemelt biztonsági kockázatot rejt magában.

- A (kifelé irányuló vagy belső) fájltovábbításokat mindig hitelesíteni és titkosítani kell amennyiben azok továbbítása e-mailen történik
- A titkosításhoz tartozó jelszót nem szabad az adatokkal együtt küldeni.
- A bizalmas információkat tartalmazó fájlokat a biztonságos hálózati zónában kell tárolni és titkosítani, és titkosítottan kell továbbítani, miután feldolgozásra kerültek. A fájlküldő szerverek, amelyek elérhetők az internetről nem használhatók titkosítatlan adatok hosszútávú tárolására.
- Titkosítás nélkül használhatóak az elektronikus közigazgatás eszközei:

- **E-papír**
- **Ügyfélkapu**
- **Cégkapu**
- **ÁNYK**
- **SZÜF űrlapok és mellékleteik**

Felhő alapú fájltovábbító szolgáltatások és felhő alapú tárolási megoldások (pl. Dropbox, WeTransfer, Google Drive stb.) használata tilos, kivéve, ha kifejezett engedélyezésre kerül sor.

Biztonsági mentés szabályai

A biztonsági mentés szabályzat célja annak biztosítása, hogy az adatok ne vesszenek el és helyreállíthatók legyenek a fizikai eszköz meghibásodása, illetve szándékos vagy véletlen rongálódás/adatvesztés vagy katasztrófa esetén. Egyedi ellenőrző mechanizmusokat kell használni, hogy az adatbiztonsági mentések és helyreállítás kezelésével kapcsolatos kockázatok csökkenjenek.

- Minden éles és kritikus rendszert és adatot, amelyek fontosak a folyamatos működéséhez, teljes egészében biztonsági mentéssel kell biztosítani legalább napi, heti vagy havi szinten attól függően, hogy mennyire érzékeny és mekkora méretű az adatállomány.
- A biztonsági mentést úgy kell végezni, hogy az biztosítsa, hogy az adatok rendszerhiba esetén is helyreállíthatók
- Azonnali teljes adatbiztonsági mentést kell készíteni, amikor nagymértékben változnak az adatok, vagy nagymértékű javítási csomagot, vagy software verzió váltásra kerül sor.
- A helyreállítási eljárásokat rendszeresen ellenőrizni és tesztelni kell (legalább évente) annak biztosítása érdekében, hogy hatékonyak és a helyreállításra előírt eljárásokban meghatározott idő alatt elvégezhetők

Harmadik országgal kapcsolatos rendelkezések

Az igazságügyi szakértő harmadik országbeli adatkezelőknek, adatfeldolgozóknak, egyéb címzetteknek vagy nemzetközi szervezeteknek nem továbbít adatot. Harmadik országgal kapcsolatos adatkezelés esetében figyelembe veszi a GDPR vonatkozó kitételeit (határon áthúzódó eljárások tekintetében).

Incidenskezelés és nyilvántartás

Az adatvédelmi incidens alatt a rendelet értelmében 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. Amennyiben az Adatkezelő tudomására jut az adatvédelmi incidens, azt indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, bejelenteni köteles 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, meg kell jelölni a késedelem okát, az előírt információkat pedig – további indokolatlan késedelem nélkül – részletekben is közölni lehet.
Az adatvédelmi incidensről szóló bejelentésben legalább:

- 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 felelős 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.

Hatálybalépés

Ez a szabályzat az aláírása napján lép hatályba.
Az igazságügyi szakértő a szabályzatot haladéktalanul, de legfeljebb 15 napon belül – a hatálybalépés naptári napjának feltüntetésével – közzéteszi a szervezeten beül mindenki számára elérhető módon, illetve az adatkezelési szabályzat publikus részéből tájékoztatót készít, amit a weboldalán is megjelentet, amennyiben weboldallal rendelkezik.