**Csapi-15 Vásárcsarnok és Piacfenntartó Kft.**
1156 Budapest, Nyírpalota út 52. Tel.: 06-1-418-3188
csapi.info@t-online.hu - http://www.ujpalotapiaca.hu

# ADATVÉDELMI INCIDENSKEZELÉSI SZABÁLYZAT

Az Európai Parlament és Tanács 2016/679 Általános Adatvédelmi Rendelete – „GDPR”

- A természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról -

alapján

Hatályos: 2023. február 01.napjától

| Készítette: | Ellenőrizte és jóváhagyta: |
|---|---|
| Dr. Miklós Péter | Szakály Kis Csilla Gabriella |
| adatvédelmi tisztviselő | ügyvezető |
| sk. | sk. |

# TARTALOMJEGYZÉK

# 1. ÁLTALÁNOS TÁJÉKOZTATÁS

1.1. Általános tájékoztatás az érintett magánszemélyek részére

A Csapi-15 Kft. mint adatkezelő (továbbiakban: adatkezelő) tájékoztatja az érintett munkavállalókat, hogy jelen szabályzatban tömör és közérthető formában igyekszik leírást adni az általa végzett személyes adatkezelések adatvédelmi incidenskezelési eljárásrendjéről.

Az adatkezelő az adatkezelési tevékenységét úgy végzi, hogy az feleljen meg 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.

1.2. A Szabályzat célja

A Szabályzat célja azoknak a belső szabályoknak és intézkedéseknek a megismertetése a munkavállalókkal, 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.

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

Jelen Szabályzat hatálya kiterjed

- az Adatkezelő és/vagy Adatfeldolgozó minden (belső és külsős) munkavállalójára, mint az adatvédelmi esemény vagy incidens észlelésekor szolgálati jelentéstételi úton az azonnali jelentési kötelezettség betartására;
- az Adatkezelő vagy Adatfeldolgozó adatvédelemért felelős vezetője számára az incidenskezelési folyamatban meghatározott feladatai végrehajtására;
- az incidenskezelés szakmai elemzésében és megoldásában, kezelésében részt vevő team tagjaira feladataik végrehajtásában.

# 2. ADATVÉDELMI INCIDENS FOGALMA

**Adatvédelmi incidens**nek minősül a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését, az azokhoz való jogosulatlan hozzáférést vagy a jogosultak számára a hozzáférhetetlenné férést eredményezi.

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.
- Stb.

# 3. ADATVÉDELMI INCIDENS ELJÁRÁSRENDJE

3.1. Adatvédelmi incidens észlelésekor az azt észlelő személy köteles azonnal tájékoztatni közvetlen munkahelyi vezetőjét, aki haladéktalanul köteles tájékoztatni az adatvédelmi tisztviselőt.

3.2. Az adatvédelmi tisztviselőnek szükség esetén eleget kell tennie a Társaságot terhelő, bejelentés megtételére vonatkozó kötelezettségnek.

3.2.1. Amennyiben a Társaság a kezelt személyes adatok vonatkozásában „Adatfeldolgozó”, akkor az észlelést (bejelentést) követően haladéktalanul, indokolatlan késedelem nélkül az incidenst az adott személyes adatok vonatkozásában jelenteni kell az Adatkezelőnek.

3.2.2. Amennyiben a Társaság a kezelt személyes adatok vonatkozásában „Adatkezelő”, akkor az észlelést (bejelentést) követően haladéktalanul, indokolatlan késedelem nélkül, de legkésőbb 72 órán belül az incidenst jelenteni kell a NAIH-nak (Hatóságnak).

Az Adatkezelő általi 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.

3.2.3. Amennyiben a Társaság a kezelt személyes adatok vonatkozásában „Adatkezelő”, és az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatkezelő indokolatlan késedelem nélkül, világos és közérthető megfogalmazásban tájékoztatni kell az érintettet az adatvédelmi incidensről.

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.

Az adatvédelmi tisztviselő, illetve amennyiben az incidens informatikai eszközzel, erőforrással kapcsolatban hozható, akkor az adatvédelmi tisztviselő és a rendszergazda együttes további feladatai:

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

3.4. Adatvédelmi incidens hatásának vagy potenciális hatásának elemzése, meghatározása a Társaság, illetve az érintettek jogai szempontjából.

3.5. Szükség esetén azonnali eszkalálás, válságkezelési terv elindítása.

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

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

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

3.6. 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.

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

3.8. Az adatvédelmi incidens kiértékelésének eredményéről tájékoztatni kell az adatvédelmi hatóságot (Nemzeti Adatvédelmi- és Információszabadság Hatóság).

# 4. ZÁRÓ RENDELKEZÉSEK

## 4.1. Hatálybalépés

Jelen szabályzat 2023. február 01. napján lép hatályba, a benne foglaltak munkavállalók és egyéb közreműködők részére történő megismertetése az adatkezelő ügyvezetőjének a feladata és felelőssége.