BUDAPEST

Mozaik Gazdasági Szervezet

Adatvédelmi incidens kezelési szabályzat

Lengyel László
igazgató

MOZAIK Gazdasági Szervezet

hatályos: 2018. május 25-étől

Mozaik Gazdasági Szervezet (a továbbiakban: Szervezet), az információszabadságról szóló 2011. CXII. törvény (a továbbiakban: Info tv.), valamint az Európai Parlament és a Tanács (EU) 2016/679 számú általános adatvédelmi rendelete (a továbbiakban: GDPR) rendelkezéseivel összhangban, a személyes adatok védelmének biztosítása érdekében az alábbiak szerint alkotja meg az adatvédelmi incidensekre vonatkozó szabályzatát.

1. Adatvédelmi incidensek

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.

Az adatvédelmi incidens megfelelő és kellő idejű intézkedés hiányában fizikai, vagyoni vagy nem vagyoni károkat okozhat az érintetteknek, többek között:

- a személyes adataik feletti rendelkezés elvesztését vagy a jogaik korlátozását;
- a hátrányos megkülönböztetést;
- a személyazonosság-lopást vagy 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;
- a szóban forgó természetes személyeket sújtó egyéb jelentős gazdasági vagy szociális hátrányt.

A Szervezet ezért a tudomására jutott adatvédelmi incidenst az alábbi előírások szerint kezeli:

2. Adatvédelmi incidens észlelése és jelentése

A Szervezet minden munkavállalója – beleértve az munkavégzésre irányuló egyéb jogviszonyban foglalkoztatott személyeket is – köteles a Szervezeten belül történt adatvédelmi incidenst a tudomására jutást követően haladéktalanul jelenteni a Szervezet vezetőjének, aki továbbítja azt az adatvédelemért felelős munkavállalóhoz. A bejelentés tartalmazza a bejelentő nevét, beosztását, valamint az incidens tárgyát, rövid leírását és azt, hogy az incidens érinti-e a Szervezet informatikai rendszerét.

Amennyiben az adatvédelmi incidens érinti a Szervezet informatikai rendszerét is, akkor a bejelentést a Szervezet informatikáért felelős személyének (a továbbiakban: rendszergazda) is meg kell küldeni.

3. Adatvédelmi incidens kivizsgálása, értékelése

A Szervezet adatvédelemért felelős munkavállalója – informatikai rendszert érintő incidens esetén az rendszergazdával együttműködve – megvizsgálja a bejelentést és amennyiben szükséges, a bejelentőtől további adatokat kér az incidensre vonatkozóan. Az adatvédelemért felelős munkavállaló 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, de legkésőbb 24 munkaórán belül teljesíti.

Amennyiben az adatvédelmi incidens értékelése vizsgálatot igényel a Szervezet adatvédelemért felelős munkavállalója, valamint egyéb, 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 tartalmazni kell ennek indokait is. Az incidens súlyosságának megállapítására a 1. számú függelék ad segítséget.

A vizsgálat eredményét haladéktalanul megküldi az adatvédelemért felelős munkavállaló az igazgatónak.

A vizsgálat eredményeként a Szervezet vezetője – szükség esetén a rendszergazda tanácsát kikérve – intézkednek a szükséges lépések megtételéről.

A vizsgálatot legkésőbb a Szervezet vezetőjéhez érkezéstől számított három munkanapon belül be kell fejezni.

4. Az adatvédelmi incidens nyilvántartása

Az adatvédelmi incidensről a Szervezet adatvédelemért felelős munkavállalója nyilvántartást vezet.

A nyilvántartás tartalmazza:

- az érintett személyes adatok körét,
- az adatvédelmi incidenssel érintettek körét és számát,
- az adatvédelmi incidens időpontját,
- az adatvédelmi incidens körülményeit,
- hatásait,
- az elhárítására megtett intézkedéseket és
- egyéb jogszabályban előírt adatokat.

5. Az adatvédelmi incidens bejelentése a Hatóság részére

A Szervezet adatvédelemért felelős munkavállalója az adatvédelmi incidenst a Szervezet tudomására jutását követően haladéktalanul, de legkésőbb az incidens Szervezet tudomására jutásától számított 72 órán belül bejelenti a Hatóság részére, kivéve, ha az incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Ha a bejelentés nem történik meg határidőben, a Szervezet adatvédelemért felelős munkavállalója köteles ennek okát igazolni a Hatóság részére.

A Hatósági bejelentésnek tartalmaznia kell:

- az adatvédelmi incidenssel érintett adatok körét és hozzávetőleges számát,
- az adatvédelmi incidenssel érintett személyek körét és hozzávetőleges számát,
- az adatvédelmi incidens jellegét, körülményeit,
- az adatvédelmi incidens valószínűsíthető következményeit és
- az adatvédelmi incidens orvoslására és enyhítésére megtett intézkedéseket.

6. Az érintettek tájékoztatása adatvédelmi incidensről

Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságára nézve és az érintettek tájékoztatása szükséges, a Szervezet adatvédelemért felelős munkavállalója haladéktalanul értesíti az érintetteket. Az érintettek tájékoztatása független a Hatóság felé irányuló tájékoztatási kötelezettségtől.

Nem kell az érintetteket tájékoztatni:

- ha a Szervezet 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.
- ha az adatvédelmi incidens bekövetkezését követően a Szervezet olyan intézkedéseket tett, amelyek biztosítják, hogy a feltárt adatkezelési kockázat valószínűsíthetően nem valósul meg.
- ha a tájékoztatás aránytalan erőfeszítést tenne szükségessé. Ebben az esetben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, mely tájékoztatás elektronikus úton is megtörténhet.

7. Záró rendelkezések

A jelen Szabályzatban nem szabályozott kérdésekben a Szervezet mindenkor hatályos Adatvédelmi és adatkezelési szabályzatának rendelkezései az irányadók azzal, hogy a jelen Szabályzat, illetve az Adatvédelmi és adatkezelési szabályzat közötti bármely eltérés esetén az Adatvédelmi és adatkezelési szabályzatban foglaltak az irányadók.

1. számú függelék

Adatvédelmi incidens súlyosságának értékelése

Az ENISA (European Union Agency for Network and Information Security), azaz az Európai Uniós Hálózat- és Információbiztonsági Ügynökség dolgozott ki 2013-ban egy ajánlást, módszertani útmutatót (a továbbiakban: Útmutató), amely teljesen megfelelő és kidolgozott metodikát ad az adatvédelmi incidens súlyozásához.

Az útmutató a súlyozáshoz az alábbi tényezőket veszi figyelembe:

I. ***Adatkezelési Környezet (AK):*** az incidenssel érintett adatokat vizsgálja, az adatkezelés összes körülményre tekintettel.

Csoportosítása

1. Egyszerű adat
2. Viselkedésre/attitűdre vonatkozó adat
3. Pénzügyi adat
4. Érzékeny adat

Az adattípusokhoz tartozó mérőszámok táblázata

1. **EGYSZERŰ ADATOK**: Életrajzi adat, elérhetőség (név, e-mail stb.), teljes név, családi élet, végzettség, munkahelyi tapasztalat.

Adatkezelési környezet	**Pontszám**
Ha valamely adatot megszerezték, és súlyosbító tényező nem merül fel.	1
Ha az adatt típusa szerint, vagy az adatot megszerző egyéb okból az adat segítségével az érintett részbeni profilozását, vagy szociális/ pénzügyi helyzetére vonatkozó megállapításokat és következtetéseket vonhat le.	2
Ha az adatt típusa/ mennyisége szerint, vagy az adatot megszerző egyéb okból az adat segítségével az érintett egészségi állapotára, szexuális irányultságára, politikai preferenciáira vagy vallásihitbeli meggyőződésére vonatkozó megállapításokat tehet.	3
Ha az adatok érzékeny csoportba tartozó személyekre (pl. hátrányos helyzetűek, kiskorúak, stb.) vonatkozik,, mivel az adatok kritikusak lehetnek az érzelmi/ mentális/lelki/fizikai fejlődésük tekintetében.	4

2. **VISELKEDÉSRE/ ATTITŰDRE VONATKOZÓ ADAT:** Pl. helymeghatározás, közlekedés, személyes érdeklődés, szokások.

Adatkezelési környezet	**Pontszám**
Ha valamely adatot megszerezték, és sem enyhítő, sem súlyosbító körülmény nem merül fel.	2
Ha az incidenssel érintett adat nem enged lényeges betekintést az érintett attitűdjeibe, vagy az adatok az incidenstől függetlenül egyébként nyilvánosan is elérhetőek (pl. a webes keresések alapján történő attitűdre vonatkozó következtetések)	1
Ha az adatt típusa/ mennyisége szerint, vagy az adatot megszerző egyéb okból képes az érintettről részben profilt alkotni, az érintett mindennapi életébe, szokásaiba betekintési lehetőséget ad.	3
Ha az érintett érzékeny adatai segítségével profilozható az érintett.	4

3. **PÉNZÜGYI ADATOK:** Bármely, az érintettre vonatkozó pénzügyi adat, így az adózásra, a pénzügyi tranzakciókra, banki státuszra, befektetésekre, hitelkártyákra, számlákra vonatkozó adatok.

Adatkezelési környezet	Pontszám
Ha valamely pénzügyi adatot megszerezték, és sem enyhítő, sem súlyosbító körülmény nem merül fel.	3
Ha az incidenssel érintett adat nem enged lényeges betekintést az érintett pénzügyi adataiba (pl. az, hogy az érintett egy adott bank ügyfele, minden további részinformáció nélkül)	1
Ha az incidenssel érintett pénzügyi adat ugyan megszerzésre kerül, de még mindig nem alkalmas az érintett pénzügyeibe történő betekintésre (például bankszámlaszámok név, vagy további részletek nélkül)	3
Ha az érintett adatai mennyiségileg vagy minőségileg már lehetőséget biztosítanak a csalásra, vagy részletes szociális/pénzügyi profil felállítására.	4

4. **ÉRZÉKENY ADATOK**: munkahelyi beléptető rendszer; speciális belépő kódokat alkalmazó IT rendszer; szem-, arc -, ujjlenyomat olvasó rendszerek; kártyás beléptető rendszerek a munkahelyen. Politikai pártok, választási bizottságok, közösségi szervezetek, kampányszervezetek, népszavazást kezdeményező szervezetek és személyek hatóságok és pártok vagy politikai szervezetek adatkezelése. Otthoni vagy magánjellegű tevékenységekhez kapcsolódó adatok alapvető jog gyakorlására is kiható adatok. Helymeghatározó adatok; pénzügyi adatok; személyes iratok; e-mailek; naplók; jegyzetelési funkcióval rendelkező e-olvasókból származó jegyzetek; valamint az életnaplózó alkalmazásokban tárolt, rendkívül személyes jellegű adatok.

Adatkezelési környezet	Pontszám
Ha valamely adatot megszerezték, és enyhítő körülmény nem merül fel.	4
Ha a megszerzett adat nem enged semmilyen lényeges betekintést az érintett viselkedésébe, vagy az adatot nyilvánosan is megosztották az adatvédelmi incidenstől függetlenül is.	1
Ha a megszerzett adatok általános következtetés(ek) levonásához vezethet.	2
Ha a megszerzett adatok érzékeny/különleges adatokra vonatkozó következtetés(ek) levonásához vezethet.	3

II. ***Azonosíthatóság Mértékének (AM) meghatározása***: vizsgálja, hogy az incidenssel érintett adatok segítségével mennyire könnyen azonosítható az érintett; e körben általánosan elmondható, hogy a kockázat annál kisebb, minél kevésbé és minél nehezebben azonosítható az érintett.

III. ***Sérülés Körülményeinek (SK) vizsgálata***: azt vizsgálja, hogy az incidens során az adatok sérülése következtében mennyire sérült az adatok biztonsága; e körben azt is vizsgálja, hogy az adatok sérülése milyen körülmények között történt.

Az értékelés módja

Az értékelés az alábbi képlet szerint történik:

Veszély súlyossága: Adatkezelési környezet (AK) x Azonosíthatóság mértéke (AM) + Sérülés körülményei (SK)

$$VS = AK \times AM + SK$$

Az értékelés eredményeként megállapítható az alacsony, közepes, magas vagy nagyon magas súlyossági fok.

Súlyossági fokok (VS) értékhez rendelve:

kisebb, mint 2	Alacsony kockázatú incidens	Vagy nem okoz gondot az érintettnek, vagy csak nagyon kis mértékben
2 vagy annál több, de 3-nál kevesebb	Közepes kockázatú incidens	Az érintettek némi kellemetlenséggel ugyan, de túljutnak az incidens okozta nehézségeken.
3 vagy annál több, de 4-nél kevesebb	Magas kockázatú incidens	Az érintettek komoly következményekkel számolhatnak, amit csak nagy nehézségekkel oldhatnak meg, hozzák helyre.
4 vagy annál több	Nagyon magas kockázatú incidens	Az érintettek hatalmas, beláthatatlan következményekkel számolhatnak, amiket lehet, hogy nem tudnak megoldani, helyrehozni.

1. számú melléklet

Adatvédelmi incidens bejelentőlap

Alulírott ....., beosztás: ....., a **Mozaik Gazdasági Szervezet**, dolgozója, 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 Európai Parlament és a Tanács (EU) 2016/679 számú általános adatvédelmi rendelete (a továbbiakban: GDPR) alapján ezúton

b e j e l e n t e m,

hogy a következő adatvédelmi incidensről szereztem tudomást.

Az incidens időpontja:

Az incidensről való tudomásszerzés időpontja és helye:

Az incidens tárgya:

Az incidenssel érintett személyek kategóriái és hozzávetőleges száma:

Az incidenssel érintett adatok kategóriái és hozzávetőleges száma:

Az incidens érinti-e a Szervezet informatikai rendszerét? igen - nem

Az incidensből eredő, valószínűsíthető következmények:

Az incidens orvoslására tett vagy tervezett intézkedések:

Az adatvédelmi tisztviselő vagy egyéb kapcsolattartó neve és elérhetősége:

Kelt:

.....

bejelentő

2. számú melléklet

Adatvédelmi incidens nyilvántartása

Sz.	Az incidenssel érintett személyes adatok köre	Adatvédelmi incidens				Az incidens körülményei, hatása	Az incidens elhárítására megtett intézkedések
		Időpont	Típus	Érintettek köre	Érintettek száma		