BUDAPEST KÖZÚT

Adatvédelmi és Adatbiztonsági Szabályzat
2. számú módosított melléklet

Kiadásért felelős:

Bodorné Boldis Erzsébet

Bodorné Boldis Erzsébet
Biztonsági és vagyonvédelmi osztályvezető

Egyetértek:

Tímár Judit
Jogi és igazgatási főosztályvezető

Jóváhagyta és a végrehajtást elrendelte:

Szőke Gábor
Vezérigazgató

Hatálybalépés dátuma: 2022. január 20.

2. számú melléklet

AZ ADATBIZTONSÁG

Adatbiztonság

Az adatbiztonsági rendszabályok és intézkedések célja a manuálisan és az elektronikusan kezelt személyes adatok, valamint az adathordozók védelme a sérülés, rongálódás, megsemmisülés és illetéktelen hozzáférés ellen (lásd Infotv. 7. §).

Az adatbiztonság általános szempontjai

A Társaság az adatkezelés során mindvégig köteles gondoskodni a kezelt személyes adatok ésszerűen elvárható legmagasabb szintű biztonságáról (adatbiztonság elve). A Társaság köteles megtenni azokat a technikai és szervezési intézkedéseket továbbá kialakítani azokat az eljárási szabályokat, amelyek az adatvédelmi jogszabályok érvényre juttatásához szükségesek.

Az adatkezelő köteles gondoskodni az általa kezelt adatok védelméről.

Az adatokat védeni kell a jogosulatlan hozzáférés, a megváltoztatás, a továbbítás, a nyilvánosságra hozatal, a törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés ellen.

Adatkarbantartást csak az erre felhatalmazott adatkezelő végezhet.

A számítástechnikai rendszerek üzemeltetését ellátó munkavállalók a feladataik ellátásához szükséges mértékig az adatállományokhoz hozzáférhetnek, az adatokat azonban más célra nem használhatják fel, és mások tudomására nem hozhatják. Rendellenesség észlelése esetén, kötelesek azt azonnal jelezni az Informatikai igazgatónak valamint az Adatvédelmi tisztviselőnek.

Az adatbiztonság érdekében megfogalmazott előírások betartásáért, betartatásáért az Informatikai igazgatóság által üzemeltetett informatikai rendszerek vonatkozásában az **Informatikai igazgatóság vezetője**, a lokális adatfeldolgozási rendszerek vonatkozásában az adatfeldolgozást végző **szervezeti egység vezetője** a felelős.

Az adatokhoz való hozzáférés szabályozása

Az adatokhoz való hozzáférést jelszavas védelemmel és jogosultsági rendszer működtetésével kell érvényesíteni.

A központi rendszerhez, illetve a szerver központi tárterületeihez való hozzáférés jelszavait és jogosultsági rendszerét az Informatikai igazgatóság állítja be és kezeli az IBSZ előírásai szerint.

Az egyedi alkalmazások lokális gépein a speciális adatfeldolgozó szoftver saját jelszó és jogosultsági rendszerét kell alkalmazni. A jelszavak használatáért, azok rendszeres változtatásáért és dokumentálásáért az adatfeldolgozást végző **gazdasági egység vezetője** felelős.

A központi rendszer és az egyedi rendszerek hozzáférési jogosultságának működtetésére egyaránt érvényesek az IBSZ-ben rögzített előírások.

Az adatok mentése, az adathordozók biztonsága

Az adatok mentésének és az adathordozók biztonságának előírásait az IBSZ rögzíti.

A központi szervereken tárolt adatok rendszeres mentése az IBSZ-ben előírt „Mentési Rend" szerint történik.

A lokális adatfeldolgozási rendszerek adatainak mentéséért, a mentések naplózásáért az adathordozók nyilvántartásának-, biztonságos tárolásának megfelelőségéért az **adatkezelő** felelős.

Az adatvédelmi incidens

Adatvédelmi és Adatbiztonsági Szabályzat
2. számú módosított melléklet

Az Adatvédelmi tisztviselő, az Informatikai igazgató és a Jogi osztály vezetője együtt vesz részt az adatvédelmi incidensek kezelésére vonatkozó eljárásrend kidolgozásában és működtetésében (továbbiakban: Bizottság).

Az adatvédelmi incidenseket a következő három klasszikus adatbiztonsági kritériumon keresztül kategorizálhatók:

1. „Bizalmas jelleg sérülése" – a személyes adatok jogosulatlan vagy véletlen közzététele vagy az ezekhez való hozzáférés
2. „Integritás sérülése" – a személyes adatok felhatalmazás nélküli vagy véletlenül bekövetkező módosítása
3. „Rendelkezésre állás sérülése" – a személyes adatok véletlen vagy jogosulatlan megsemmisítése vagy a személyes adatok elvesztése

Az adatvédelmi incidenst indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 (hetvenkettő) órával azután, hogy az adatvédelmi incidens a Társaság valamely munkavállalójának tudomására jutott, be kell jelenteni az illetékes Hatóságnak.

Az incidens adatkezelő általi tudomásszerzésnek minősül például:

ha harmadik személy jelzi az adatkezelőnek, hogy az ügyféléről véletlenül személyes adatokat kapott meg, és az ennek alátámasztására alkalmas bizonyítékokat juttat el az adatkezelő részére – ekkor nincs kétség afelől, hogy az adatkezelő tudomást szerzett az adatvédelmi incidens bekövetkezéséről,

ha az adatkezelő észleli, hogy behatolás történt a hálózatába és megállapítja, hogy a hálózaton tároltak személyes adatokat, illetve, hogy azokat érintően következett be az incidens.

Az a munkavállaló, aki a Társaság által kezelt vagy feldolgozott személyes adatokkal kapcsolatban adatvédelmi incidenst, azaz a biztonság olyan sérülését észleli, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést észlel, az köteles haladéktalanul megtenni a bejelentést, megadva a nevét, telefonszámát és/vagy e-mail címét, dátum és pontos idő megadásával mikor észlelte az incidenst, az incidens tárgyát, valamint azt, hogy az incidens milyen eszközt, alkalmazást, rendszert érint.

A bejelentő további olyan információkat is megadhat, amelyeket az incidens beazonosítása, megvizsgálása szempontjából lényegesnek ítél.

Az incidenssel kapcsolatos bejelentéseket az adatvedelmitisztviselo@budapestkozut.hu e-mail címen lehet megtenni.

Az adatvédelmi incidens kezelése

Az incidens bejelentése alapján a Bizottság tagjai a bejelentést követően haladéktalanul felveszik egymással a kapcsolatot e-mailben, személyesen, vagy telefonon annak érdekében, hogy az incidens bekövetkezéséről, körülményeiről – a 72 (hetvenkettő) órán belüli hatósági bejelentési határidőre tekintettel – értékelést, vizsgálatot végezzenek, illetve az incidens operatív kezelésére maguk közül egy tagot kijelöljenek. A Bizottság elkészíti az incidens kivizsgálására vonatkozó jegyzőkönyvet, dönt az incidens minősítéséről, a szükséges intézkedésekről, az egyes intézkedésekért felelős személyekről és határidőkről.

A bejelentés minősítése során különösen az alábbiakat kell figyelembe venni:

- az incidens eseményének elemzését,
- az érintettek kategóriáit (természetes személy vagy jogi személy ügyfél, ügyfélnek nem minősülő harmadik személy, munkavállaló, hozzátartozók, kiskorú személyek stb.),
- az érintettek – legalább hozzávetőleges – számának beazonosítását,
- az incidenssel érintett adatok kategóriáját (személyazonosító adatok, gazdasági adatok, pénzügyi adatok, családi állapotra vonatkozó adatok stb.),
- az incidenssel érintett adatok hozzávetőleges számát,
- az incidenssel érintett további kockázatok meghatározását,
- a kockázat alacsony vagy magas voltának meghatározását,
- a bekövetkezett károk azonosítását,
- az elhárításra tett intézkedések elemzését.

Amennyiben megállapítják, hogy az adatvédelmi incidens a természetes személyek jogaira és szabadságaira nézve valószínűsíthetően magas kockázattal járhat, a Bizottság adott incidensre kijelölt tagja megkezdi a Hatóság részére a szakaszos bejelentést.

Az incidens bejelentést a Hatóság honlapján kell megtenni. Amennyiben a bejelentés teljesítéséhez további adatok, információk, dokumentumok szükségesek, akkor a Bizottság bejelentésre kijelölt tagja jogosult a Társaság bármely Érintett szervezeti egységét felhívni a kért adatok, információk átadására.

A bejelentés részletekben is teljesíthető, de törekedni kell arra, hogy a tudomásra jutástól számított 72 (hetvenkettő) órán belül legalább a bejelentés megkezdésére sor kerüljön. Amennyiben a bejelentés megkezdése nem kezdődik meg 72 (hetvenkettő) órán belül, akkor a bejelentés mellé mellékelni kell a késedelem igazolására szolgáló indokokat is.

Az érintettek tájékoztatása az adatvédelmi incidensről

A természetes személyek jogaira és szabadságaira nézve magas kockázattal járó adatvédelmi incidensről az Adatkezelő köteles indokolatlan késedelem nélkül tájékoztatni az érintetteket.

A tájékoztatási kötelezettségnek az adatkezelő nevében az Adatvédelmi tisztviselő vagy az Informatikai igazgató tesz eleget.

Az érintettek részére nyújtott tájékoztatásban világosan és közérthetően ismertetni kell az incidens jellegének leírását és azt legalább az alábbi tartalommal kell megadni:

a) az Adatvédelmi tisztviselő és az Informatikai igazgató, illetve a további kapcsolattartásra esetlegesen kijelölt személy nevét és elérhetőségeit;
b) az adatvédelmi incidens valószínűsíthető következményeinek ismertetését;
c) az adatvédelmi incidens orvoslására tett vagy tervezett intézkedések ismertetését, beleértve adott esetben az incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket is;
d) az érintettek által az adatvédelmi incidens orvoslására tehető intézkedések ismertetését, beleértve adott esetben az incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket is.

A tájékoztatást az incidensben érintett személyi kör sajátosságaira tekintettel kell megadni. Amennyiben az érintettek a szervezeten belüli munkaviszonyban vagy munkavégzésre irányuló egyéb jogviszonyban álló személyek, úgy az értesítés a szervezeten belül szokásos módon történik. Egyéb szervezeten kívüli érintettek vonatkozásában a releváns és gyors érdemi tájékoztatás jegyében a rendelkezésre álló kommunikációs csatornákon kell az értesítésnek eleget tenni. A tájékoztatásra használt kommunikációs csatornákat biztonságosan kell megválasztani ügyelve arra is, hogy az incidensben esetlegesen érintett kommunikációs utat mellőzzék.
Figyelemmel kell lenni arra, hogy a tájékoztatás tartalmában egyedi legyen és egyéb tájékoztatással ne szerepeljen együtt.

Az érintettek nagy száma esetén a tájékoztatás helyi vagy országos médián keresztül is történhet, feltéve, hogy a személyes tájékoztatás lehetetlen lenne vagy az Adatkezelőre nézve aránytalan költséggel járna.
Ilyen esetben az Adatkezelő honlapján figyelemfelhívó jelzést kell elhelyezni, amely általános tájékoztatást nyújt az incidens jellegéről, az érintett személyes adatok, illetve az érintettek kategóriáról.

Amennyiben a GDPR 34. cikk (3) bekezdésében foglalt feltételek teljesülése esetén az érintettek tájékoztatása mellőzhető, úgy ennek indokait az Adatvédelmi tisztviselő dokumentálni köteles.

Az adatvédelmi incidensekről vezetett nyilvántartás

Adatvédelmi és Adatbiztonsági Szabályzat
2. számú módosított melléklet

A Társaság, mint adatkezelő nyilvántartást vezet a bejelentett incidensekről, feltüntetve benne az adatvédelmi incidensekhez kapcsolódó tényeket, annak hatásait és az orvoslására tett intézkedéseket. E nyilvántartás lehetővé teszi, hogy a Hatóság ellenőrizze az adatvédelmi incidensek nyilvántartására vonatkozó jogszabályi követelményeknek való megfelelést.

A bejelentett incidens alapján a megvalósítandó további intézkedések végrehajtását figyelemmel kell kísérni.

Az adatvédelmi incidens nyilvántartásában rögzíteni kell:

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

JEGYZŐKÖNYV (minta)

Értekezlet részletei

Az értekezlet neve és célja:	
Dátum és helyszín:	
Jegyzőkönyv száma:	
Jegyzőkönyvvezető:	
Résztvevők neve és munkaköre:	

1. Előzmények:

2. Az esemény besorolása

A leírtak alapján megállapítható, hogy adatvédelmi incidens történt /nem történt, amely ez eset biztonsági incidensnek is minősül egyben / nem minősül. (indok: …)

3. Adatvédelmi incidens jellemzői:

- *Az érintettek jellege:*
- *Az érintettek száma:*
- *Sérülés jelleg:*
- *Adatvédelmi incidens jellege:*
- *Adatvédelmi incidens oka:*
- *Az adatvédelmi incidens körülményei és hatásai:*
- *Az adatvédelmi incidens előtt alkalmazott intézkedések leírása:*
- *Az adatvédelmi incidens következményei:*
- *Az érintett személyes adatok jellege:*

4. Megállapítások és javaslatok:

Tekintettel az adatvédelmi incidens jellegére és súlyossági fokára, valamint annak az érintettre gyakorolt következményeire, illetve hátrányos hatásaira, az Adatvédelmi Bizottság úgy határozott, hogy szükséges /nem szükséges bejelentést tenni a Hatóság felé, az adatvédelmi incidens magas kockázattal jár /nem jár az érintettek jogaira és szabadságaira, azaz a magánszférájukra.

5. Az Adatvédelmi Bizottság javaslatai:

a)

Intézkedés:

Felelős:

Határidő:

...

Kelt:

.....	.....	.....
név, munkakör	név, munkakör jegyzőkönyvvezető	név, munkakör