EVIN

ERZSÉBETVÁROSI
INGATLANGAZDÁLKODÁSI
NONPROFIT ZRT.

ADATVÉDELMI ÉS ADATKEZELÉSI SZABÁLYZAT

2.0. verzió. Hatályos: 2024. augusztus 1-től visszavonásig.

KIVONAT
Az EU Általános Adatvédelmi Rendelete (GDPR) szempontjai alapján a vállalkozásra adaptált jelen Szabályzat foglalja össze a kötelezettségeket és a szükséges adatvédelmi intézkedéseket.

EVIN
Nonprofit Zrt.

Készítette:	Baksai Zoltán DPO	2024.07.25.
Egyeztette és szakmailag jóváhagyta:		
Jóváhagyta:	dr. Halmai Gyula vezérigazgató	

Tartalom

1. Cél, hatály, fogalmak

1) A jelen Adatvédelmi és Adatkezelési Szabályzat (a továbbiakban: **Szabályzat**) célja, hogy:
   a) meghatározza az EVIN Nonprofit Zrt-nél (a továbbiakban: Adatkezelő vagy Munkáltató) folytatott személyes adatok kezelésének jogszerű rendjét, valamint
   b) biztosítsa az adatvédelem alkotmányos elveinek, az információs önrendelkezési jognak és az adatbiztonság követelményeinek érvényesülését,
   c) segítse a mindenkor hatályos, vonatkozó jogszabályoknak [így különösen AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETÉNEK (**GDPR** – a továbbiakban: **Rendelet**) az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvénynek (**Infotv.**)] történő megfelelést,
   d) biztosítsa a Rendelet 5. cikke szerinti elvek (jogszerűség, tisztességes eljárás és átláthatóság, célhoz kötöttség, adattakarékosság, pontosság, korlátozott tárolhatóság, integritás és bizalmas jelleg, elszámoltathatóság) konkrét megvalósulását.
2) A Szabályzat időbeli hatályát a fedlapon és oldalanként a láblécben szereplő dátum jelzi. Az Adatkezelő fenntartja a jogot, hogy a Szabályzatot bármikor módosítsa és új Szabályzatot tegyen közzé honlapján. Új verzió hatályba lépésével a korábbi verzió hatályát veszti.
3) A Szabályzat személyi hatálya kiterjed a Munkáltatónál foglalkoztatott valamennyi munkavállalóra, valamint a munkavégzésre irányuló egyéb jogviszony keretében foglalkoztatottra (a továbbiakban együtt: foglalkoztatott).
4) A Szabályzatban használt fogalmak, meghatározások
   Érintett: azonosított vagy azonosítható természetes személy
   (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);
   Személyes adat: az érintettre vonatkozó bármely információ;
   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;
   Adatkezelő: az a természetes vagy jogi személy, aki vagy amely a személyes adatok kezelésének céljait és eszközeit önállóan, vagy másokkal együtt meghatározza;
   Adatfeldolgozó: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel;
   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;
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;
Hatóság: a Nemzeti Adatvédelmi és Információszabadság Hatóság

5) A jelen szabályzathoz kapcsolódó más szabályzatok:
   a) Az Adatkezelőhöz beérkező és az Adatkezelőnél keletkezett iratok készítésének, kezelésének, nyilvántartásának, irattározásának és selejtezésének alapvetői szabályait, a Munkáltató Iratkezelési Szabályzatával összhangban kell alkalmazni.
   b) Az Adatkezelő elektronikus információs rendszereiben tárolt személyes adatok védelmére irányuló követelményeket az Informatikai Biztonság Szabályzattal összhangban kell alkalmazni.

2. Az Adatkezelőre vonatkozó adatok

Neve:	**EVIN Erzsébetvárosi Ingatlangazdálkodási Nonprofit Zártkörűen Működő Részvénytársaság (EVIN Nonprofit Zrt.)**
Adószáma:	**12194528-2-42**
Cégjegyzékszáma:	**01-10-043258**
Székhelye:	**1071 Budapest, Damjanich u 12.**
postai címe:	**1400 Budapest, 7. posta, Pf. 67.**
weboldala:	**https://evin.hu**
e-mail címe:	**evin@evin.hu**

Az Adatkezelő adatvédelmi tisztviselője:

neve:	**Baksai Zoltán**
postai címe:	**1071 Budapest, Damjanich u 12.**
e-mail címe:	**dpo@evin.hu**

3. A Munkáltató (Adatkezelő) adatvédelmi rendszere

A Munkáltató adatvédelmi rendszere többszintű, minden egyes szinten lévő szereplőnek a szabályok szerinti feladatellátása szükséges a személyes adatok komplex védelméhez és az adatkezelés megfelelőségéhez.

3.1. A vezérigazgató feladatai

1) A személyes adatok védelméért, az adatkezelés jogszerűségéért a vezérigazgató felel. Ennek keretében:
   a) szabályzatok és kötelező utasítások útján meghatározza a személyes adatok védelme és az adatkezelés jogszerűsége szempontjából elvárt, megfelelő technikai és szervezési intézkedéseket és rendelkezik azok folyamatos alkalmazásáról és naprakészen tartásáról;
   b) gondoskodik az adatkezelés személyi és tárgyi feltételeinek biztosításáról, az adatvédelmi és adatbiztonsági intézményrendszer működtetéséről, a működéshez szükséges intézkedések megtételéről;

c) gondoskodik megfelelő adatvédelmi tisztviselőről akár a munkavállalók közül történő kijelöléssel, akár a külső szolgáltató szolgáltatásának beszerzésével;
d) meghozza a Munkáltatóra, mint adatkezelőre vonatkozó adatkezelést érintő döntéseket;
e) felel a Munkáltató adatkezelési tevékenységével kapcsolatos közzétételi kötelezettség teljesítéséért.

2) A vezérigazgató az adatkezelés személyi és tárgyi feltételeinek biztosításáról, a szabályzatban foglaltak végrehajtásáról, az adatvédelemmel kapcsolatos szabályok foglalkoztatottak általi megismeréséről és betartásáról az önálló szervezeti egységek vezetői útján, a Munkáltató Szervezeti és Működési Szabályzatában (a továbbiakban: SZMSZ) meghatározottakkal összhangban gondoskodik.
3) A vezérigazgató az adatkezeléssel kapcsolatos döntések előkészítését, az elszámoltathatóság érdekében szükséges dokumentáció és intézkedések tervezetének összeállítását az adatvédelmi tisztviselő útján végzi.

3.2. Az önálló szervezeti egység vezetőjének feladatai

1) Az önálló szervezeti egység vezetője gondoskodik a szervezeti egysége állományába tartozó, vagy az amellett foglalkoztatott személyek kapcsán:
a) az adatvédelmi követelmények érvényre juttatásáról;
b) a Szabályzatban vagy más kötelező erejű adatvédelmi előírásban foglaltak ellenőrzéséről, azok megsértése esetén a hiányosságok haladéktalan felszámolásáról;
c) a szükséges hozzáférési jogosultságok kiadására és visszavonására irányuló előterjesztésekről;
d) az adatvédelmi tudatosító – ideértve az adatvédelmi incidenskezeléssel, a kapcsolódó információbiztonsággal, valamint az iratkezeléssel összefüggő ismereteket is – képzéseken történő részvételről, szükség esetén ilyen képzés szervezésének kezdeményezéséről.

3.3. A Munkáltatónál foglalkoztatottak feladatai

1) A Munkáltatónál foglalkoztatottak:
a) a Szabályzatban meghatározottak szerint kezelik a feladataik ellátásával összefüggésben tudomásukra jutott személyes adatokat;
b) betartják az adatkezelésre vonatkozó jogszabályokban, más belső szabályzatokban foglalt előírásokat;
c) tudásukat naprakészen tartják a munkavégzésükre irányadó adatvédelmi és adatbiztonsági előírások kapcsán és az adatvédelmi incidensek gyanújának felismerése érdekében.

2) Ha a személyes adatok védelmével kapcsolatos előírások megsértése miatt a Munkáltatónak jogerősen sérelemdíj, kártérítés fizetési kötelezettsége keletkezik, a jogsérelmet okozó foglalkoztatottat, foglalkoztatottakat a Munka Törvénykönyve szerinti kártérítési felelősség terheli.

3.4. A Munkáltató szervezetén kívüli személyekkel kapcsolatos feladatok

1) Amennyiben a Munkáltató feladatának ellátása érdekében adatfeldolgozó igénybevétele szükséges, úgy az általános adatvédelmi rendelet 28. cikke szerinti tartalommal az adatfeldolgozó felelősségét önálló szerződésben vagy a felek között létrejövő szolgáltatási szerződés részeként kell rögzíteni. A szerződés tartalmának összeállítása során ki kell kérni az adatvédelmi tisztviselő véleményét.
2) Amennyiben a Munkáltató feladatának ellátása érdekében közös adatkezelői jogviszony létesítése szükséges, úgy a felek között létrejövő írásbeli megállapodás tartalmazza legalább a GDPR 26. cikke szerinti tartalmi elemeket.
3) szerződés tartalmának összeállítása során ki kell kérni az adatvédelmi tisztviselő véleményét.

3.5. Az adatvédelmi tisztviselő feladatai

1) A Munkáltató adatvédelmi tisztviselője közvetlenül a vezérigazgatónak felel, függetlenül és befolyásolástól mentesen látja el az általános adatvédelmi rendeletben és az e Szabályzatban meghatározott feladatait.
2) Az adatvédelmi tisztviselő a GDPR 39. cikkében foglalt feladatai mellett:
   a) vezeti a Munkáltató, mint adatkezelő adatvédelmi nyilvántartását;
   b) adatvédelmi ellenőrzési tervet készít, amelyet a vezérigazgató hagy jóvá;
   c) az adatvédelmi ellenőrzési terv alapján – szükség szerint azon túl is, különösen érintettől érkező, az Adatkezelő adatkezelését érintő panasz, vagy adatvédelmi incidens bekövetkezte esetén – ellenőrzi az Adatkezelőnél az adatvédelmi és adatbiztonsági követelmények teljesítésülését;
   d) közreműködik az adatvédelmi incidens kezelésében, kivizsgálásában, és a vizsgálat eredménye alapján az adatvédelmi incidenst a GDPR 33. cikke szerint bejelenti a Hatóság részére;
   e) a személyes adatok kezelését igénylő új tevékenység ellátásáért felelős szervezeti egység kérésére előzetesen is véleményezi a tervezett adatkezelést;
   f) megvizsgálja a Munkáltató által tervezett vagy módosuló adatkezelések érintettekre gyakorolt kockázatát, szükség esetén adatvédelmi hatásvizsgálatot kezdeményez és közreműködik annak lefolytatásában;
   g) adatvédelmi szempontból véleményezi az adatfeldolgozóval, közös adatkezelővel vagy más önálló adatkezelővel kötendő megállapodást;
   h) új adatkezeléssel járó tevékenység tervezése vagy valamely adatkezelés körülményeinek változása esetén megvizsgálja, hogy szükséges-e azzal kapcsolatban adatkezelési tájékoztató, új adatvédelmi nyilvántartás bejegyzés, vagy más dokumentáció összeállítása, illetőleg a már létező dokumentum módosítása;
   i) kezdeményezi a Munkáltató munkatársainak adatvédelmi tudatosító képzését, részt vesz az ilyen képzéssel kapcsolatos feladatok ellátásában, kijelölés esetén képzést tart;
   j) elősegíti az érintetteket megillető jogok gyakorlását, valamint véleményezi a Munkáltatóhoz, mint adatkezelőhöz érkező, érintetti joggyakorlásra irányuló beadványokra összeállított válaszok tervezetét;

k) részt vesz az Adatvédelmi Hatóság elnöke által összehívott adatvédelmi tisztviselők éves konferenciáján.

3) Az adatvédelmi tisztviselő jogosult:
   a) tájékoztatást, felvilágosítást kérni minden, e Szabályzat hatálya alá tartozó adatkezelésről;
   b) minden, e Szabályzat hatálya alá tartozó adatkezelést vizsgálni és minden olyan helyiségbe belépni, ahol adatkezelés folyik;
   c) tanácskozási és véleményezési joggal részt venni minden olyan fórumon, ahol a feladatai ellátásával összefüggő kérdések szerepelnek a napirenden;
   d) javaslatot tenni közvetlenül a vezérigazgatónak valamely személyes adatok kezelését érintő kérdésben.
4) Az adatvédelmi tisztviselő az ellenőrzései kapcsán és a vizsgálatával összefüggésben a fentiek mellett:
   a) felszólíthatja az adatkezelésben résztvevő személyt a jogszerű állapot helyreállítására;
   b) kisebb súlyú ügyben közvetlenül az adatkezelésért felelős önálló szervezeti egység vezetőjénél kezdeményezheti az alkalmazott adatkezelési gyakorlat felülvizsgálatát;
   c) kezdeményezheti a vezérigazgatónál a vonatkozó adatvédelmi előírások, valamint a kialakult adatkezelési gyakorlat átalakítását, vagy az adatkezelést érintő más szükséges intézkedések megtételét.
5) A jelen (Az adatvédelmi tisztviselő feladatai) pontban nem szabályozott kérdésekben a 29. CIKK SZERINTI ADATVÉDELMI MUNKACSOPORT 16/HU WP 243 rev.01 számú, „Iránymutatás az adatvédelmi tisztviselőkkel kapcsolatban” című dokumentumában foglaltak szerint kell eljárni.

4. A beépített és alapértelmezett adatvédelem elvének érvényesülése

4.1. Adatkezelés kialakításával összefüggő kötelezettségek

1) A személyes adatok kezelésével járó új tevékenység megkezdése, vagy a folyamatban lévő adatkezelési tevékenységekkel kapcsolatos módosítások hatályba lépése előtt az SZMSZ alapján a feladat ellátásáért felelős szervezeti egység vezetője kezdeményezi az adatvédelmi tisztviselőnél az adatkezelés jogszerű kialakítása, illetve az elszámoltathatóság elvének történő megfelelés érdekében szükséges és arányos intézkedések meghozatalát.
2) Az adatkezeléssel járó feladat ellátásáért felelős szervezeti egység vezetője rögzíti a tervezett adatkezelés legfontosabb jellemzőit, így legalább:
   a) az adatok kezelésére okot adó körülményt vagy jogszabályi rendelkezést;
   b) a feladat ellátásához szükséges adatköröket és azok tervezett forrását;
   c) a tervezett vagy jogszabályban meghatározott megőrzési időt, vagy az annak meghatározásához szükséges szempontokat;
   d) az ahhoz kapcsolódó adattovábbítás címzettjeit;
   e) az adatok biztonsága, valamint az érintettekre nézve azonosított kockázatok csökkentése érdekében tervezett intézkedéseket.
3) A megadott adatok alapján az adatvédelmi tisztviselő véleményezi a tervezetet, majd az alapján – szükség esetén az előterjesztő szervezeti egységgel történő

konzultáció, az értesítés kiegészítése vagy pontosítására történő felhívást követően – javaslatot tesz a vezérigazgatónak:
   a) az ahhoz kapcsolódóan szükségesnek tartott további szervezési és technikai intézkedésekre, vagy a GDPR 5. cikkében foglalt alapelveknek megfelelő adatkezelés kialakításának szempontjaira nézve;
   b) a kapcsolódó adatvédelmi hatásvizsgálat szükségessége kapcsán;
   c) az ahhoz kapcsolódó adatkezelési tájékoztató tartalmára és esetleges közzétételére vonatkozóan.
4) Kizárólag akkor képezheti a Munkáltató, mint adatkezelő adatkezelésének jogalapját a GDPR 6. cikk (1) bekezdés a) pontja szerinti érintetti hozzájárulás, ha az adatkezelés vonatkozásában igazolható módon nincs az érintett és a Munkáltató között egyértelműen egyenlőtlen viszony, továbbá szervezési és technikai intézkedésekkel biztosítható, hogy az érintett hozzájárulását bármikor ugyanolyan könnyen visszavonhassa, ahogy azt megadta.
5) Személyes adatokat továbbítani kizárólag pontosan meghatározott és jogszerű célból, a konkrét esetben közvetlenül hivatkozható jogalap birtokában lehetséges, és a továbbítandó adatok körét az alkalmazandó jogszabályi követelményeket és az iratkezelésre vonatkozó belső előírásokat is mérlegelve az adatkezelés céljához szükséges körre kell szűkíteni.

4.2. Adatbiztonsági követelmények

1) A Munkáltató a kezelésében lévő személyes adatok bizalmasságát, sértetlenségét és rendelkezésre állását biztosítandó, az érintettekre nézve megjelenő kockázatokkal arányos, a technológiai fejlődés szempontjából naprakész, zárt, teljes körű és folytonos szervezési és technikai védelmi intézkedéseket alkalmaz, melyről részletes dokumentációt tartalmaz az Informatikai Biztonság Szabályzat.
2) Az alkalmazott védelmi intézkedések naprakészen tartása érdekében az SZMSZ szerinti feladatkörük kapcsán az önálló szervezeti egységek vezetői, valamint az információbiztonsági felelős, és az adatvédelmi tisztviselő írásban javaslatot tehet azok pontosítására vagy fejlesztésére a vezérigazgatónak.
3) Telefonos ügyfélszolgálati tevékenység ellátása során a Munkáltató rendszereiből személyes adatot továbbítani tilos, tekintettel arra, hogy a hívó fél minden kétséget kizáró módon történő azonosítása a Munkáltatónál nem lehetséges.

4.3. Az adatkezelési műveletek átláthatóságára vonatkozó követelmények

1) Az Adatkezelő adatkezelési tevékenységeire vonatkozóan az adatkezelés érintettje számára világos, könnyen értelmezhető és átlátható módon, az adatkezelés céljai mentén a GDPR 13-14. cikke szerinti tartalommal szükséges az adatkezelési tájékoztatókat összeállítani.
2) Az adatkezelési tájékoztatókban foglaltak tartalmi megfelelőségét, naprakészségét és elérhetőségét az adatvédelmi tisztviselő és az SZMSZ-ben meghatározott feladataihoz kötődően a tevékenység ellátásáért felelős önálló szervezeti egység is köteles figyelemmel kísérni.

3) A kizárólag az Adatkezelő foglalkoztatottjait érintő adatkezelési célok kapcsán összeállított adatkezelési tájékoztatókat a Munkáltató zárt informatikai rendszerében kell a foglalkoztatottak számára elérhetővé tenni.
4) A Munkáltató székhelyén, telephelyein személyesen megjelenő érintetteket, a rájuk vonatkozó adatkezelésekről a belépési ponthoz közel elérhető papíralapú adatkezelési tájékoztató, valamint figyelemfelhívó jelzés útján kell tájékoztatni. Emellett szükség esetén, így különösen látássérültek vagy olvasási, szövegértési képességükben korlátozott érintettek esetében szóbeli tájékoztatás nyújtása is szükséges.
5) Bármely egyéb érintett esetében a Munkáltató a honlapján, az „Adatkezelési tájékoztatók” cím alatt közzétéve bocsátja az érintettek rendelkezésére a szükséges tájékoztatást.

5. Az adatvédelmi incidenskezelés feladatai

1) Amennyiben a Munkáltató bármely munkatársa adatvédelmi incidens bekövetkezésének gyanúját észleli, haladéktalanul tájékoztatja arról a szervezeti egységének vezetőjét. A szervezeti egység vezetője az általa észlelt adatvédelmi incidens kapcsán saját hatáskörben jár el.
2) A szervezeti egység vezetője vagy az általa kijelölt személy haladéktalanul tájékozódik az eset lényeges körülményeiről.
3) Amennyiben a rendelkezésre álló adatok alapján egyértelműen megállapítható, hogy az adatvédelmi incidens a saját szervezeti egység tevékenységével összefüggésben, vagy azt érintően következett be, az azt észlelő személy soron kívül megkezdi az incidens érintettekre nézve megjelenő hatásainak csökkentését és arról haladéktalanul írásban értesíti az adatvédelmi tisztviselőt.
4) Az értesítés az adatvédelmi incidens bekövetkeztének, illetőleg az általa az érintettre nézve jelentett kockázatok és annak hatásainak megállapítása érdekében tartalmazza legalább:
   a) az adatvédelmi incidens jellegét és rövid leírását, ideértve különösen az észlelés és bekövetkezés feltételezett időpontját, az érintett rendszer vagy irat megjelölését;
   b) a valószínűsíthetően érintett személyek körét;
   c) a valószínűsíthetően érintett személyes adatok kategóriáit, nagyságrendjét;
   d) az általa megtett halaszthatatlan intézkedéseket;
   e) megítélése szerint az érintettek jogaira és szabadságaira gyakorolt hatásának súlyosságát;
   f) az általa tervezett további intézkedések leírását.
5) Az adatvédelmi incidenst észlelő szervezeti egység vezetője haladéktalanul értesíti az adatvédelmi tisztviselőt a bekövetkezett eseményről és a nála rendelkezésre álló információról, ha:
   a) az adatvédelmi incidens bekövetkezte vagy annak jellemzői számára nem állapíthatók meg egyértelműen és legfeljebb az észlelését követő 24 órán belül,
   b) az adatvédelmi incidens megítélése szerint elsősorban más önálló szervezeti egység tevékenységét érinti, illetőleg
   c) az adatvédelmi incidens több önálló szervezeti egységet is érinthet.
6) Az adatvédelmi tisztviselő megvizsgálja a kapott értesítésben foglaltakat, és az adatvédelmi incidens lehetséges hatásainak felmérése és megállapítása

érdekében szükség szerint bevonja az információbiztonsági felelőst vagy az adatvédelmi incidenssel érintett szakterület tekintetében szakértelemmel rendelkező személyeket is.

7) Abban az esetben, ha az adatvédelmi incidens feltételezhetően a Munkáltató által üzemeltetett elektronikus információs rendszerek biztonságával összefüggésben következett be, az adatvédelmi tisztviselő az információbiztonsági felelősnek is köteles jelezni a bejelentést. Az információbiztonsági felelős a jelzést követően köteles haladéktalanul véleményt összeállítani az adatvédelmi tisztviselő részére arról, hogy az adatvédelmi incidens valóban érinti-e az informatikai rendszer biztonságát, és ismertetni az ezzel kapcsolatos javasolt, valamint megtett intézkedéseket.
8) Amennyiben az adatvédelmi incidens a Munkáltató által igénybe vett adatfeldolgozó tevékenységével kapcsolatban következett be, az adatvédelmi incidens körülményeinek, és az azzal összefüggő lehetséges kockázatok és hatások kivizsgálásába az adatfeldolgozó képviselőjét is be kell vonni.
9) Az adatvédelmi tisztviselő az incidensvizsgálata keretében mérlegeli az adatvédelmi incidens következtében az érintettekre nézve megjelenő kockázatokat. Ennek során legalább a következőket veszi figyelembe:
   a) az adatvédelmi incidens jellegét;
   b) az érintettek körét, hozzávetőleges számukat;
   c) az incidenssel érintett adatok kategóriáit, az érintett különleges adatokat és a GDPR preambulumának (75) bekezdése szerinti szenzitív adatokat és azok hozzávetőleges számát, illetve nagyságrendjét;
   d) az adatvédelmi incidensből eredő, valószínűsíthető következményeket;
   e) minden, az adatvédelmi incidens megoldására tett vagy tervezett intézkedést, ideértve az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket;
   f) az elektronikus információbiztonságot is érintő incidensek esetén az elektronikus információbiztonsági felelős által azonosított további kockázatot;
   g) az adatvédelmi incidensek kezelése és a kapcsolódó kockázatok mérlegelése tárgyában az Európai Adatvédelmi Testület által elfogadott – vagy a GDPR alkalmazandóvá válását követően fenntartott – iránymutatást;
   h) az adatkezelés kapcsán korábban lefolytatott adatvédelmi hatásvizsgálat dokumentációját.
10) Az adatvédelmi tisztviselő a GDPR 33. cikk (1) bekezdésében meghatározott bejelentési kötelezettség határidőben történő teljesítésének sérelme nélkül, írásban, sürgős esetben szóban tájékoztatja a vezérigazgatót az adatvédelmi incidens kapcsán tett megállapításairól és az érintettre nézve megjelenő valószínűsített kockázatokról, valamint javaslatot állít össze az adatvédelmi incidens kapcsán teendő intézkedésekről.
11) A szóban nyújtott tájékoztatást és a kezelésre vonatkozó javaslatokat az adatvédelmi incidens elhárítását követően kell írásba foglalni.
12) Amennyiben a vezérigazgató a kapott tájékoztatás alapján úgy ítéli meg, hogy az adatvédelmi incidens valószínűsíthetően kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatvédelmi tisztviselő az Adatvédelmi Hatóság honlapjáról letölthető formanyomtatvány alkalmazásával és a GDPR 33. cikk (3) bekezdése szerinti tartalommal bejelenti azt a Hatóság által vezetett nyilvántartásba.
13) Amennyiben a vizsgálatot az adatvédelmi tisztviselő véleménye szerint
   a) nem lehet 72 órán belül teljeskörűen lefolytatni, vagy

b) nem lehet megállapítani egyértelműen a rendelkezésre álló adatok alapján az adatvédelmi incidenssel érintettek körét, az azzal érintett adatkört, vagy az adatvédelmi incidens bekövetkezésének valamennyi más lényeges körülményét,

úgy az adatvédelmi tisztviselő a rendelkezésre álló adatok alapján, szakaszos bejelentésre tesz javaslatot a vezérigazgató részére. A hiányzó adatok megállapítását követően az adatvédelmi tisztviselő intézkedik a teljes bejelentés benyújtása iránt.

14) Amennyiben a vezérigazgató a kapott tájékoztatás alapján úgy ítéli meg, hogy az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, vagy az esemény egyéb körülményei alapján azt szükségesnek látja, a GDPR 34. cikk (3) bekezdésében felsorolt esetek kivételével elrendeli az érintettek tájékoztatását az adatvédelmi incidens kapcsán.

15) Amennyiben az adatvédelmi incidenssel érintett természetes személyek tájékoztatására – különösen az érintettek köre vagy a kapcsolattartási adatok biztonságának sérülése miatt – észszerű módon nincs lehetőség, úgy az adatvédelmi tisztviselő az adatvédelmi incidens főbb jellemzőire vonatkozó értesítés soron kívüli közzétételét kezdeményezi a Munkáltató honlapján.

16) Az adatvédelmi tisztviselő a bekövetkezett adatvédelmi incidensekről a GDPR 33. cikk (5) bekezdése szerint, személyes adatokat nem tartalmazó, a Munkáltató székhelyén elérhető nyilvántartást vezet, amely tartalmazza:
   a) az adatvédelmi incidensről készült feljegyzés iktatószámát;
   b) az adatvédelmi incidenssel érintett irat vagy nyilvántartás, elektronikus információs rendszer megjelölését vagy azonosítóját;
   c) az incidens észlelésének időpontját és a bekövetkezésének megállapított vagy valószínűsített időpontját;
   d) az érintett személyes adatok körét;
   e) az incidens hatásait, következményeit, valamint az orvoslásukra tett intézkedéseket;
   f) a bejelentés időpontját – amennyiben az adatvédelmi incidenst a Hatóság részére a GDPR 33. cikk (1) bekezdése szerint bejelentették, vagy annak rövid indokolását, ami miatt az adatvédelmi incidenst nem jelentették be.

6. Az érintettek jogainak gyakorlásával kapcsolatos eljárás általános szabályai

1) Az Adatkezelő a GDPR 5. cikkében foglalt adatkezelési elvek sérelme nélkül, a GDPR 32. cikke szerinti technikai és szervezési intézkedések végrehajtásával az érintetti joggyakorlásra irányuló minden beadvány kapcsán esetileg és érdemben vizsgálja azt, hogy merülhetnek-e fel kétségek:
   a) a kérelmet benyújtó természetes személy kilétével,
   b) az adatkezelés érintettjének az Adatkezelő általi azonosításával kapcsolatban.

2) Az érintetti joggyakorlásra irányuló beadvány kapcsán a kérelmet benyújtó természetes személy személyazonosságának megállapítása érdekében további intézkedéseket indokolt tenni különösen, ha az:
   a) a kérelmező személyének azonosítását nem biztosító elektronikus levélben, elektronikus aláírás nélkül,
   b) telefax útján, vagy

c) nem a polgári perrendtartásról szóló **2016. évi CXXX. törvény** 325. §-a által meghatározott teljes bizonyító erejű magánokiratba vagy közokiratba foglalt postai küldeményként

került az Adatkezelőhöz.

3) A kérelmet benyújtó természetes személy azonosítása érdekében kizárólag az adott célra szükséges és elégséges többlet személyes adat kérhető. Valamely okiratról készült egyszerű elektronikus másolat, vagy nem hitelesített nem elektronikus másolat megküldése a személy azonosítására nem alkalmas, ezért e célra azok megküldését a kérelmet előterjesztő személytől kétség felmerülése esetén sem lehet kérni.
4) Az Adatkezelő az ellenkező bizonyításáig a kérelmet előterjesztő személy megfelelő azonosításának ismeri el az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló **2015. évi CCXXII. törvény** 18. §-a szerint megvalósuló beadványokat, a teljes bizonyító erejű magánokiratokban foglalt postai úton előterjesztett és az érintett azonosításához szükséges adatokat tartalmazó kérelmeket és az Adatkezelő ügyfélszolgálatán a személyazonosság okirattal történő előzetes igazolását követően személyesen előterjesztett beadványokat.
5) Amennyiben egy érintetti joggyakorlásra irányuló beadvány kapcsán a kérelmet benyújtó természetes személy kilétével kapcsolatban nem merül fel kétség, azonban az Adatkezelő által kezelt adatok körében megállapítást nyer, hogy az érintett nem azonosítható, – így különösen mert az Adatkezelő adatkezelésének célja nem teszi szükségessé az érintettnek az Adatkezelő általi azonosítását és bizonyítani tudja, nincs abban a helyzetben, hogy azonosítsa az érintettet – erről haladéktalanul írásban tájékoztatja a kérelmet benyújtó személyt.
6) Abban az esetben, ha a kérelmet előterjesztő személy megfelelő azonosítására nem alkalmas beadvány érkezik az Adatkezelőhöz, és az abban foglalt – a GDPR 15. cikke szerinti hozzáférési joggyakorlásra, vagy az adatok másolatának kiadására irányuló – kérés olyan adatokra vonatkozik, amelyek megőrzési ideje az Adatkezelőnél a kérelemtől számítva rövidebb, mint 1 hónap, akkor a kérelmet előterjesztő személy megfelelő azonosítására nem alkalmas kérelemmel érintett adatok kezelését az azonosítást lehetővé tevő kérelem beérkezéséig, de legfeljebb 1 hónapig korlátozza.
7) Abban az esetben, ha a kérelmet előterjesztő személy megfelelő azonosítására nem alkalmas beadvány érkezik az Adatkezelőhöz, és abban valamely érintett kapcsolattartási adataira vonatkozó helyesbítéshez való jog gyakorlására irányuló kérelem van, az Adatkezelő hivatalból is köteles vizsgálni, hogy az általa kezelt kapcsolattartási adatok naprakészek-e. A pontosság elvének történő megfelelés érdekében különösen az Adatkezelő által kezelt adatok összevetése lehet indokolt a személyiadat- és lakcímnyilvántartásban nyilvántartott és a Rendelkezési Nyilvántartásban szereplő adatokkal.
8) Az érintetti jogok gyakorlására irányuló kérelem elintézésébe az adatvédelmi tisztviselőt be kell vonni. Az Adatkezelőhöz bármely módon - akár nem hivatalos elérhetőségein keresztül, vagy nem megfelelő módon, esetleg formában - előterjesztett, érintetti joggyakorlásra irányuló kérelmet köteles az azt fogadó önálló szervezeti egység vezetője soron kívül az adatvédelmi tisztviselő részére is továbbítani.
9) Az érintetti joggyakorlásra utaló beadványok kapcsán – az adatvédelmi tisztviselő bevonásával – mindenekelőtt meg kell állapítani, hogy abban az

általános adatvédelmi rendelet szerinti valamely érintetti jogot, különösen a GDPR 15. cikke szerinti hozzáférési jogot, vagy esetleg közérdekű adatigénylést kíván-e előterjeszteni.

10) Az érintetti joggyakorlások teljesítése során a kérelem tárgyában érintett önálló szervezeti egységek közreműködésével vizsgálni szükséges az Adatkezelő elektronikus iratkezelő rendszerét, és az Adatkezelő által üzemeltetett elektronikus információs rendszereit is.
11) Az Adatkezelő a hozzáférési jog biztosítása során a harmadik fél jogainak védelmét szem előtt tartva jár el az adatokról készített másolat és az azokba történő betekintés biztosítása során is.
12) Az Adatkezelő indokolatlan késedelem nélkül és a lehető legrövidebb időn belül, de legkésőbb az azonosítható érintettől származó kérelem beérkezésétől számított egy hónapon belül (a továbbiakban: alaphatáridő) tájékoztatja az érintettet a jogai gyakorlására irányuló kérelme nyomán hozott intézkedésekről.
13) Amennyiben annak a GDPR 12. cikkében foglalt feltételei fennállnak, a válaszadás határideje a vezérigazgató döntése szerint további két hónappal meghosszabbítható, azonban ennek megítélése kapcsán részére az alaphatáridőn belül, írásban kell igazolni a késedelem okait, és előterjeszteni a hosszabbítás kapcsán az érintettnek nyújtandó tájékoztatás tervezetét.
14) Az Adatkezelő az érintett részére a kérelmével kapcsolatos tájékoztatást az általa a Rendelkezési Nyilvántartásban történt rendelkezéseit figyelembe véve nyújtja. Ilyen rendelkezés hiányában az érintett kérelmében foglaltaknak megfelelő módon, kivételes esetben és arról jegyzőkönyv egyidejű felvétele mellett személyesen is megadhatja.
15) Az elektronikus úton biztonságosan nem továbbítható személyes adatokat az Adatkezelő postai úton, tértivevényes küldeményben, elektronikus adathordozón küldi meg az érintett részére, vagy külön kérésére jegyzőkönyv egyidejű felvétele mellett azt személyesen adja át.

7. Változásmutató

A jelen dokumentum a 2.0. verzió, a korábbi 1.0. verziótól alapvetően eltérő szerkezetű. Ezért tételes változás-összehasonlítás az esetleges későbbi 2.1. verzióban történik a 2.0. verzióhoz képest.