

# ADATVÉDELMI INCIDENS BEJELENTÉSÉRE VONATKOZÓ ELJÁRÁSI REND

## I.

### A Szabályzat célja

1.1. A **CAPITAL EXPERT SOLUTIONS Kft.** (székhely: 2613 Rád, Vörösmarty u. 6.; bejegyezve a Budapest Környéki Törvényszék Cégbírósága által Cg.: 13-09-181237 cégjegyzékszámom; a továbbiakban: a Társaság) jelen szabályzat megalkotásával biztosítani kívánja az információs önrendelkezési jogról és információszabadságról szóló 2011. évi CXII. törvény (Infotv.), valamint a Az Európai Parlament és a Tanács (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 rendelet hatályon kívül helyezéséről szóló (GDPR általános adatvédelmi rendelet) szabályozásának megfelelő adatvédelmi incidens kezelési eljárásrendet.

1.2. Jelen szabályzattal a Társaság biztosítani kívánja az adatvédelmi incidensre vonatkozó nyilvántartások működésének törvényes rendjét, az adatvédelem alkotmányos elveinek, az adatbiztonság követelményeinek érvényesülését, meg kívánja akadályozni a személyes adatokhoz való jogosulatlan hozzáférést, a személyes adatok jogosultalan megváltoztatását, továbbítását, nyilvánosságra hozatalát, törlését vagy megsemmisítését, ideértve a véletlen megsemmisülés és adatsérülés eseteit is. Jelen szabályzat célja továbbá, hogy szabályozza és megakadályozza a biztonság olyan sérülését, amely a továbbított, tárolt, vagy egyéb módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az ezen adatokhoz való jogosultalan hozzáférést.

1.3. Az adatvédelmi incidens megfelelő és kellő idejű intézkedés hiányában fizikai, vagyoni vagy nem vagyoni károkat okozhat a természetes személyeknek, többek között a személyes adataik feletti rendelkezés elvesztését vagy a jogaik korlátozását, a hátrányos megkülönböztetést, a személyazonossággal való visszaélést, a pénzügyi veszteséget, az álnevesítés engedély nélküli feloldását, a jó hírnév sérelmét, a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülését, illetve természetes személyeket sújtó egyéb jelentős gazdasági vagy szociális hátrányt okozhat. Jelen szabályzat célja, hogy az adatkezelő tudomására jutott az adatvédelmi incidens észlelésére, nyilvántartására és bejelentésére vonatkozó szabályrendszer meghatározza.

## II.

### Fogalmak

2.1. „**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;

2.2. **„adatkezelés”**: a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés;

2.3. **„nyilvántartási rendszer”**: a személyes adatok bármely módon – centralizált, decentralizált vagy funkcionális vagy földrajzi szempontok szerint – tagolt állománya, amely meghatározott ismérvek alapján hozzáférhető;

2.4. **„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;

2.5. **„adatfeldolgozó”**: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel;

2.6. **„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. Azon közhatalmi szervek, amelyek egy egyedi vizsgálat keretében az uniós vagy a tagállami joggal összhangban férhetnek hozzá személyes adatokhoz, nem minősülnek címzettek; az említett adatok e közhatalmi szervek általi kezelése meg kell, hogy feleljen az adatkezelés céljainak megfelelően az alkalmazandó adatvédelmi szabályoknak;

2.7. **„harmadik fél”**: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely nem azonos az érintettel, az adatkezelővel, az adatfeldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére felhatalmazást kaptak;

2.8. **„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;

2.9. **„érintett felügyeleti hatóság”**: az a felügyeleti hatóság, amelyet a személyes adatok kezelése a következő okok valamelyike alapján érint:

- a) az adatkezelő vagy az adatfeldolgozó az említett felügyeleti hatóság tagállamának területén rendelkezik tevékenységi hellyel; a Társaság esetében a Nemzeti Adatvédelmi és Információszabadság Hatóság (1125 Budapest Szilágyi Erzsébet fasor 22/C, a továbbiakban: NAIH);
- b) az adatkezelés jelentős mértékben érinti vagy valószínűsíthetően jelentős mértékben érinti a felügyeleti hatóság tagállamában lakóhellyel rendelkező érintetteket; vagy
- c) panaszt nyújtottak be az említett felügyeleti hatósághoz.

### **III.**

#### **Az adatvédelmi incidens kezelése/észlelése/jelentése**

3.1. A Társaság minden munkavállalója – *beleértve az egyéb jogviszonyban foglalkoztatott személyeket is* – köteles a Társaságon belül történt adatvédelmi incidenst indokolatlan késedelem nélkül jelenteni a Társaság adatvédelmi tisztviselője – ilyen kijelölésének hiányában a Társaság mindenkori ügyvezetője – (a továbbiakban: adatvédelmi tisztviselő) részére.

A Társasággal egyéb szerződéses jogviszony alapján, vagy címzettként, harmadik félként adatfeldolgozást/adatkezelést végző partnerek is kötelesek a Társaság vonatkozásában/érdekében kezelt személyes adatok kezelése/feldolgozása során felmerült adatvédelmi incidenst indokolatlan késedelem nélkül jelenteni a Társaság adatvédelmi tisztviselője részére.

3.2. A bejelentés tartalmazza a bejelentő nevét, telefonszámát, beosztását, a Társaság munkavállalója esetében szervezeti egységének megnevezését, valamint az incidens tárgyát, rövid leírását és azt, hogy az incidens érinti-e a Társaság informatikai rendszerét. *Az adatvédelmi incidens bejelentő lap mintáját a jelen szabályzat 1. sz. melléklete tartalmazza.*

3.3 Az adatvédelmi incidens kockázata/súlyossága vonatkozásában az azt észlelőnek mérlegelési jogosultsága nem áll fenn, az adatvédelmi incidens minősítése, kockázati besorolása kizárólag a Társaság adatvédelmi tisztviselőjének jogköre. A bejelentés adatvédelmi tisztviselőhöz érkezését követően az adatvédelmi tisztviselő haladéktalanul megkezdzi az adatvédelmi incidens kivizsgálását és értékelését.

### **IV.**

#### **Az adatvédelmi incidens kivizsgálása, értékelése, nyilvántartásba vétele**

4.1. Az adatvédelmi tisztviselő megvizsgálja a bejelentést és amennyiben szükséges, a bejelentőtől további adatokat kér az incidensre vonatkozóan. Az adatvédelmi tisztviselő felhívására a bejelentő köteles megadni: az adatvédelmi incidens bekövetkezésének időpontját és helyét, az adatvédelmi incidens egyéb körülményeit, az adatvédelmi incidens által érintett adatok körét, mennyiségét, az adatvédelmi incidenssel érintett személyek körét és számát, az adatvédelmi incidens várható hatásait, az adatvédelmi incidens megelőzésére, következményeinek enyhítésére megtett intézkedések felsorolását.

A bejelentő az adatszolgáltatást haladéktalanul köteles teljesíteni az adatvédelmi tisztviselő részére.

Amennyiben az adatvédelmi incidens értékelése vizsgálatot igényel az adatvédelmi tisztviselő a vizsgálat lefolytatásához szükséges munkatársak bevonásával lefolytatja a vizsgálatot. A vizsgálatnak tartalmaznia kell, hogy az adatvédelmi incidens magas kockázattal jár-e az érintettek jogaira és kötelezettségeire, milyen jellegű kockázatról van szó és szükséges-e az érintettek tájékoztatása az incidensről. Amennyiben nem szükséges az érintettek tájékoztatása, a vizsgálatnak tartalmaznia kell ennek indokait is.

4.2. A vizsgálat eredményeként az adatvédelmi tisztviselő javaslatot tesz az adatvédelmi incidenssel érintett szervezeti egység vezetőjének az incidens kezeléshez szükséges intézkedések megtételére. A javaslat alapján a megvalósítandó további intézkedésekről az adatok kezelését vagy feldolgozását végző szakterület vezetője dönt.

A vizsgálatot legkésőbb a bejelentés adatvédelmi tisztviselőhöz érkezésétől számított három munkanapon belül be kell fejezni és a vizsgálat eredményéről a Társaság vezető tisztviselőjét az adatvédelmi tisztviselő tájékoztatja.

4.3. Az adatvédelmi tisztviselő az adatvédelmi incidensről nyilvántartást vezet. A nyilvántartás tartalmazza: (i) az érintett személyes adatok körét, (ii) az adatvédelmi incidenssel érintettek körét és számát, (iii) az adatvédelmi incidens időpontját, (iv) az adatvédelmi incidens körülményeit, hatásait, (v) az elhárítására megtett intézkedéseket és (vii) egyéb jogszabályban előírt adatokat. Az adatvédelmi incidensnyilvántartás pontos vezetéséről, aktualizálásáról az adatvédelmi tisztviselő gondoskodik. *Az adatvédelmi nyilvántartást a jelen szabályzat 2. sz. melléklete tartalmazza.*

## V.

### **Az adatvédelmi incidens bejelentése a felügyeleti hatóság részére**

5.1. Az adatvédelmi incidenst az adatkezelő/adatvédelmi tisztviselő indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, az illetékes felügyeleti hatóságnak köteles bejelenteni. Amennyiben az adatvédelmi tisztviselő az adatvédelmi incidens kivizsgálása alapján az adatvédelmi incidenst valószínűsíthetően kockázat nélkülinek minősíti a természetes személyek jogaira és szabadságaira nézve a bejelentésre nem köteles. Amennyiben a bejelentés nem történik meg 72 órán belül, kötelező mellékelni a késedelem igazolására szolgáló indokokat is.

5.2. A felügyeleti hatóság részére történő bejelentésben *(a 3. számú melléklet szerinti formában)*

- 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 az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb 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. Az adatvédelmi incidens orvoslására és enyhítésére tett intézkedéseket.

5.3. Amennyiben nem lehetséges a fenti információkat egyidejűleg közölni, azok további indokolatlan késedelem nélkül később részletekben is közölhetők. *A felügyeleti hatóság részére küldendő bejelentő lap a jelen szabályzat 3. sz. melléklete.*

## VI. Az érintettek tájékoztatása

6.1. Ha a vizsgálat eredményeként megállapítást nyert, hogy az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságára nézve és az érintettek tájékoztatása szükséges, az adatvédelmi tisztviselő haladéktalanul értesíti az érintetteket és erről a Társaság vezető tisztségviselőjét is értesíti.

6.2. Nem kell az érintetteket tájékoztatni, ha a Társaság olyan technikai, szervezési, védelmi intézkedéseket hajtott végre az érintett adatokra vonatkozóan, amelyek megakadályozzák az illetéktelen személyek számára való hozzáférést az adatokhoz vagy megakadályozzák az adatok értelmezhetőségét, valamint, ha a tájékoztatás aránytalan erőfeszítést tenne szükségessé. Ebben az esetben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, mely tájékoztatás elektronikus úton is megtörténhet.

## VII. Adatvédelmi incidenssel kapcsolatos eljárásra vonatkozó oktatás/tréning

7.1. Az adatvédelmi tisztviselő jelen szabályzatban foglaltak szerint gondoskodik az adatvédelmi tudatosság növelése céljából adatvédelmi incidensekkel kapcsolatos oktatásról, mely során a múltban bekövetkezett adatvédelmi incidensek tapasztalatait, vagy a lehetséges adatvédelmi incidensek veszélyeit ismerteti, elemzi, a kockázatok csökkentésével, megelőzésével kapcsolatosan tájékoztatást ad, illetve az ismereteket ellenőrzi.

7.2. A munkavállalók általános adatvédelmi-információbiztonsági tréning rendje hathavonta (*kapcsolható más rendszeres képzésekhez is*) egy óra időtartamban történjen. Ez vonatkozik az informatikai és nem informatikai munkavállalókra egyaránt.

**Adatkezelő és elérhetősége:** CAPITAL EXPERT SOLUTIONS Kft., (Tel.: +36706378424; Email: [capitalexpertsolutions@gmail.com](mailto:capitalexpertsolutions@gmail.com))

**Adatvédelmi tisztviselő és elérhetősége:** Mészáros Józsefné ügyvezető (Tel.: +36706378424; Email: [capitalexpertsolutions@gmail.com](mailto:capitalexpertsolutions@gmail.com))

Mellékletek:

1. sz. melléklet: Bejelentő adatvédelmi incidens észleléséről
2. sz. melléklet: Adatvédelmi incidens nyilvántartó lap
3. sz. melléklet: Adatvédelmi incidens bejelentő lap

Budapest, 2018. május 25.

CAPITAL EXPERT SOLUTIONS KFT.  
képviselésében  
Mészáros Józsefné ügyvezető

**1. sz. Melléklet**

**BEJELENTŐ LAP ADATVÉDELMI INCIDENS ÉSZLELÉSÉRŐL**  
*- az adatvédelmi tisztviselő részére-*

**Bejelentő neve:**

**Bejelentő szervezeti egységének/munkakörének megnevezése:**

**Az adatvédelmi incidens tárgya, megnevezése:**

**Az adatvédelmi incidenssel érintett adatok és személyek köre, száma:**

**Az adatvédelmi incidens rövid leírása, ismertetése:**

**Az adatvédelmi incidens érinti-e az informatikai rendszert, aha igen milyen módon:**

Kelt, hely, év, hónap, nap

.....  
Bejelentő aláírása

**2. számú Melléklet**

**ADATVÉDELMI INCIDENS NYILVÁNTARTÓ LAP**

*Az adatvédelmi tisztviselő tölti ki!*

**Az adatvédelmi incidens időpontja:**

**Az adatvédelmi incidenssel érintett szervezeti egység:**

**Az adatvédelmi incidens észlelésének releváns körülményei:**

**Az adatvédelmi incidenssel érintett személyes adatok köre:**

**Az adatvédelmi incidenssel érintettek köre és száma:**

**Az adatvédelmi incidens körülményeinek leírása:**

**Az adatvédelmi incidens hatásai:**

**Az adatvédelmi incidens kockázati értékelése:**

**Az adatvédelmi incidens elhárítására tett intézkedések leírása:**

**Hatósági értesítések:**

**NAIH értesítésének dátuma:**

**Operatív rendszer, vonatkozó szabályzat megjelölése:**

Kelt, hely, év, hónap, nap

.....  
az adatvédelmi tisztviselő  
aláírása

**3. sz. Melléklet**

**ADATVÉDELMI INCIDENS BEJELENTŐ LAP**

**- a felügyeleti hatóság részére-**  
*Az adatvédelmi tisztviselő tölti ki!*

**Adatvédelmi tisztviselő neve és elérhetősége (postai levelezési cím, elektronikus levelezési cím):**

**Adatvédelmi incidens jellege, az érintettek kategóriája, száma:**

**Az adatvédelmi incidenssel érintett adatok kategóriája, száma:**

**Az adatvédelmi incidens észlelésének körülményei**

**Az adatvédelmi incidens következményei:**

**Az adatvédelmi incidens elhárítására/orvoslására/enyhítésére tett intézkedések:**

Kelt, hely, év, hónap, nap

.....  
Adatvédelmi tisztviselő  
aláírása