JÓZSEFVÁROSI GAZDÁLKODÁSI KÖZPONT ZRT.

VEZÉRIGAZGATÓ

20/2025. (V. 07.) számú utasítás

az adatvédelmi incidensek kezeléséről

1. A Józsefvárosi Gazdálkodási Központ Zrt. (a továbbiakban: JGK Zrt.) által végzett személyes adatkezelés során bekövetkező incidens (a továbbiakban: adatvédelmi incidens) esetére, az adatvédelmi incidens hatályos jogszabályoknak és iránymutatásoknak megfelelő kezelésének biztosítása érdekében a mellékelt szabályzatot adom ki.

2. Az utasítás 2025. május 08. napján lép hatályba, a hatályba lépéssel egyidejűleg az Igazgatóság 25/2024. (IX. 24.) számú határozatával 2024. szeptember 24-én hatályba léptetett szabályzat hatályát veszti.

Budapest, 2025. május 7.

Józsefvárosi Gazdálkodási Központ Zrt. 1

Borbás Gabriella
vezérigazgató

ADATVÉDELMI INCIDENSEK KEZELÉSE SZABÁLYZAT

I. Bevezetés

1. 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 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, illetve a szóban forgó természetes személyeket sújtó egyéb jelentős gazdasági vagy szociális hátrányt.

II. Általános rendelkezések

2. A szabályzat célja, hogy a JGK Zrt. területén (székhelyén, telephelyein) megakadályozza a jogosulatlan hozzáférést, az adatok megváltoztatását és jogosulatlan nyilvánosságra hozatalát, a személyes adatok jogosulatlan kezelését, biztosítsa a személyes adatok biztonságára vonatkozó követelmények érvényesülését, figyelemmel a JGK Zrt. adatvédelmi szabályzatában foglalt kapcsolódó rendelkezésekre.
   Ezzel együtt amennyiben a személyes adat jogellenes kezelése vagy feldolgozása, így különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés következik be, úgy biztosítani lehessen a kivizsgáláshoz szükséges adatokat, eljárásrendet.

3. A szabályzat hatálya a JGK Zrt. valamennyi a Munka Törvénykönyvéről szóló 2012. évi I. törvény (a továbbiakban: Mt.) hatálya alatt álló, illetve megbízási, vagy munkavégzésre irányuló egyéb jogviszony keretében foglalkoztatott munkatársakra – a JGK Zrt. működésével kapcsolatba kerülő minden természetes személy jogainak érvényesítése, adott esetben jogsértő magatartásának bizonyítása szempontjából – kiterjed.
4. A JGK Zrt. tulajdonában lévő, a JGK Zrt. által, valamint a megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által kezelt

- személyes, különleges adatokra valamennyi belső kamerára (képfelvevő berendezésre, elektronikus megfigyelő rendszerre), és a hozzájuk kapcsolódó számítástechnikai, informatikai berendezésre (ideértve a mobil eszközöket és az együttműködési megállapodás keretében használt lekérdező klienseket is), valamint ezek műszaki dokumentációjára is,
- rendszer- és felhasználói programokra,
- védelmet élvező adatok teljes körére, keletkezésük és feldolgozási helyüktől, idejüktől és az adatok fizikai megjelenési formájától függetlenül,
- adatok felhasználására, tárolására vonatkozó utasításokra,
- adathordozók tárolására, felhasználására, valamint
- a számítástechnikai folyamatban szereplő összes dokumentációra (fejlesztési, szervezési, programozási, üzemeltetési dokumentáció).

5. **Az adatvédelmi incidens fogalma**: 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.

6. Biztosítani kell az alapvető jogok érvényesülését a JGK Zrt. valamennyi szervezeti egységénél folyó személyes adatkezelés szempontjából érintett munkavégzés során, másrészt az előírt feladatok ellátása keretében érvényt kell szerezni az adatvédelem szabályainak, az érintett tájékoztatására vonatkozó előírások betartásának. Ezen túlmenően az érintetteket megillető, és a jogszabályok által rögzített jogok érvényesülését is biztosítani szükséges.

III. Részletes szabályok

7. A JGK Zrt. az általa, illetve a megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által kezelt adatokkal összefüggésben felmerült adatvédelmi incidens kapcsán rögzíti a természetes személyek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet) szóló az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. 04.27.) (a továbbiakban: GDPR) 33. cikk (3) bekezdés a), c) és d) pontja szerinti adatokat, valamint az adatvédelmi incidenst a (3) bekezdés b.) pontjában szereplő adatokkal együtt haladéktalanul, de legfeljebb az adatvédelmi incidensről való tudomásszerzését követően 72 órával bejelenti a Nemzeti Adatvédelmi és Információszabadság Hatóságnak (a továbbiakban: NAIH).

8. Az adatvédelmi incidenst nem kell bejelenteni, ha valószínűsíthető, hogy az nem jár kockázattal az érintettek jogainak érvényesülésére.

9. Amennyiben a JGK Zrt. érintett munkatársa meghatározott bejelentési kötelezettséget akadályoztatása miatt határidőben nem teljesítette, azt az akadály megszűnését követően haladéktalanul teljesíteni kell és a bejelentéshez mellékelni a késedelem okait feltáró nyilatkozatot is.

10. Amennyiben az adatvédelmi incidens az adatfeldolgozó tevékenységével összefüggésben merült fel vagy azt egyébként az adatfeldolgozó észleli, arról – az adatvédelmi incidensről való tudomásszerzését követően – haladéktalanul tájékoztatja a JGK Zrt. adatvédelmi tisztviselőjét.

11. A meghatározott bejelentési kötelezettség keretei között a JGK Zrt. adatvédelmi tisztviselője:
    a) ismerteti az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek körét és hozzávetőleges számát, valamint az incidenssel érintett adatok körét és hozzávetőleges mennyiségét,
    b) tájékoztatást nyújt az adatvédelmi tisztviselő vagy a további tájékoztatás nyújtására kijelölt más kapcsolattartó nevéről és elérhetőségi adatairól,
    c) ismerteti az adatvédelmi incidensből eredő, valószínűsíthető következményeket, és
    d) ismerteti az adatkezelő által az adatvédelmi incidens kezelésére tett vagy tervezett – az adatvédelmi incidensből eredő esetleges hátrányos következmények mérséklését célzó és egyéb – intézkedéseket.

12. Amennyiben a GDPR 33. cikk (3) bekezdés a)-d) pontjában foglalt valamely információ a bejelentés időpontjában nem áll az adatvédelmi tisztviselő rendelkezésére, azzal a bejelentést annak benyújtását követően utólag – az információrendelkezésre állásáról való tudomásszerzését követően haladéktalanul – kiegészíti.

13. Ha az adatvédelmi incidens során olyan adat érintett, amelyet valamely más EGT-állam adatkezelője továbbított az adatkezelő részére, vagy amelyet a JGK Zrt. más EGT-állam adatkezelője részére továbbított, a GDPR 33. cikk (3) a)-d) pontokban meghatározott információkat az adatvédelmi tisztviselő ezen EGT-állam adatkezelőjével haladéktalanul közli.

14. A GDPR 33. cikk (1) bekezdésében meghatározott bejelentési kötelezettséget az adatvédelmi tisztviselő a NAIH által e célra biztosított elektronikus felületen teljesíti. Ha az adatvédelmi incidens valószínűsíthetően az érintettet megillető valamely alapvető jog érvényesülését lényegesen befolyásoló következményekkel járhat (a továbbiakban: magas kockázatú adatvédelmi incidens), az adatvédelmi tisztviselő az érintettet az adatvédelmi incidensről haladéktalanul tájékoztatja.

15. A GDPR 33. cikk (1) bekezdés utolsó fordulatában foglaltak szerinti tájékoztatásának kötelezettsége alól – figyelemmel a 34. cikkben, különösen az (1) bekezdésében foglaltakra – a JGK Zrt. mentesül, ha:
    a) az adatkezelő megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre, és ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében alkalmazták, különösen azokat az intézkedéseket – mint például a titkosítás alkalmazása –, amelyek a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik az adatokat;
    b) az adatkezelő az adatvédelmi incidenst követően olyan további intézkedéseket tett, amelyek biztosítják, hogy az érintett jogaira és szabadságaira jelentett, az (1) bekezdésben említett magas kockázat a továbbiakban valószínűsíthetően nem valósul meg;
    c) a tájékoztatás aránytalan erőfeszítést tenne szükségessé. Ilyen esetekben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, vagy olyan hasonló intézkedést kell hozni, amely biztosítja az érintettek hasonlóan hatékony tájékoztatását.

16. A GDPR 34. cikkben meghatározott tájékoztatási kötelezettség keretei között az adatvédelmi tisztviselő világosan és közérthetően ismerteti az adatvédelmi incidens jellegét, valamint az érintett rendelkezésére bocsátja a 33. cikk (3) bekezdés *b), c)* és *d)* pontjában meghatározott információkat.

17. Ha a NAIH a GDPR 33. cikkben foglaltak szerint teljesített bejelentés alapján azt állapítja meg, hogy az adatvédelmi incidens magas kockázata miatt az érintett tájékoztatása szükséges, a JGK Zrt. az általa még nem teljesített tájékoztatási kötelezettségét e megállapítást követően haladéktalanul teljesíti.

18. Ha az adatvédelmi tisztviselő 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 (3) bekezdésben említett feltételek valamelyikének teljesülését.

19. A JGK Zrt. biztosítja, hogy fizikai vagy műszaki incidens esetén a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását kellő időben vissza lehessen állítani.

20. Az adatvédelmi incidensről a szervezeti egység vezetője a tudomására jutásától számított 1 munkanapon belül adatvédelmi jegyzőkönyvet vesz fel, amelynek mintáját az 1. számú melléklet tartalmazza.

21. Amennyiben az adatvédelmi incidensre külsős természetes személy hívja fel a figyelmet (tesz bejelentést), kérheti adatainak álnevesítését vagy titkosítását figyelemmel a GDPR 32. cikk (1) a) pontjára.

22. A bejelentőt a bejelentés kapcsán – kivéve a szándékosan valótlan tartalommal tett bejelentés esetét –, hátrány nem érheti.

23. Az adatvédelmet sértő események megelőzése és kezelése (az eljárásrend kialakítása, a szükséges intézkedések meghozatala) a vezérigazgató felelőssége és feladata, amely szervezeti struktúrában meghatározott szervezeti egységek vezetői hatáskörének, felelősségének és beszámoltathatóságának szabályozottságán keresztül valósul meg.

    Ennek érdekében a vezetők alapvető kötelezettsége, hogy:
    a) a jogszabályoknak megfelelően működjön a szervezet, és ennek érdekében a szükséges, feladatkörükhöz tartozó szabályozások előkészítésre kerüljenek,
    b) a szabályozottságot, valamint a szabályok betartását minden vezető folyamatosan kísérje figyelemmel, amely elsődleges feltétele az adatvédelmet sértő események megelőzésének,
    c) adatvédelmet sértő esemény észlelése esetén minél gyorsabban kellően hatékony intézkedés történjen annak érdekében, hogy azadatvédelmet sértő esemény megszüntetésre, a hibás belső szabályozás helyesbítésre kerüljön,

24. Minden szervezeti egység vezetője felelős a feladatkörébe tartozó szakterületen észlelt adatvédelmet sértő esemény ismételt előfordulásának megelőzéséhez szükséges intézkedések megtételéért, a bekövetkezett esemény feltárásáért, szükség esetén annak dokumentálásáért, továbbá indokolt esetben a felelősségre vonással és a hiányosságok megszüntetésével kapcsolatos intézkedések kezdeményezéséért és megvalósításuk ellenőrzéséért.

25. A munkavállalók konkrét feladatát, hatáskörét, felelősségét a munkaköri leírások tartalmazzák. Valamennyi dolgozó feladata és kötelessége az észlelt adatvédelmet sértő esemény jelzése a közvetlen vezetője felé és megszüntetésük érdekében javaslatok tétele, valamint az elrendelt intézkedések megvalósítása.

26. Az adatvédelmi incidensről jegyzőkönyvet felvevő az aláírását követően azonnal továbbítja az adatvédelmi tisztviselőnek, amennyiben a jegyzőkönyv felvételében az adatvédelmi tisztviselő személyesen nem vett részt. A JGK Zrt. nyilvántartja az adatvédelmi incidenseket, feltüntetve az ahhoz kapcsolódó tényeket, annak hatásait és az orvoslására tett intézkedéseket.

27. Az adatvédelmi tisztviselő adatai a https://www.jgk.hu/kozerdeku-adatok/tevekenysegre-mukodesre-vonatkozo-adatok/ menüpont alatt érhető el. Az adatvédelmi tisztviselő – elfogadható akadályoztatása kivételével – közreműködik az adatvédelmi incidens kivizsgáláshoz, a következmények enyhítéséhez, orvoslásához kapcsolódó feladatok végrehajtásában.

28. Az adatvédelmi incidensekről nyilvántartást kell vezetni, amely lehetővé teszi, hogy a felügyeleti hatóság ellenőrizze az e követelménynek való megfelelést. A nyilvántartás mintáját az adatvédelmi szabályzat 8. számú melléklete tartalmazza.

29. Bűncselekmény vagy szabálysértés gyanúja esetén a vonatkozó jogszabályok eljárásrendje alapján kell a további intézkedéseket megtenni.

IV. ZÁRÓ RENDELKEZÉSEK

30. A szabályzathoz kapcsolódó személyes adatok védelméért, az adatkezelés jogszerűségéért minden olyan munkavállaló, aki személyes (különleges) adatot kezel felelős, amelynek érvényesítését az adatvédelmi tisztviselő biztosítja.

31. Jelen szabályzatot szükség szerint, de legalább évente kell felülvizsgálni, módosítani vagy visszavonásával új szabályzatot alkotni az adatvédelmi tisztviselő bevonásával. Jelen szabályzat felülvizsgálatáért a Titkárságvezető felel.

32. Jelen szabályzat kihirdetést követő megismerése a Titkárságvezető feladata. Új belépő munkavállalókkal való megismertetését a Személyügyi iroda vezetője végzi a megismerésről szóló, a 2. számú melléklet szerinti megismerési nyilatkozat aláírattatásával.

33. Jelen szabályzatot a JGK Zrt. honlapján közzé kell tenni.

1. számú melléklet

Jegyzőkönyv adatvédelmi incidensről

Készült,

Hely:
Időpont:
Jelen vannak:

1.) Az érintett személyes adatok köre:

2.) Az adatvédelmi incidens jellege:

3.) Az adatvédelmi tisztviselő/tájékoztatást nyújtó kapcsolattartó elérhetősége:

4.) Az adatvédelmi incidens orvoslására/enyhítésére tett intézkedések:

5.) Az adatvédelmi incidenssel érintettek köre és száma:

6.) Az adatvédelmi incidens (vélelmezett) időpontja:

7.) Az adatvédelmi incidens körülményei és hatásai, következményei:

8.) Az adatvédelmi incidenst lehetővé tévő okok:

9.) Az adatvédelmi incidenssel kapcsolatos egyéb adatok:

A jegyzőkönyv lezárásra került: ……..-kor

Kmf.

……. ……
a jegyzőkönyvet felvevő adatvédelmi tisztviselő

2. számú melléklet

Megismerési nyilatkozat

Az adatvédelmi incidens kezelésére vonatkozó eljárásrendben foglaltakat megismertem. Tudomásul veszem, hogy az abban foglaltak munkavégzésemmel összefüggésben kerületek ismertetésre, az abban foglaltakat munkavégzésem során köteles vagyok betartani.

Név	Beosztás	Kelt	Aláírás