ÓCSA VÁROS ÖNKORMÁNYZAT
és
ÓCSAI POLGÁRMESTERI HIVATAL

ADATVÉDELMI INCIDENSKEZELÉSI SZABÁLYZAT

Érvényes: 2022. május 16. napjától határozatlan ideig

Bukodi Károly
polgármester

dr. Molnár Csaba
jegyző

1. ÁLTALÁNOS RENDELKEZÉSEK

1.1. A szabályzat célja

Ócsa Város Önkormányzat (a továbbiakban: Önkormányzat) és Polgármesteri Hivatal (a továbbiakban: Hivatal) mint adatkezelő a kezelésében lévő személyes adatokat érintő adatvédelmi incidensek kezelésével összefüggő kötelezettségei teljesítése érdekében megalkotja a jelen adatvédelmi incidenskezelési szabályzatot (a továbbiakban: Szabályzat).

A Szabályzat meghatározza az Önkormányzat és a Hivatal működése során a kezelt személyes adatokat érintő adatvédelmi incidens bekövetkezése esetén követendő eljárásrendet, így különösen a bekövetkezett adatvédelmi incidensek észlelésére, nyilvántartására, hatósági bejelentésére, érintetti tájékoztatására, következményeinek enyhítésére, elhárítására vonatkozó szabályokat a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről szóló 2016/679 európai parlamenti és tanácsi rendelet (a továbbiakban: GDPR) és az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Info tv.) vonatkozó rendelkezéseivel összhangban.

1.2. A Szabályzat hatálya

(1) A Szabályzat személyi hatálya kiterjed az Önkormányzatra, így a képviselőtestület és a bizottságok tagjaira, a polgármesterre, alpolgármesterre, a Hivatalra, annak valamennyi önálló szervezeti egységére (Iroda), annak – foglalkoztatási jogviszony jellegétől függetlenül – valamennyi dolgozójára (köztisztviselő, ügykezelő, munkavállaló, a továbbiakban együttesen: munkatársak), továbbá az Önkormányzattal vagy a Hivatallal a személyes adatok kezelésével összefüggő szerződéses jogviszonyban végző harmadik személyekre (a továbbiakban együttesen: Adatkezelő).

(2) A Szabályzat tárgyi hatálya kiterjed az Adatkezelő kezelésében lévő személyes adatot érintő valamennyi adatvédelmi incidensre.

(3) A Szabályzat az Önkormányzat és a Hivatal Adatvédelmi és Adatbiztonsági Szabályzatával összhangban alkalmazandó, összeütközés esetén a Szabályzat rendelkezései az irányadóak.

(4) A Szabályzat a szokásos módon történő kihirdetés útján lép hatályba.

(5) A munkatársak a Szabályzat megismerést a Szabályzat 1. melléklete szerinti Megismerési nyilatkozat aláírásával ismerik el.

1.3. Fogalommagyarázat

(1) 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. Az olyan biztonsági incidens, amely nem érint személyes adatot nem minősül adatvédelmi incidensnek.

(2) Az adatvédelmi incidensek jellegük szerint három fő elv szerint kategorizálhatók, azzal, hogy az incidens konkrét körülményeitől függően több kategória is érintett lehet egyidejűleg:

- Bizalmassági incidens: a személyes adatok jogosulatlan vagy véletlen közlése, illetve az ilyen adatokhoz való jogosulatlan vagy véletlen hozzáférés;
- Integritási incidens: a személyes adatok jogosulatlan vagy véletlen módosítása;
- Hozzáférhetőségi incidens: a személyes adatokhoz való hozzáférés véletlen vagy jogosulatlan elvesztése, illetve a személyes adatok véletlen vagy jogosulatlan megsemmisítése.

(3) A személyes adatok – előre nem tervezett – átmeneti elvesztése adatvédelmi incidensnek minősülhet, mivel az adatokhoz való hozzáférés hiánya jelentős kihatással lehet az érintett jogaira és szabadságaira.

(4) Adatvédelmi incidens különösen, de nem kizárólag:

- adathalászat (pl. telefonos adathalászat során információ megszerzése; vagy biztonsági hiba miatt titkos átirányítás egy hamis weboldalra, ahol a felhasználói fiók feletti ellenőrzést megszerzi a támadó);
- a személyes adatok nem kerültek megsemmisítésre egy elavult eszközön (elektronikus hulladék keletkezett);
- eszköz elhagyása, ellopása (pendrive, laptop, számítógép, telefon, rajta személyes adatokkal);
- az informatikai rendszer feltörése (hackelés);
- személyes adatokat tartalmazó levél elhagyása vagy jogosulatlan felnyitása;
- papír alapú dokumentumok elhagyása, ellopása, illetéktelenek általi megismerése;
- papír alapú dokumentum nem megfelelő megsemmisítése és ezáltal illetéktelenek általi megismerése;
- rosszindulatú számítógépes program az informatikai eszközökön;
- elektronikus dokumentumok illetéktelenek általi megismerése;
- személyes adatok szóbeli közlése illetéktelen személyekkel;
- személyes adatok jogellenes közzététele nyilvánosság előtt;
- személyes adatok téves címzett részére történő elküldése.

2. RÉSZLETES RENDELKEZÉSEK

2.1. Alapvető rendelkezések

(1) Az Adatkezelő az adatkezelésre vonatkozó egyéb szabályzatokra is figyelemmel minden szükséges intézkedést megtesz a személyes adatok megfelelő szintű biztonságának garantálása, így az adatvédelmi incidensek megakadályozása érdekében.

(2) A Szabályzatban foglaltak szerint:

- a személyes adatok biztonságát érintő összes esemény, incidens esetén haladéktalanul tájékoztatni kell a felelős személyt;
- fel kell mérni az incidens lehetséges hatásait, az egyéneket érintő kockázatokat;
- szükség esetén az incidensről bejelentést kell tenni a Nemzeti Adatvédelmi és Információszabadság Hatóságnak (NAIH) mint felügyeleti hatóságnak (a továbbiakban: felügyeleti hatóság);
- szükség esetén az incidensről tájékoztatni kell az érintettet;
- gondoskodni kell az incidens elhárításáról, a hatások mérsékléséről;
- vezetni kell az adatvédelmi incidens-nyilvántartást (a továbbiakban: incidens-nyilvántartás).

(3) A 2.4. pont (1) bekezdése szerinti határidőn belül az Adatkezelőnek fel kell mérnie az egyéneket valószínűleg érintő kockázatot annak megállapítása céljából, hogy fennáll-e a felügyeleti hatóság felé a bejelentési, illetve az érintettek irányába az értesítési kötelezettség, és milyen intézkedést kell tenni az adatok sérelmének kezelése érdekében.

(4) Az Adatkezelő az elszámoltathatóság elvének biztosítása érdekében az incidenskezeléssel kapcsolatos eljárását dokumentálni kötetes a Szabályzat rendelkezéseinek megfelelően.

(5) Amennyiben egy adott adatvédelmi incidens esetében ez értelmezhető, az Adatkezelőnek az adatkezelésre, adatbiztonságra vonatkozó egyéb szabályzatok alapján helyreállítási stratégiákat és eljárásokat kell kialakítania, ideértve a biztonsági másolatok készítését, az incidensek esetén történő helyreállítást és az adatok kezelési stratégiáit, tekintettel arra, hogy az Adatkezelő számára fontos annak megállapítása, hogy a rendelkezésre állás helyreállt-e, vagy helyreállítás alatt áll, figyelemmel arra, hogy az adatok és a feldolgozó rendszerek

visszanyerésének ténye az ilyen személyes adatok megsértése által okozott kár mérséklésének módja.

(6) Az Adatkezelő köteles felmérni, hogy szükséges-e bármilyen szervezési vagy technikai rendszert érintő változtatás, hogy az adatvédelmi incidens a jövőben megelőzhető legyen. A megfelelő intézkedések megtételét követően zárható le az incidenskezelési folyamat.

2.2. Az adatvédelmi incidens észlelése

(1) Az Adatkezelő az adatkezelésre vonatkozó egyéb szabályzatokra is figyelemmel megfelelő technikai és szervezési intézkedések útján mindent megtesz az adatvédelmi incidensek időben történő észlelése, kezelése érdekében.

(2) Abban az esetben, ha az Adatkezelő más forrásból értesül először az esetlegesen bekövetkezett adatvédelmi incidensről, vagy saját maga észlel biztonsági incidenst, rövid vizsgálatot folytat le annak megállapítása érdekében, hogy valóban sérültek-e a személyes adatok, tehát történt-e ténylegesen adatvédelmi incidens. E vizsgálat ideje alatt nem tekinthető úgy, hogy az Adatkezelő tudomására jutott az incidens.

(3) A személyes adatok megsértésének észlelésekor vagy erre irányuló bejelentés esetén az Adatkezelőnek az incidens-nyilvántartás szerinti, de minimálisan az alábbi információkat biztosítania kell az adatvédelmi tisztviselő részére:

- az incidensről való tudomásszerzés módja és ideje;
- incidens rövid leírása;
- észlelés időpontja:
- érintettek köre;
- érintettek – hozzávetőleges – száma;
- az érintett adatok kategóriái, hozzávetőleges száma;
- annak tényét, hogy az incidens érinti-e az Adatkezelő informatikai rendszert vagy sem;
- milyen azonnali lépéseket tettek a jogsértés felfedezése után;
- vonatkozó szabályzatok és eljárások dokumentációja.

(4) Az Adatkezelőnek az incidens akkor jutott a tudomására, amikor az Adatkezelő észszerű bizonyossággal meggyőződött arról, hogy olyan biztonsági esemény történt, amelynek következtében a személyes adatok veszélybe kerültek, amely a személyes adatokkal kapcsolatos jogellenes műveletekhez vezethet.

(5) Az adatvédelmi incidens tudomásra jutása esetén az incidens-nyilvántartásban megjelölt adatköröket dokumentálni kell.

2.3. Az adatvédelmi incidens lehetséges következményei, kockázatértékelés

(1) Az Adatkezelőnek az incidensről való tudomásszerzést követően az incidens elhárításra mellett az incidens hatásait és a felmerülő kockázatokat is fel kell mérnie, így meg kell állapítania, hogy melyek az incidens lehetséges következményei, ezek milyen valószínűséggel következhetnek be, hogyan érinthetik az érintettek jogait és szabadságait, milyen súlyossággal járhatnak.

(2) A kockázatértékelés során az Adatkezelő értékeli az incidens érintett egyénekre gyakorolt hatásai bekövetkezésének valószínűségét és lehetséges súlyosságát, amelynek ismeretében az Adatkezelő

- könnyebben tud hatékony intézkedéseket hozni az incidens elhárítására és kezelésére;
- gördülékenyebben meg tudja állapítani, hogy kell-e a felügyeleti hatóságnak bejelentést tenni, és szükség esetén az érintett egyéneket értesíteni.

(3) A kockázatértékelés során az Adatkezelő az alábbi tényezőket vizsgálja és mérlegeli:

- az incidens jellege (bizalmassági, integritási, hozzáférhetőségi);
- a személyes adatok jellege, érzékenysége, kategóriái és mennyisége;
- az érintettek kategóriái (pl.: kiszolgáltatott személy, gyermek, idős, beteg) és száma;
- az érintettek közvetlen vagy közvetett azonosíthatósága;
- az érintettekre nézve fennálló következmények valószínűsége, súlyossága, tartóssága;

- az álnevesítés „visszafordíthatóságának" valószínűsége, a bizalmasság sérülése;
- az érintett adatok olvashatósága, megfelelő védelmi intézkedések megléte;
- személyazonossági csalás, pénzügyi veszteség, a személyes adatokkal való visszaélés egyéb formáinak valószínűsége;
- a személyes adatokat felhasználhatják-e vagy valószínűsíthetően felhasználják-e rosszindulatúan;
- annak valószínűsége, hogy az incidens az érintettek fizikai, vagyoni vagy nem vagyoni kárát okozza, és ennek súlyossága;
- a jogsértés hátrányos megkülönböztetést, jó hírnév sérelmét vagy az érintettek egyéb alapvető jogainak sérelmét eredményezheti-e;
- az egyén sajátosságai;
- az Adatkezelő és tevékenységes sajátosságai.

(4) Az adatvédelmi incidenseknek különféle, jelentősen hátrányos hatásai lehetnek az érintettre, ezek a hatások pedig fizikai, vagyoni vagy nem vagyoni károkhoz vezethetnek.

(5) Az érintettek vonatkozásában kár lehet:
- a személyes adatok feletti rendelkezés elvesztése vagy a jogok korlátozása;
- hátrányos megkülönböztetés;
- személyazonosság-lopás vagy a személyazonossággal való visszaélés;
- pénzügyi veszteség;
- az álnevesítés engedély nélküli feloldása;
- a jó hírnév sérelme, becsület csorbítása;
- szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülése;
- egyéb jelentős gazdasági vagy szociális hátrány.

(6) Amennyiben az adatvédelmi incidens
- a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre, szakszervezeti tagságra utaló személyes adatokat érint,
- genetikai adatokra, egészségügyi adatokra, szexuális irányultságára vonatkozó adatokra, büntetőjogi felelősség megállapítására vonatkozó határozatokra és a bűncselekményekre, illetve a kapcsolódó biztonsági intézkedésekre vonatkozó adatokra is kiterjed,
- személyes jellemzők értékelésére, kiszolgáltatott személyek személyes adatai kezelésére kerül sor,
- nagy mennyiségű adatot érint, amely nagyszámú érintettre vonatkozik,

akkor a 2.3. pont (5) bekezdése szerinti károk valószínűleg bekövetkeznek.

(7) Az Adatkezelő az adatvédelmi incidens súlyosságának értékelésére elsődlegesen az Európai Uniós Hálózat- és Információbiztonsági Ügynökség (ENISA) által közzétett módszertant (Recommendations for a methodology of the assessment of severity of personal data breaches Working Document, v1.0, December 2013) használja, azzal, hogy az nem feltétlenül alkalmazható egy az egyben valamennyi adatvédelmi incidensre, így az adott incidens sajátosságait minden esetben figyelembe kell venni.

(8) Amennyiben a felügyeleti hatóság az adatvédelmi incidensek értékelésével összefüggésben a 2.3. pont (7) bekezdése szerinti módszer helyett más módszertan alkalmazását írja elő, úgy az Adatkezelő azt alkalmazza.

2.4. Az adatvédelmi incidens bejelentése

(1) Az Adatkezelő az adatvédelmi incidenst indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, köteles bejelenteni a felügyeleti hatóságnak, amennyiben a 2.4. pont (9) bekezdése szerinti feltétel nem áll fenn (teljes bejelentés).

(2) Ha a bejelentés nem történik meg 72 órán belül, a bejelentéshez mellékelni kell a késedelem igazolására szolgáló indokokat is.

(3) Amennyiben az incidensek viszonylag rövid időn belül ugyanolyan módon megsértett, azonos jellegű személyes adatokat érintenek az Adatkezelő az összes incidensre vonatkozó

összevont bejelentést is benyújthat. Összevont bejelentést több hasonló, 72 órán belül jelentett incidensről is tehető.

(4) Amennyiben sorozatosan következnek be olyan incidensek, amelyek különböző módon megsértett, eltérő jellegű személyes adatokat érintenek, akkor a bejelentést a 2.4. pont (1) bekezdése szerinti módon kell megtenni.

(5) A bejelentés legalább az alábbi információkat tartalmazza:
- incidens jellegének leírása;
- az érintettek kategóriái és hozzávetőleges száma;
- az incidenssel érintett adatok kategóriái és hozzávetőleges száma;
- az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó neve és elérhetőségei;
- az adatvédelmi incidensből eredő, valószínűsíthető következmények ismertetése;
- az Adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedések ismertetése, beleértve az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket is.

(6) Az adatvédelmi incidens függvényében, amennyiben nem lehetséges az információk egyidejű közlése és az Adatkezelőnek további vizsgálatot kell lefolytatnia, az Adatkezelő az információkat indokolatlan késedelem nélkül részletekben is közölheti. Ilyen esetben az incidens első alkalommal történő bejelentésével egyidejűleg arról is tájékoztatni kell a felügyeleti hatóságot, hogy az Adatkezelő nem rendelkezik az összes szükséges információval, a későbbiekben további részleteket fog közölni (szakaszos bejelentés).

(7) A bejelentést elektronikus úton a felügyeleti hatóság erre rendszeresített online felületén (https://www.naih.hu/adatvedelmi-incidensbejelent--rendszer.html), vagy e-papír szolgáltatáson keresztül kell benyújtani.

(8) A bejelentésben lehetőség szerint a 2.4. pont (5) bekezdésében megjelölt információkon kívül egyéb információkat is meg kell adni.

(9) Az adatvédelmi incidenst nem kell bejelenteni a felügyeleti hatóságnak, amennyiben az valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Ezen körülmények minden egyes incidens esetén külön-külön vizsgálandóak.

2.5. Érintett tájékoztatása

(1) Amennyiben az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az Adatkezelő indokolatlan késedelem nélkül tájékoztatja az érintettet az adatvédelmi incidensről.

(2) Az érintett részére nyújtott tájékoztatás világosan és közérthetően legalább az alábbi információkat tartalmazza:
- az incidens jellegének leírása;
- adatvédelmi tisztviselő vagy további tájékoztatást nyújtó egyéb kapcsolattartó neve és elérhetőségei;
- az adatvédelmi incidensből eredő, valószínűsíthető következmények ismertetése;
- az Adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedések ismertetése, beleértve az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket is.

(3) Az incidens jellegére tekintettel az Adatkezelő arról is tájékoztatja az érintettet, hogy hogyan tud védekezni a lehetséges hátrányos következményekkel szemben.

(4) Az incidensről szóló tájékoztatáshoz kifejezetten erre vonatkozó üzenetet kell alkalmazni, az nem küldhető más jellegű tájékoztatással (pl.: hírlevél) együtt.

(5) Az Adatkezelő az incidensről szóló tájékoztatáshoz nem használhat incidens által veszélyeztetett kapcsolattartási csatornát.

(6) Főszabály szerint az érintetteket közvetlenül kell tájékoztatni az incidensről, ennek érdekében szükség esetén többféle tájékoztatási eszköz is igénybe vehető (pl.: SMS, levél, e-mail).

(7) Az Adatkezelő felveheti a kapcsolatot a felügyeleti hatósággal és konzultálhat vele nemcsak arról, hogy szükséges-e tájékoztatni az érintetteket az adatvédelmi incidensről, hanem arról is, hogy milyen tartalmú üzenetet küldjenek nekik és mi a legalkalmasabb mód az érintettekkel való kapcsolatfelvételre.

(8) Amennyiben célszerű, az érintett egyének tájékoztatásáról a felügyeleti hatósággal együttműködve kell gondoskodni, szükség esetén betartva más érintett hatóságok útmutatását, ez alapján indokolt esetben az Adatkezelő értesítési kötelezettségét késleltetve teljesítheti (pl.: incidens körülményeinek kivizsgálása indokolja a későbbi értesítést).

(9) Az érintett egyéneket nem szükséges közvetlenül értesíteni az alábbi esetekben:

- az Adatkezelő az incidens bekövetkezése előtt megfelelő technikai és szervezési intézkedéseket alkalmazott a személyes adatok védelme érdekében, ideértve különösen azokat az intézkedéseket, amelyek a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik az adatokat (pl.: a személyes adatok legkorszerűbb titkosítással történő védelme);
- az Adatkezelő rögtön az incidenst követően olyan további intézkedéseket tett, amelyek biztosítják, hogy az érintett jogaira és szabadságaira jelentett magas kockázat a továbbiakban valószínűsíthetően nem valósul meg (pl.: előfordulhat, hogy az Adatkezelő azonnal azonosította azt az egyént, aki még azelőtt hozzáfért a személyes adatokhoz, mielőtt bármit lehetett volna velük kezdeni, és intézkedéseket hozhatott vele szemben. Ilyen esetben is kellő figyelmet kell fordítani a titoksértés lehetséges következményeire az érintett adatok jellegétől függően);
- az érintettekkel való kapcsolatfelvétel és egyedi tájékoztatás aránytalan erőfeszítést tenne szükségessé, amely esetben az Adatkezelőnek nyilvánosan közzétett információk útján kell tájékoztatnia az érintetteket vagy olyan hasonló intézkedést kell hoznia, amely biztosítja a hasonlóan hatékony tájékoztatást (pl.: érintettek elérhetőségi adatai az incidens következtében elvesztek, vagy eleve nem is voltak ismertek, így megfelelő lehet a honlapon történő tájékoztatás, kiemelt újsághirdetés vagy közlemény közzététele).

(10) A 2.5. pont (9) bekezdésében foglalt feltétel fennállát az Adatkezelőnek kell bizonyítania.

(11) Ha az Adatkezelő még nem értesítette az érintettet az adatvédelmi incidensről, a felügyeleti hatóság, miután mérlegelte, hogy az adatvédelmi incidens valószínűsíthetően magas kockázattal jár-e, elrendelheti az érintett tájékoztatását, vagy megállapíthatja a 2.5. pont (9) bekezdésében foglalt feltételek valamelyikének teljesülését.

(12) Az érintetti tájékoztatás megtörténtét az Adatkezelőnek bizonyítania kell tudni.

2.6. Incidens-nyilvántartás

(1) Az Adatkezelő az elszámoltathatóság elvének biztosítása céljából elektronikus úton naprakészen nyilvántartja az adatvédelmi incidenseket az incidens-nyilvántartásban.

(2) Az incidens-nyilvántartásban az alábbi információk megadása minden esetben kötelező:

- incidenshez kapcsolódó tények (incidens időpontja, oka, a bekövetkezése, az érintettek száma és köre, az érintett személyes adatok száma és köre);
- az incidens hatásainak és következményeinek leírása;
- az incidens hatásainak és következményeinek orvoslására tett intézkedések és a döntés indokolása.

(3) Az incidens-nyilvántartásba valamennyi adatvédelmi incidenst rögzíteni kell, függetlenül annak súlyosságától, illetve függetlenül attól, hogy a felügyeleti hatóság felé bejelentési, illetve az érintett felé tájékoztatási kötelezettség fennáll-e.

(4) Az incidens-nyilvántartást az Adatkezelő mindaddig megőrzi, amíg a felügyeleti hatóság felszólíthatja arra, hogy szolgáltasson bizonyítékot a jogszabályokban rögzített nyilvántartási elemek vagy általánosabban az elszámoltathatósági elv betartására.

(5) Amennyiben az incidens-nyilvántartás nem tartalmaz személyes adatot, úgy az adott incidensre vonatkozó információ időbeli korlát nélkül tárolható. Amennyiben az incidens-nyilvántartás személyes adatot is tartalmaz, úgy az Adatkezelőnek megfelelő jogalapot és megőrzési időszakot is meg kell állapítania a személyes adat vonatkozásában.

(6) Amennyiben az Adatkezelő késedelmesen jelenti be az incidenst a felügyeleti hatóságnak, úgy a késedelem okát az incidens-nyilvántartásban is rögzíteni kell.

(7) Az incidens-nyilvántartás lehetővé teszi, hogy a felügyeleti hatóság ellenőrizze a jogszabályoknak történő megfelelést.

3. AZ ADATVÉDELEM SZERVEZETE

3.1. Az adatkezelésben részt vevő szervek és személyek

(1) Az adatvédelmi incidens kezelésére vonatkozó szabályok a Szabályzat 1.2. pont (1) bekezdésében megjelölt valamennyi személyre vonatkoznak, ezen személyek kötelesek a Szabályzatban és a személyes adatok kezelésére vonatkozó egyéb szabályzatban, utasításban előírt rendelkezéseket megismerni és betartani.

3.2. A jegyző

(1) A jegyző mint a Hivatal vezetője a felelős az adatvédelmi incidensek kezelésére vonatkozó rendelkezések érvényesítéséért, az ehhez szükséges személyi, tárgyi és technikai feltételek biztosításáért.

(2) Az adatvédelmi incidensek kezelésével kapcsolatos feladatokat a jegyző az adatvédelmi tisztviselő és a szervezeti egységek vezetői útján látja el.

(3) Az adatvédelmi incidensek kezelésével kapcsolatos feladati körében a jegyző

- kiadja a Szabályzatot;
- ellenőrzi a Szabályzat érvényesülését;
- felelős az adatvédelmi incidenssel összefüggésben feltárt hiányosságok, jogszabálysértő körülmények megszüntetéséért;
- dönt az incidensek megelőzését szolgáló helyesbítő és megelőző intézkedések bevezetéséről, kijelöli a felelősöket és a végrehajtás határidejét;
- dönt az incidensek elhárítását, megszüntetését, hatásait csökkentő intézkedések alkalmazásáról, kijelöli a felelősöket és a végrehajtás határidejét;
- a tudomására jutott visszásság esetén utasítja az érintett munkatársat az incidens megszüntetésére, következményei elhárítására;
- döntést hoz a felügyeleti hatósághoz történő bejelentés, valamint az érintetti tájékoztatás szükségességéről;
- amennyiben az adatvédelmi incidens bejelentése szükséges a felügyeleti hatóság felé, megteszi a bejelentést;
- amennyiben az adatvédelmi incidensről az érintettek értesítése szükséges, értesíti az érintetteket;
- minden eszközt és információt biztosít az adatvédelmi tisztviselő számára ahhoz, hogy az adatvédelmi tisztviselő el tudja látni a feladatát;
- lefolytatja az adatvédelmi incidens kivizsgálását.

3.3. Az adatvédelmi tisztviselő

(1) Az adatvédelmi tisztviselő tájékoztat és szakmai tanácsot ad az adatvédelmi incidens megelőzésével, bekövetkezett incidens kezelésével kapcsolatban, így különösen:

- az esemény incidensként történő minősítése,
- az adatvédelmi incidenskezelési folyamat megvalósítása,
- az adatvédelmi incidens érintettek jogaira és szabadságaira gyakorolt hatásai, a kockázatok és következmények értékelése,
- az adatvédelmi incidens hatásainak mérséklése érdekében meghozandó megfelelő intézkedések,
- helyesbítő és megelőző intézkedések bevezetése,

- az adatvédelmi incidens felügyeleti hatóság részére történő bejelentésének szükségessége,
- az adatvédelmi incidens érintettek részére történő értesítése,
- közös adatkezelő/adatfeldolgozó részére az adatvédelmi incidenssel kapcsolatos kötelezettségek és felelősség

tárgyában.

(2) Az adatvédelmi tisztviselő az adatvédelmi incidenssel összefüggésben ellátja a következő feladatokat:

- az Adatkezelő bármely szervezeti egységénél, bármely munkatársánál jogosult ellenőrzést végezni, tájékoztatást kérni;
- az Adatkezelő bármely szervezeti egységét, annak vezetőjét, munkatársát bevonhatja az incidens kivizsgálásába;
- az adatvédelmi incidenssel összefüggő kérdésekben segítséget nyújt a munkatársak részére;
- amennyiben szükséges az incidens felügyeleti hatóság részére történő bejelentése, előkészíti a bejelentést, a bejelentésről készített másolatot mellékeli az eseményt rögzítő incidens-nyilvántartáshoz;
- amennyiben szükséges az érintettek tájékoztatása az incidensről, előkészíti az érintettek tájékoztatására szolgáló dokumentumot;
- ellenőrzi az adatvédelemre vonatkozó szabályok, különösen a Szabályzat rendelkezéseinek érvényre juttatását, betartását;
- javaslatot tesz az incidens-nyilvántartás szerkezetére, összeállítására, kezelésére;
- gondoskodik az incidens-nyilvántartás vezetéséről;
- az incidens bekövetkezte esetén együttműködik a felügyeleti hatósággal;
- az incidenssel összefüggésben kapcsolattartó pontként szolgál a felügyeleti hatóság és az érintettek felé;

3.4. A szervezeti egységek vezetői

(1) A szervezeti egység vezetője

- köteles a vezetése alá tartozó szervezeti egységnél az adatvédelmi incidensek elkerülése érdekében szükséges intézkedéseket meghozni;
- a vezetése alá tartozó szervezeti egységnél bekövetkezett adatvédelmi incidensről haladéktalanul tájékoztatja a jegyzőt, illetve az adatvédelmi tisztviselőt;
- minden szükséges intézkedést megtesz az incidens megszüntetése érdekében, szükség esetén részt vesz az incidens kivizsgálásában.

3.5. Munkatársak

(1) Valamennyi munkatárs köteles

- a Szabályzatot megismerni és betartani;
- minden szükséges intézkedést megtenni az adatvédelmi incidens elkerülése, késedelem nélküli elhárítása, megszüntetése, hatásai csökkentése érdekében;
- a tudomására jutott személyes adatok biztonságát érintő eseményről, az adatvédelmi incidensről haladéktalanul – lehetőség szerint elektronikus úton írásban is – tájékoztatni a szervezeti egység vezetőjét, a jegyzőt, illetve az adatvédelmi tisztviselőt, elektronikus dokumentumokat, informatikai rendszereket érintő biztonsági esemény, incidens esetén az informatikust.

(2) A munkatársak kötelesek az adatvédelmi incidens kivizsgálásában közreműködni és a kivizsgáláshoz, az incidens-nyilvántartás vezetéséhez, a felügyeleti hatóság részére történő bejelentéshez, illetve az érintetti tájékoztatáshoz szükséges valamennyi információval az adatvédelmi tisztviselő munkáját segíteni.

(3) A munkatársak kötelesek jelenteni azt is, ha egy adatkezelési művelet során fennáll az adatvédelmi incidens lehetősége, javaslatokat tehetnek szervezési, technikai intézkedésekre, amelyekkel az incidens megelőzhető.

3.6. Az informatikus

(1) Az informatikus köteles:
- az elektronikus dokumentumokat, informatikai rendszereket érintő incidens esetén soron kívül, de legkésőbb 24 órán belül megtenni mindazon intézkedéseket, amelyek az incidens megszüntetése, a rendszer helyreállítása érdekében szükségesek;
- szükség esetén értesíteni az információbiztonsági felelőst;
- javaslatot tenni olyan szervezési, technikai megoldásokra, amelyek az incidensek megelőzését elősegítik.

(2) Az informatikus köteles az adatvédelmi incidens kivizsgálásában közreműködni – ide nem értve a papír alapú dokumentumok kezelése során bekövetkezett incidenseket –, és a kivizsgáláshoz, az incidens-nyilvántartás vezetéséhez, a felügyeleti hatóság részére történő bejelentéshez, illetve az érintetti tájékoztatáshoz szükséges valamennyi információval az adatvédelmi tisztviselő munkáját segíteni.

3.7. Közös adatkezelők

(1) Amennyiben közös adatkezelésre kerül sor, az Adatkezelő a másik adatkezelővel írásban köteles megállapodni az adatvédelmi incidens felügyeleti hatóságnak történő bejelentésével, illetve az érintettek tájékoztatásával kapcsolatos kötelezettségek teljesítésének rendjéről, így a felelős adatkezelő kijelöléséről.

3.8. Adatfeldolgozó

(1) Az adatfeldolgozó segíti az Adatkezelőt az adatvédelmi incidens kezelésében, a felügyeleti hatóságnak történő bejelentésével, illetve az érintettek tájékoztatásával kapcsolatos kötelezettségi teljesítésében, figyelembe véve az adatkezelés jellegét és az adatfeldolgozó rendelkezésére álló információkat.

(2) Az adatfeldolgozó az Adatkezelő nevében általa kezelt személyes adatokat érintő adatvédelmi incidenst az arról való tudomásszerzést követően haladéktalanul köteles bejelenteni az Adatkezelőnek, az adatfeldolgozási szerződéses alapján esetlegesen vállalt többletkötelezettségek ellenére is.

(3) Adatvédelmi incidens bekövetkezte esetén az adatfeldolgozó köteles a kötelezettségei teljesítéséhez szükséges valamennyi információt kellő időben és megfelelő formában átadni az Adatkezelőnek.

(4) A 3.8. pont (1) bekezdésétől eltérően az adatfeldolgozó kizárólag abban az esetben teheti meg a bejelentést, illetve az értesítést az Adatkezelő nevében, ha azt az Adatkezelővel kötött adatfeldolgozási szerződés vagy jogszabály így rendelkezik. Ennek ellenére az Adatkezelőnek ez esetben is gondoskodnia kell a válaszintézkedések megtételéről, valamint a megfelelő értesítési és kommunikációs intézkedésekről, tekintettel arra, hogy a funkciók átruházása nem jár a felelősség átruházásával.

(5) Az adatfeldolgozó számára javasolt annak dokumentált igazolása, hogy időben tájékoztatta az Adatkezelőt az adatvédelmi incidensről.

(6) Az adatfeldolgozó köteles megfelelő technikai és szervezési intézkedéseket végrehajtani annak érdekében, hogy időben azonosítani tudja a biztonsági incidenseket és meg tudja állapítani azt, hogy a biztonsági incidens adatvédelmi incidensnek minősül-e.

(7) Az adatfeldolgozóknak képesnek kell lennie annak kielemzésére, hogy egy biztonsági incidens adatvédelmi incidensnek minősül-e. Ezt az elemzést dokumentálnia kell.

(8) Ha az adatfeldolgozó nem tudja eldönteni azt, hogy egy biztonsági incidens adatvédelmi incidensnek minősül-e vagy, ha a biztonsági incidens később adatvédelmi incidenssé válhat, akkor köteles megfelelő időben tájékoztatni az Adatkezelőt az incidensről.

(9) Az adatfeldolgozás tárgyában az Adatkezelő és az adatfeldolgozó között szerződésnek a 3.8. pont szerinti rendelkezéseket tartalmaznia kell, amennyiben az adatfeldolgozóra vonatkozóan ezen rendelkezéseket jogszabály nem szabályozza.

4. ZÁRÓ RENDELKEZÉSEK

A Szabályzatban nem szabályozott kérdésekben a mindenkor hatályos GDPR rendelkezései, továbbá a vonatkozó ágazati jogszabályok, az Adatvédelmi és Adatbiztonsági Szabályzat és a személyes adatok kezelésére vonatkozó egyéb szabályzatok, utasítások rendelkezései az irányadók.

A Szabályzat 2022. május 16. napján lép hatályba és határozatlan időre szól.

A Szabályzat hatályba lépésével egyidejűleg Ócsa Város Önkormányzat és az Ócsai Polgármesteri Hivatal korábbi Incidenskezelési Szabályzata hatályát veszti

Ócsa, 2022. május 16.

A Szabályzathoz tartozó mellékletek listája:

1. SZÁMÚ MELLÉKLET: Megismerési nyilvántartás
2. SZÁMÚ MELLÉKLET: Adatvédelmi incidens-nyilvántartás (.xlsx)
3. SZÁMÚ MELLÉKLET: Minta érintetti tájékoztató

Ócsa Város Polgármestere

Bukodi Károly
polgármester

Ócsa Város Jegyzője

dr. Molnár Csaba
jegyző