A

VÁROSLIGET INGATLANFEJLESZTŐ ZÁRTKÖRŰEN MŰKÖDŐ RÉSZVÉNYTÁRSASÁG

ADATKEZELÉSI ÉS ADATVÉDELMI SZABÁLYZATA

Tartalomjegyzék

I. A SZABÁLYZAT CÉLJA

A **Városliget Ingatlanfejlesztő Zártkörűen Működő Részvénytársaság** (székhely: 1146 Budapest, Dózsa György út 41., cégjegyzékszám: 01-10-047989, képviseli: dr. Gyorgyevics Benedek Tamás, vezérigazgató, mint a munkáltatói jogkör gyakorlója; a továbbiakban: **Városliget Zrt., vagy Adatkezelő**) a tevékenységét érintő személyes adatok kezelésével és védelmével összefüggésben jelen szabályzatot alkotja:

Jelen Szabályzat célja, hogy rögzítésre kerüljön a Városliget Zrt. adatvédelmi és adatkezelési eljárásrendje, és egyúttal tájékoztassa munkavállalóit, ügyfeleit/szerződő partnereit (ezek kapcsolattartóit), és vendégeit (a továbbiakban együttesen: Érintett vagy Érintettek) az általa kezelt személyes adatokról, a személyes adatok kezelése körében követett elveiről és gyakorlatáról, valamint az Érintettek jogai gyakorlásának módjáról és lehetőségeiről. Jelen Szabályzat a Városliget Zrt. adatkezelésének általános szabályait tartalmazza. Az egyes adatkezeléseket érintő külön rendelkezések a külön adatkezelési tájékoztatókban találhatóak.

A Városliget Zrt. elkötelezett az Érintettek személyes adatainak védelme iránt, kiemelten fontosnak tartja az Érintettek információs önrendelkezési jogának tiszteletben tartását és kijelenti, hogy tiszteletben tartja az Érintettek személyhez fűződő jogait.

A rögzített személyes adatokat bizalmasan, az Európai Parlament és a (EU) 2016/679. (2016. április 27.) 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 rendeletével (GDPR), a nemzetközi ajánlásokkal, valamint az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény rendelkezéseivel összhangban, a jelen Szabályzatban foglaltaknak megfelelően kezeli, és megtesz minden olyan biztonsági, technikai és szervezési intézkedést, mely az adatok biztonságát garantálja.

Az adatokat védi különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, az adatok károsodása és véletlen elvesztése, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen.

A Városliget Zrt. adatkezelési tevékenységével kapcsolatosan felmerülő információk, a Szabályzat mindenkor érvényes verziója folyamatosan elérhető a Városliget Zrt. honlapján: https://www.ligetbudapest.hu.

A Városliget Zrt. fenntartja a jogát arra, hogy a jelen Szabályzatot bármikor megváltoztassa. Az esetleges változásokról kellő időben és megfelelő módon értesíti az Érintetteket.

A Szabályzat elkészítéséért, aktualizálásáért a Városliget Zrt. adatvédelmi tisztviselője – a Városliget Zrt. jogi tanácsadói partnerének bevonásával - felelős.

II. ÁLTALÁNOS RENDELKEZÉSEK

II.1. Fogalmak

Adatbiztonság: Városliget Zrt., mint Adatkezelő megfelelő intézkedésekkel védi az adatok, különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, sérülés ellen és gondoskodik az adatok biztonságáról, melynek keretében megteszi azokat a technikai, műszaki és szervezési intézkedéseket, melyek szükségesek az adatvédelmi szabályok érvényre juttatásához.

Adatfeldolgozás: az adatkezelő megbízásából vagy rendelkezése alapján az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése (függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől).

Adatfeldolgozó: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel.

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, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza; ha az adatkezelés céljait és eszközeit az uniós vagy a tagállami jog határozza meg, az adatkezelőt vagy az adatkezelő kijelölésére vonatkozó különös szempontokat az uniós vagy a tagállami jog is meghatározhatja.

Adatmegsemmisítés: az adatokat tartalmazó adathordozó teljes fizikai megsemmisítése;

Adattovábbítás: az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele;

Adattörlés: az adatok felismerhetetlenné tétele oly módon, hogy a helyreállításuk többé nem lehetséges;

Érintett(ek): azon természetes személyek, akik személyes adatát a Városliget Zrt., mint Adatkezelő kezeli.

Harmadik személy: olyan természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki, vagy amely nem azonos az Érintettel, az adatkezelővel vagy az adatfeldolgozóval;

Hozzájárulás: az érintett akaratának önkéntes és határozott kinyilvánítása, amely megfelelő tájékoztatáson alapul, és amellyel félreérthetetlen beleegyezését adja a rá vonatkozó személyes, vagy

különleges adatok – teljes körű vagy egyes műveletekre kiterjedő – kezeléséhez. Különleges adatok esetében feltétlenül szükséges az írásos forma.

Különleges adat: a személyes adatok különleges kategóriáiba tartozó minden adat, azaz a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a genetikai adatok, a természetes személyek egyedi azonosítását célzó biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok.

Nyilvánosságra hozatal: az adat bárki számára történő hozzáférhetővé tétele;

Személyes adat: a Városliget Zrt. adatkezelési tevékenysége során azonosított vagy azonosítható természetes személyre („érintett") vonatkozó bármely információ; 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;

II.2. A szabályzat alkalmazási köre

A szabályzat személyi hatálya kiterjed a Városliget Zrt. valamennyi munkavállalójára. A Szabályzat rendelkezéseit alkalmazni kell ezen túl a Városliget Zrt-vel polgári jogi szerződéses jogviszonyban álló magánszemélyekre, jogi személyekre és jogi személyiséggel nem rendelkező egyéb szervezetekre és alkalmazottaikra (a továbbiakban: külső munkavállalók) (együttesen: Foglalkoztatottak, Adatkezelésben érintett munkatársak) is, továbbá biztosítani kell, hogy a külső munkavállalók a szabályzatot a szükséges mértékben megismerjék, a velük kötött polgári jogi szerződéseknek erre vonatkozóan utalást kell tartalmaznia. A Szabályzat ezen túlmenően kiterjed a Városliget Zrt. tulajdonában álló vagy általa hasznosított, üzemeltetett épület és terület valamennyi látogatójára is.

A szabályzat tárgyi hatálya kiterjed a Városliget Zrt. minden adatkezelésére és adatfeldolgozására, amely:

a) természetes személy személyes adataira vagy

b) közérdekű adatokra vonatkozik, beleértve az adatkezelés minden elemét, függetlenül attól, hogy az elektronikusan vagy papíralapon történik.

II.3. Az adatkezelés alapelvei

A jogszerű és tisztességes adatkezelés elve alapján:

a) A Városliget Zrt. adatkezelésben érintett munkatársai személyes adatot kizárólag az érintett hozzájárulásával vagy jogszabályi felhatalmazás alapján, a jogszabályban rögzített előírásoknak megfelelően, az érintett számára átlátható módon kezelhet. A jogszabályi felhatalmazással esnek egy

tekintet alá a Magyarország területén közvetlenül hatályosuló, a hazai jogrendbe átültetést nem igénylő kötelező uniós aktusok is.

b) Külső munkavállalók a velük kötött polgári jogi szerződés által meghatározott módon kezelhetnek és dolgozhatnak fel személyes adatot.

A célhoz kötöttség elve alapján:

a) a foglalkoztatottak kizárólag meghatározott feladataik ellátása céljából, a részükre biztosított jogosultságok rendeltetésszerű használatával kezelhetnek személyes adatot;

b) a konkrét, jogszabályban rögzített vagy az érintett által adott hozzájárulásban megfogalmazott célhoz nem köthető adatkezelés tilos;

c) a kezelt személyes adatok magáncélra történő felhasználása tilos;

d) amennyiben az adatkezelés célja teljesült vagy megszűnt, az adatkezelésre irányadó jogszabályban vagy a levéltári törvényben szereplő tárolási határidőt követően az adatot elektronikusan törölni, a papíralapú adathordozót pedig selejtezni kell.

A pontosság elve alapján: amennyiben az Adatkezelő foglalkoztatottja tudomást szerez arról, hogy az általa kezelt személyes adat hibás, hiányos, vagy időszerűtlen, köteles azt helyesbíteni, aktualizálni vagy az adat helyesbítését, aktualizálását az adat rögzítéséért felelős foglalkoztatottnál kezdeményezni, és erről mindazokat értesíteni, akiknek az adat továbbításra került. Amennyiben az Adatkezelő az érintett hozzájárulásával kezeli személyes adatot, az adataiban bekövetkezett változást a foglalkoztatott haladéktalanul köteles közölni az érintettel.

Az adatbiztonság elve alapján: az adat kezelése során a tudomány és a technológia állását, illetve a megvalósítás költségeit is figyelembe véve megfelelő technikai és adminisztratív intézkedésekkel biztosítani kell, hogy:

a) a személyes adat illetéktelen harmadik személy tudomására ne jusson (bizalmasság),

b) az adat illetéktelen harmadik személy által ne legyen módosítható (sértetlenség),

c) az adat elérhető legyen a feljogosított személyek, szervezetek számára (rendelkezésre állás).

Az adatbiztonságot növelő megoldás az „álnevesítés", amikor az adott nyilvántartásból további információk felhasználása nélkül nem állapítható meg, hogy az adatkezelés mely konkrét természetes személyre vonatkozik.

Az adattakarékosság elve alapján: az adatok körét a célhoz szükséges minimumra kell csökkenteni, az Adatkezelő kizárólag annyi és olyan személyes adatot kezelhet, amely az érintett egyértelmű azonosításához és ügyének elintézéséhez minimálisan szükséges, arra alkalmas.

Az elszámoltathatóság elve alapján: az Adatkezelőnek bármikor képesnek kell lenni annak

bizonyítására, hogy adatkezelése valamennyi adatkezelési művelet tekintetében jogszerű, és mindenben megfelel az adatkezelés elveinek.

Az Adatkezelő köteles az alapelveknek történő megfelelést igazolni, így különösen az érintett jogainak biztosítása és hozzájárulásának megszerzése kapcsán, a végrehajtott ellenőrzésekre és oktatásokra, az előírt nyilvántartások vezetésére, továbbá az adatvédelmi hatásvizsgálatokhoz kapcsolódó feladatokra vonatkozóan.

III. RÉSZLETES RENDELKEZÉSEK

A Városliget Zrt. minden adatkezelésben érintett munkatársa felelősséggel tartozik a feladatai teljesítése során végzett adatkezelés jogszerűségéért, jelen Szabályzatban foglaltak betartásáért.

A foglalkoztatott felelősséggel tartozik különösen, ha

a) a feladatai teljesítése során jogszerűen megismert személyes adatot illetéktelen harmadik személy számára átadja, vagy hozzáférhetővé teszi,

b) jogosultságait nem rendeltetésszerűen használja (pl. jogosulatlan lekérdezést hajt végre), adatokat jogosulatlanul más alkalmazott vagy illetéktelen harmadik személy részére hozzáférhetővé tesz.

Az adatkezelési cél megszűnését követően az adatok törlésére az adatot ténylegesen kezelő foglalkoztatott gondoskodni köteles.

III.1. Az adatvédelmi szervezet

1. A **Vezérigazgató** felelős a Városliget Zrt. adatkezelésének jogszerűségéért; gondoskodik az adatkezelés személyi és tárgyi feltételeinek biztosításáról, ennek keretében:

a) az adatvédelemre és adatkezelésre vonatkozó szabályzatot ad ki,

a) határozatlan időre adatvédelmi tisztviselőt nevez ki;

b) jogosult a Városliget Zrt. adatkezeléseire vonatkozó döntések meghozatalára;

c) kivizsgáltatja az ellenőrzések során feltárt hiányosságokat, gondoskodik a jogsértő körülmények megszüntetéséről;

2. **Az adatvédelmi tisztviselő**

Az adatvédelmi tisztviselőt a személyes adatok védelme területén szerzett ismeretei és gyakorlati tapasztalatai, valamint a számára jogszabályban vagy normában meghatározott feladatok ellátására való alkalmasság alapján jelöli ki.

Az Adatvédelmi tisztviselő: **Zsigó Mariann** (elérhetőségei: **adatvedelem@ligetbudapest.hu**). Bármely érintett az adatvédelmi tisztviselőhöz fordulhat az illetékességébe tartozó kérdésben.
A kijelölés a NAIH megfelelő nyilvántartásába bejelentésre kerül.

Az adatkezelő szerv vezetője köteles bevonni az adatvédelmi tisztviselőt a személyes adatok védelmét érintő döntések, így különösen az adatvédelmet érintő normák, szerződések, együttműködési megállapodások és adatkezelésekre vonatkozó döntések előkészítésébe és kidolgozásába.

Az adatkezelő szerv vezetője biztosítja az adatvédelmi tisztviselő számára a hozzáférést a feladatai végrehajtásához szükséges elektronikus rendszerekhez, iratokhoz, egyéb adathordozókhoz, valamint a szakmai ismeretei naprakészen tartásához szükséges feltételeket, jogosultságokat és erőforrásokat rendelkezésére bocsátja.

Az adatvédelmi tisztviselő tevékenységi körét tekintve a Vezérigazgató közvetlen irányítása alatt működik, munkája során függetlenül jár el, csak a Vezérigazgatónak tartozik beszámolási kötelezettséggel,

3. Az adatgazdák

A szervezeti egységek vezetői, akik felelősek az irányításuk alá tartozó szervezeti egységek adatkezelésének jogszerűségéért, jelen Szabályzatban foglaltak végrehajtásáért és betartásáért.

Jogosulatlan hozzáférés vagy az adatvédelmi előírások egyéb megsértésének észlelése esetén az adatvédelmi tisztviselő egyidejű tájékoztatása mellett intézkedést tesznek annak megszüntetésére.

Adatvédelmi incidens bekövetkezése esetén részt vesznek az adatvédelmi tisztviselő által összehívott munkacsoport munkájában.

4. Az adatkezelést végző munkatárs

a) köteles az általa végzett adatfeldolgozást jogszerűen végezni;

b) köteles a tudomására jutott személyes adatokat kizárólag jelen Szabályzat rendelkezései szerint feldolgozni, tárolni és megőrizni;

c) haladéktalanul, de legkésőbb egy munkanapon belül köteles jelenteni a szervezeti egysége vezetőjének és az adatvédelmi tisztviselőnek, ha adatvédelmet vagy adatbiztonságot veszélyeztető eseményt, adatvédelmi rendelkezések sérelmét vagy annak következményeit észlelik.

Az adatkezelést végző munkatársak az általuk használt, vagy birtokukban lévő, személyes adatokat is tartalmazó adathordozókat kötelesek biztonságosan őrizni, és védeni a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés ellen.

Az adatkezelést végző munkatárs saját célra adatfeldolgozást nem végezhet.
Az adatkezelésben érintett munkatársakat az adatkezelés megkezdése előtt adatvédelmi képzésben, az

adatvédelemre vonatkozó jogszabályi környezet megváltozásakor, továbbá ha az Adatkezelő adatkezelését vagy adatbiztonságát, illetve a szabályzat tartalmát érintő jelentős változás következik be, adatvédelmi továbbképzésben, a külső munkavállalókat adatvédelmi tájékoztatásban kell részesíteni (a továbbiakban együtt: oktatás).

III.2. Az adatkezelés szabályai

A papír alapon kezelt személyes adatokat keletkezésükkor megfelelő minőségű adathordozóra kell rögzíteni, az adatok olvashatóságáért az azokat felvevő, illetve rögzítő személy felel. A személyes adatok jogosulatlan megismerésének megakadályozása érdekében az adathordozókat folyamatos felügyelet alatt kell tartani vagy el kell zárni.

Az adatkezelés jogalapját, célját, a kezelt adatok minimálisan szükséges kategóriáit, az adatokhoz hozzáférők körét és a törlési határidőket az adatkezelés megkezdése előtt, konkrétan meg kell határozni. Személyes adat ezen feltételek hiányában nem kezelhető. Az adatok őrzési, törlési határidejét a célhoz kötöttség elve és az adat kezelését meghatározó jogszabályok előírásai alapján kell megállapítani.

III.3. Adatvédelmi hatásvizsgálat és előzetes konzultáció

Ha az Adatkezelés valamely – különösen új technológiákat alkalmazó – típusa, figyelemmel annak jellegére, hatókörére, körülményére és céljaira, valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, akkor az Adatkezelő az Adatkezelést megelőzően hatásvizsgálatot végez arra vonatkozóan, hogy a tervezett adatkezelési műveletek a személyes adatok védelmét hogyan érintik.

III.4. Adatbiztonság

A Városliget Zrt. a foglalkoztatottaktól megköveteli, hogy a napi munkavégzés befejezésével a foglalkoztatott úgy hagyhatja el munkaállomását, hogy az általa kezelt adathordozókat elzárja.

1. **Informatikai nyilvántartások védelme:** A helyi számítógépeken (asztali számítógép, laptop, tablet, okostelefon) és az informatikai hálózatokon tárolt személyes adatok biztonsága az alábbi intézkedéseket kell alkalmazni:
    a) helyi számítógépre adatmentés nem végezhető, a személyes adatokat tartalmazó dokumentumokat, nyilvántartásokat stb. központi szerverekre kell menteni.
    b) a hálózati kiszolgáló gépen (a továbbiakban: szerver) tárolt adatokhoz csak a megfelelő jogosultsággal rendelkező és arra kijelölt személyek férhetnek hozzá;

c) Amennyiben a személyes adatok adathordozója nem papír, hanem más fizikai eszköz, úgy a fizikai eszköz megsemmisítésére a papírok megsemmisítési szabályai irányadóak.

d) a számítógépen található adatokhoz csak érvényes, személyre szóló, azonosítható jogosultsággal - legalább felhasználói névvel és jelszóval - lehet csak hozzáférni, a jelszavak cseréjéről rendszeresen, illetve indokolt esetben soron kívül gondoskodni kell;

e) amennyiben az adatkezelés célja megvalósult, az adatkezelés határideje letelt, úgy az adatot visszaállíthatatlanul törölni kell;

f) a hálózaton tárolt adatok biztonsága és az adatvesztés elkerülése érdekében a szerveren folyamatos adatmentést kell végezni;

g) a személyes adatokat tartalmazó adatbázisok aktív adatairól a központi szerver teljes adatállományára vonatkozóan naponta adatmentést kell végezni;

h) a személyes adatokat kezelő hálózaton a vírusvédelemről folyamatosan gondoskodni kell;

i) illetéktelen személyek hálózati hozzáférését a rendelkezésre álló számítástechnikai eszközök alkalmazásával meg kell akadályozni.

Az adatbiztonságra vonatkozó részletes szabályokat a Városliget Zrt. Informatikai Biztonsági Szabályzata tartalmazza.

2. **Papíralapú nyilvántartások védelme:** A papíralapon kezelt személyes adatok biztonsága érdekében a Városliget Zrt. az alábbi intézkedéseket alkalmazza:

a) az adatokat csak az arra jogosultak ismerhetik meg, azokhoz más nem férhet hozzá, más számára nem tárhatók fel;

b) biztosítja, hogy a folyamatos, aktív kezelésben lévő iratokhoz csak az illetékesek férhetnek hozzá;

c) amennyiben a papíralapon tárolt személyes adat kezelésének célja megvalósult, intézkedik a selejtezéséről, valamint a megsemmisítéséről. A selejtezésről jegyzőkönyv készül.

III.5. Jogosultságkezelés

Az informatikai rendszerben a jogosultságok változásait (létező jogosultságok, új jogosultságok kiosztása, módosítása, megszűnése) dokumentálni kell. A jogosultság kezelés célja, hogy a kiosztott jogosultságok naprakészen, pontosan nyomon követhetőek legyenek, dokumentált formában megőrzésre kerüljenek, valamint az egyes jogosultságokkal rendelkező személyek tevékenysége és az általuk felhasznált adatok köre ellenőrizhető legyen.

A személyes adatok biztonsága érdekében új jogosultság beállítását, illetve jogosultság megváltoztatását az adatgazda felhatalmazása alapján rendszergazda végzi.

III.6. Adatfeldolgozó igénybevételének szabályai

A Városliget Zrt., mint Adatkezelő nevében más jogi személy vagy szervezet is végezhet adatkezelési tevékenységét azzal, hogy az Adatkezelő határozza meg az adatkezelés céljait és eszközeit.

Az Adatkezelővel az adatfeldolgozó minden esetben írásbeli szerződést köt, amelyben rögzíti legalább az alábbi pontokat:

a) az adatfeldolgozó az átvett adatokat, – jogszabályon alapuló adatkezelés kivételével – kizárólag az adatkezelő szerv írásbeli utasításai alapján, annak keretei között kezeli;

b) az adatfeldolgozó köteles megakadályozni az adatokhoz történő jogosulatlan, illetve jogosultságot meghaladó mértékű hozzáférést, amelynek érdekében kötelezettséget vállal arra, hogy az adattovábbítással érintett adatok kezelésére feljogosított személyek – jogszabályon alapuló megfelelő titoktartási kötelezettség hiányában – titoktartási kötelezettséget vállalnak;

c) az adatfeldolgozó gondoskodik a jogszabály által meghatározott adatbiztonsági követelményeknek való maradéktalan megfelelőségről, annak legfontosabb jellemzőiről tájékoztatja a rendőrségi adatkezelő szervet az adatkezelésre vonatkozó tájékoztató elkészítése és az adatvédelmi hatásvizsgálat teljes körű lefolytathatósága érdekében;

d) az adatfeldolgozó vállalja, hogy az Adatkezelő előzetes írásbeli hozzájárulása nélkül nem vesz igénybe további adatfeldolgozót, a további adatfeldolgozó igénybevétele esetén pedig az betartja a rendőrségi adatkezelő szerv, valamint az adatfeldolgozó között létrejött adatfeldolgozói szerződésben foglaltakat;

e) az adatfeldolgozó az adatkezelés jellegének figyelembevételével megfelelő technikai és szervezési intézkedésekkel a lehetséges mértékben segíti az adatkezelőt abban, hogy teljesíteni tudja kötelezettségét az érintett jogainak gyakorlásához kapcsolódó kérelmek megválaszolása tekintetében;

f) az adatfeldolgozó köteles segítséget nyújtani a rendőrségi adatkezelő szerv részére az érintett tájékoztatásra vonatkozó kötelezettségének teljesítése során, figyelembe véve az adatkezelés jellegét és az adatfeldolgozó rendelkezésére álló információkat;

g) az adatfeldolgozó köteles az adatfeldolgozói szerződés teljesítését követően – az Adatkezelő szerv döntése alapján – valamennyi, a részére átadott személyes adatot törölni, megsemmisíteni vagy azokat visszajuttatni a rendőrségi adatkezelő szerv részére, beleértve az arról készített másolatokat is, kivéve, ha jogszabály a személyes adatok további tárolását írja elő, vagy azok az alkalmazott technikai megoldások jellemzőiből eredően nem törölhetők;

h) az adatfeldolgozó köteles az Adatkezelő szerv rendelkezésére bocsátani minden olyan információt, amely az adatfeldolgozói tevékenységből származó kötelezettségek

teljesítésének igazolásához szükséges, továbbá amely lehetővé teszi és elősegíti a rendőrségi adatkezelő szerv vagy az általa megbízott más ellenőr által végzett auditokat, beleértve a helyszíni vizsgálatokat is.

Az adat megismerésére vagy továbbítására vonatkozó kérelem esetén az érdemi döntést az adatkezelő szerv vezetője vagy az általa kijelölt személy köteles, illetve jogosult meghozni, erre az adatfeldolgozó figyelmét az adatfeldolgozói szerződésben is fel kell hívni.

A Városliget Zrt. által igénybe vett adatfeldolgozókról és az adatfeldolgozás során átadott személyes adatokról az adatvédelmi tisztviselő nyilvántartást vezet.

III.7. Közérdekű adat nyilvánossága

A közérdekű adat megismerése iránt bárki szóban, írásban, vagy elektronikus úton terjeszthet elő kérelmet.

A közérdekű adat megismerése iránti igénynek az adatkezelő szerv az igény beérkezését követő legrövidebb idő alatt, legfeljebb azonban 15 napon belül köteles eleget tenni.

Ha a közérdekű adatot kezelő szerv az igény teljesítését megtagadja, arról – annak indokaival együtt - az igény beérkezését követő 15 napon belül írásban vagy - amennyiben elektronikus levelezési címét közölte - elektronikus úton értesíti az igénylőt.

Amennyiben az igényelt adat kezelője nem a megkeresett szerv, úgy azt haladéktalanul köteles továbbítani a közérdekű adatot kezelő szervnek. Az igény áttételéről egyidejűleg tájékoztatni kell az igénylőt.

Amennyiben az igénylés jelentős terjedelmű, illetve nagyszámú adatra vonatkozik, vagy az adatigénylés teljesítése a közfeladatot ellátó szerv alaptevékenységének ellátásához szükséges munkaerőforrás aránytalan mértékű igénybevételével jár, az adatkezelő szerv vezetője a határidőt egy alkalommal 15 nappal meghosszabbíthatja, melyről az igénylőt az igény beérkezését követő 15 napon belül írásban vagy - amennyiben elektronikus levelezési címét közölte - elektronikus úton tájékoztatni kell.

Az adatigénylésnek közérthető formában és - amennyiben az aránytalan költséggel nem jár - az igénylő által kívánt technikai eszközzel, illetve módon kell eleget tenni.

Ha az igénylő az adatokat tartalmazó dokumentumról, vagy dokumentumrészről másolatot kíván kérni, a másolat készítésével felmerült anyagi és személyi költségek (így különösen az igényelt adatokat tartalmazó adathordozó és annak kézbesítési költsége, illetve a munkaerő-ráfordítás költsége) az igénylővel szemben érvényesíthetők. A költség várható összegét az igénylővel előre közölni kell.

Az igény teljesítése során kiemelt figyelmet kell fordítani arra, hogy a közérdekű adatok közlése ne járjon mások jogainak, vagy törvény által nyilvánosságában korlátozott adatok bizalmasságának sérelmével. Különös figyelmet kell fordítani arra, hogy az adatszolgáltatással ne kerüljenek

nyilvánosságra személyes adatok, minősített adatok, törvény által nyilvánosságában korlátozott adatok.

Ha a közérdekű adatot tartalmazó dokumentum az igénylő által meg nem ismerhető adatot is tartalmaz, a másolaton a meg nem ismerhető adatot felismerhetetlenné kell tenni, olyan módon, hogy a törvény által nyilvánosságában korlátozott adatok tartalmára megalapozott következtetést ne lehessen levonni.

Az adatigénylő személyazonosító adatai csak annyiban kezelhetők, amennyiben az az igény teljesítéséhez - beleértve az esetleges költségek megfizetését is - elengedhetetlenül szükséges. Az igény teljesítését, illetőleg a költségek megfizetését követően az igénylő személyes adatait - törvény eltérő rendelkezése hiányában - haladéktalanul törölni kell. Ezzel összefüggésben a keletkezett iratok kezelésére az iratok kezelésére vonatkozó irányító eszközben meghatározott megőrzési idők irányadók, azonban az igény teljesítéséhez, illetve a költségek megfizetéséhez szükséges időtartam lejártát követően az igénylő személyes adatait felismerhetetlenné kell tenni.

III.8. Jogszabályon alapuló adatszolgáltatási kötelezettség teljesítése

A Városliget Zrt. adatot jogszabályban meghatározott szerv, vagy személy részére és adatkörben a célhoz kötöttség elvének maradéktalan érvényesítésével szolgáltathat.
Jogszabályban meghatározott adatszolgáltatási kötelezettség esetén a Városliget Zrt. adatkezelést végző munkatársa minden esetben ellenőrzi az adatkezelés jogalapjának meglétét.
A fentieken túl adatot továbbítani csak akkor lehet, ha ahhoz az érintett egyértelműen és dokumentálhatóan hozzájárult. Az érintettek hozzájárulásához kötött adattovábbítás esetén az érintett a nyilatkozatát az adattovábbítás címzettje és célja ismeretében adja meg.

III.9. Ellenőrzés

Az adatvédelemmel kapcsolatos jogszabályi előírások és belső szabályozási dokumentumok betartását az adatkezelést végző szervezeti egységek vezetői (adatgazdák) jogosultak és kötelesek folyamatosan ellenőrizni jelen szabályozás alapján.
A Városliget Zrt. adatvédelmi tisztviselője jogosult általános és célellenőrzéseket végezni. Az ellenőrzés megkezdéséről a belső ellenőrzési vezetőt - az ellenőrzés megkezdéséig, vagy azzal egyidejűleg - tájékoztatni köteles.

Az ellenőrzésnek különösen az alábbiakra kell kiterjednie:

- az adattovábbítási nyilvántartás vezetése,
- az adathordozók meglétének szúrópróbaszerű ellenőrzése,
- selejtezés, megsemmisítés végrehajtása, dokumentálása,
- jelen Szabályzat rendelkezéseinek betartása.

Az ellenőrzésre feljogosított az ellenőrzés céljára figyelemmel az ellenőrzés érdekében az adatkezelést végzőktől minden olyan kérdésben felvilágosítást kérhet, minden olyan adatkezelést megismerhet, vagy abba betekinthet, amely az ellenőrzött szerv adatkezelési tevékenységével összefügg.

Az adatvédelmi tisztviselő jogosult az irat és adatkezeléssel kapcsolatos belső szabályozási dokumentumok, jegyzőkönyvek és nyilvántartások áttekintésével ellenőrizni az adatkezelés törvényes rendjének megtartását. Törvénysértés esetén annak megszüntetésére szólítja fel az adatkezelő személyt vagy szervezeti egység vezetőjét, különösen súlyos jogszabálysértés esetén pedig a Vezérigazgatóhoz fordul.

Az adatvédelmi tisztviselő jogosult a személy és munkaügyi nyilvántartások rendszerét ellenőrizni.

III.10. A Hatóság vizsgálatában való közreműködés

A Városliget Zrt. az adatvédelmi tisztviselője útján együttműködik a Hatósággal, a Hatóság kérésének a megállapított határidőn belül eleget tesz, illetve amennyiben a Hatóság által tett megállapításokkal, illetve a Hatóság által meghatározott határozatokkal nem ért egyet, megteszi a szükséges és lehetséges lépéseket.

III.11. Az adattovábbítás szabályai

Adatok továbbítására kizárólag jogszabály felhatalmazása, polgári jogi szerződés, vagy az érintett hozzájárulása alapján kerülhet sor.
Az adattovábbítást megelőzően a Városliget Zrt. adatkezelést végző munkatársa ellenőrzi a továbbítandó adatok naprakészségét, pontosságát és teljességét, valamint az adattovábbítás feltételeinek meglétét.
Városliget Zrt-n belüli adattovábbítás során a személyes adatokat kezelő munkatárs köteles körültekintően eljárni, csak olyan munkatársnak küldheti tovább az adatokat, akinek azok kezelésére jogosultsága van. Az adott adatcsoportok útját minden esetben nyomon kell tudni követni.
A harmadik fél felé történő adattovábbítás esetén az adattovábbítást minden esetben írásban dokumentálni kell oly módon, hogy annak menete és jogszerűsége bizonyítható legyen. Az egyes adatkezelésekhez készült adatkezelési tájékoztatóban tájékoztatni kell az érintetteket az adattovábbítások tényéről és címzettjeiről. Az adattovábbítás előtt az adatkezelést végző munkatárs tájékoztatja az adatvédelmi tisztviselőt az adattovábbítás lényeges jellemzőiről (a kezelt adatok továbbításának módja és időpontja, a továbbított adatkörök, az adattovábbítás jogalapja, az adattovábbítás címzettje, az adattovábbításért felelős neve és elérhetősége) szükség esetén kikéri álláspontját. Az adattovábbításokról az adatvédelmi tisztviselő naprakész nyilvántartást vezet.

III.12. Az adatvédelmi incidenskezelési eljárásrend

Az adatbiztonság sérülése, illetve a Városliget Zrt. által kezelt személyes adatok véletlen vagy jogellenes megsemmisülése, elvesztése, módosulása, jogosulatlan továbbítása vagy nyilvánosságra hozatala, továbbá az azokhoz való jogosulatlan hozzáférés (a továbbiakban: adatvédelmi incidens) bekövetkezését annak észlelését követően azonnal jelenteni kell az adatvédelmi tisztviselőnek és az Adatkezelő vezetőjének.

A leggyakrabban előforduló adatvédelmi incidensek például:

- hivatali laptop vagy mobiltelefon elvesztése;
- bármilyen számítógépes vírus előfordulása
- e-mail vagy elektronikus üzenet téves címzett részére való kiküldése, illetve nagyszámú címzett részére úgy kiküldött e-mail, hogy a címzettek nem „titkos másolat"-ban szerepelnek.
- személyes adatok nem biztonságos tárolása, továbbítása;
- ügyfél- és partnerlisták illetéktelen másolása, továbbítása;
- szerver elleni támadás;
- honlap feltörése
- jelszó nem megfelelő védelme, illetéktelen személyek hozzáférése a jelszavakhoz.

Az adatvédelmi tisztviselő a jelzést követően azonnal tájékozódik az eset lényeges körülményeiről, és a kárenyhítési intézkedések megtétele mellett értékeli annak az érintettek jogaira nézve gyakorolt hatásának súlyosságát.

Az értesítésnek tartalmaznia kell

- bejelentő nevét
- a bekövetkezett incidens jellegét;
- az incidenssel valószínűsíthetően érintett személyek körét;
- a valószínűsíthetően érintett adatok kategóriáit, nagyságrendjét;
- a megtett halaszthatatlan intézkedéseket.

Az adatvédelmi tisztviselő megvizsgálja az értesítésben foglaltakat.

Az adatvédelmi tisztviselő indokolatlan késedelem nélkül, de legkésőbb az adatvédelmi incidens észlelésétől számított 72 órán belül a rendelkezésre álló adatokat és a megtett intézkedéseket bejelenti a NAIH-hoz az e célból rendszeresített felületen keresztül, amennyiben az értesítésben foglaltak az adatvédelmi tisztviselő előzetes értékelése szerint valószínűsíthetően helytállóak, és annak jogszabályban meghatározott feltételei fennállnak. A bejelentés mellőzhető, amennyiben az adatvédelmi tisztviselő az előzetes értékelése alapján azt állapítja meg, hogy az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve.

Ha a bejelentés 72 órán belül nem tehető meg, akkor a késedelmes jelentésben meg kell jelölni a késedelem okát, az előírt információkat pedig – további indokolatlan késedelem nélkül– részletekben is közölni lehet.

Az adatvédelmi tisztviselő a bejelentést követően intézkedik a kivizsgálás szükség szerinti pontosításáról, és amennyiben megállapítja, hogy az incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira nézve, akkor tájékoztatnia kell az érintetteket az adatvédelmi incidensről.

Az adatvédelmi tisztviselő értesítését munkaidőben telefonon majd írásban megerősítve e-mailben, munkaidőn túl e-mailben kell megtenni az adatvédelemi tisztviselő számára a honlapon közzétett telefonszámon és az adatvedelem@ligetbudapest.hu e-mailcímen.

Az adatvédelmi tisztviselő az adatvédelmi incidenssel kapcsolatos intézkedések ellenőrzése, valamint az érintett tájékoztatása céljából az adatvédelmi incidensekről nyilvántartást vezet, amely az adatvédelmi incidenssel érintett személyes adatok körét, az adatvédelmi incidenssel érintettek körét és számát, az adatvédelmi incidens időpontját, körülményeit, hatásait és az elhárítására megtett intézkedéseket, valamint az adatkezelést előíró jogszabályban meghatározott egyéb adatokat tartalmazza.

Az adatvédelmi incidens értékelése

Az Adatkezelő az 1. mellékletben szereplő szempontrendszer szerint értékeli az adatvédelmi incidenst

Az érintettek tájékoztatása

A GDPR 34. cikke szerint: '*Ha 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.*" Ennek megfelelően az Adatkezelő az érintettek értesítését a GDPR 34. cikke (2) bekezdése szerint végzi.

Az Adatvédelmi tisztviselő az eset összes körülményének a mérlegelésével dönti el az értesítés módját, de szükség esetén köteles kapcsolatba lépni a Nemzeti Adatvédelmi és Információ Hatósággal a legmegfelelőbb tájékoztatási mód kiválasztására.

(3) Az érintettet nem kell tájékoztatni, ha a következő feltételek bármelyike teljesül:

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, és a külön értékelő lap szerint értékelve a 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.

IV. AZ ÉRINTETTEK JOGAI

Az érintett

a) tájékoztatást kérhet személyes adatainak kezeléséről,

b) kérheti személyes adatainak helyesbítését, törlését vagy az adatkezelés korlátozását,

c) tiltakozhat az Adatkezelő által folytatott adatkezelés ellen, kivéve, ha az adatkezelést jogszabály írja elő,

d) jogainak megsértése, valamint az Adatkezelő adatkezelésre vonatkozó döntése ellen a NAIH-hoz vagy bírósághoz fordulhat.

Az érintett részére – személyazonosságának egyértelmű megállapítását követően - az egyes nyilvántartásokban szereplő konkrét személyes adatainak megadásával kell teljesíteni a tájékoztatást.

Az érintett jogainak érvényesítése iránti kérelméről az adatvédelmi tisztviselőt haladéktalanul értesíteni kell.

Az adatvédelmi tisztviselő

a) a kézhezvételtől számított 3 napon belül értesíti az adatkezelés szakmai felügyeletét ellátó szervezeti egységet, szervet

b) a kérelem kivizsgálása során egyeztet azok vezetőivel,

c) vizsgálata kiterjed valamennyi olyan nyilvántartásra, amelyben az érintett szerepel,

d) az érintettet a jogszabályban előírt határidőn belül tájékoztatja a vizsgálat eredményéről.

Amennyiben az érintett adatát helyesbíteni vagy törölni kell,

a) az adatvédelmi tisztviselő soron kívül kezdeményezi annak végrehajtását,

b) az adatkezelés szakmai felügyeletét ellátó, illetve az adattovábbításért felelős szervezeti egység, szerv vezetője soron kívül intézkedik annak végrehajtásáról.

1. **Előzetes tájékozódáshoz való jog:**

a) Az adatkezelő az adatkezelés megkezdése előtt minden esetben tájékoztatja az érintettet az adatkezelés céljáról és jogalapjáról adatkezelési tájékoztatót készít és tesz elérhetővé. Az adatkezelési tájékoztató elérhetővé tétele előtt az adatkezelés nem kezdhető meg.

b) Az adatkezelési tájékoztatót a Városliget Zrt. honlapján közzé kell tenni, mely az adatvédelmi tisztviselő feladata.

2. **A hozzáféréshez való jog (tájékoztatás az érintett kérelmére):**

a) Az érintettnek a Városliget Zrt. által végzett adatkezelések kapcsán joga van ahhoz, hogy a Városliget Zrt. által tárolt személyes adatait és a kezelésükkel kapcsolatos információkat megismerhesse, bármikor kikérje, ellenőrizze, hogy a Városliget Zrt. milyen személyes adatait kezeli.

b) Hozzáférési jog gyakorlása esetén az érintett az alábbi információkról kérhet tájékoztatást:

- a kezelt adatok köre,
- az adatkezelés célja, ideje, jogalapja,
- történik-e vagy fog-e történi adattovábbítás és kinek a részére,
- az adatok tárolásának tervezett időtartama, vagy ezen időtartam meghatározásának szempontjai,
- a tárolt adatok helyesbítésének, törlésének, kezelés korlátozása kérelmezésének joga, adatok kezelésével kapcsolatos tiltakozás joga, adatforrás megjelölése, amennyiben nem az érintettől gyűjtötték,

3. **Kezelt személyes adatok helyesbítéséhez, kiegészítéséhez való jog:**

Az érintett kérelmére a Városliget Zrt. adatkezelést végző munkatársa indokolatlan késedelem nélkül helyesbíti az érintett által, írásban megjelölt pontatlan személyes adatokat, illetve az adatkezelés célját szem előtt tartva - a hiányos adatok kiegészítését elvégzi az érintett által megjelölt tartalommal. A helyesbítés tényéről az adatkezelést végző munkatársa köteles tájékoztatni mindenkit, akinek az érintett adatot továbbította, átadta, megosztotta.

4. **A törléshez való jog:**

A Városliget Zrt. adatkezelést végző munkatársa az alábbi esetekben haladéktalanul köteles törölni az adatokat:

a) ha az adatkezelésének célja megvalósult és már nincs szükség az adatok további kezelésére;

b) az érintett a hozzájárulását visszavonta és más jogalap nem támasztja alá azadatkezelés jogszerűségét;

c) az adatok kezelése jogellenes;

d) az adatokat az adatkezelőre vonatkozó uniós vagy tagállami jogban előírt jogi kötelezettség teljesítéséhez törölnie kell;

e) az adatok gyűjtésére az információs társadalommal összefüggő szolgáltatások kínálása céljából került sor.

A Városliget Zrt. adatkezelést végző munkatársa a törlést illetően minden rendelkezésre álló technikai eszközt felhasznál , hogy a törlés teljes körű legyen (linkek, másolatok, másodpéldányok törlése, további adatkezelők, adatfeldolgozók, címzettek tájékoztatása a törlés tényéről).

5. Adatkezelés korlátozásához való jog:

Az érintett jogosult arra, hogy írásbeli kérelme esetén a Városliget Zrt. mint adatkezelő korlátozza az adatkezelést, ha

a) az érintett vitatja a személyes adatok pontosságát, ez esetben a korlátozás arra az időtartamra vonatkozik, amely lehetővé teszi, hogy a Városliget Zrt. adatkezelést végző munkatársa ellenőrizze a személyes adatok pontosságát;

b) az adatkezelés jogellenes, az érintett az adatok törlését ellenzi és ehelyett azok felhasználásának korlátozását kéri;

c) a Városliget Zrt-nek már nincs szüksége a személyes adatokra adatkezelés céljából , de az érintett azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez igényli;

d) az érintett tiltakozik az adatkezelés ellen; ez esetben a korlátozás arra az időtartamra vonatkozik, amíg megállapításra nem kerül, hogy a Városliget Zrt. jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben.

A korlátozás időtartama alatt ezen adatokat a tároláson kívül a Városliget Zrt. csak az érintett hozzájárulásával, vagy jogi igények előterjesztéséhez, érvényesítéséhez, vagy védelméhez, vagy más természetes vagy jogi személy jogainak védelmében, vagy fontos közérdekből kezelheti.

A Városliget Zrt. adatkezelést végző munkatársa az adatkezelés korlátozásának feloldásáról előzetesen tájékoztatja azt az érintettet, akinek kérelmére az adatkezelést korlátozta.

6. Adathordozhatósághoz való jog:

Az adathordozhatóság azt teszi lehetővé, hogy az érintett megszerezhesse, és a továbbiakban felhasználhassa a Városliget Zrt. rendszerében megtalálható általa átadott saját személyes adatait, továbbá ezeket az adatokat egy másik adatkezelőnek továbbítsa. Minden esetben az érintett által átadott adatokra korlátozódik a jogosultság, egyéb adatok hordozhatóságára lehetőség nincs

Az érintett a rá vonatkozó adatokat:

a) tagolt, széles körben használt, géppel olvasható formátumban megkapja,

b) jogosult más adatkezelőhöz továbbítani,

c) kérheti az adatok közvetlen továbbítását a másik adatkezelőhöz

Az adathordozhatóság joga kizárólag abban az esetben illeti meg az érintettet, ha az adatkezelés hozzájáruláson vagy szerződésen alapul és az adatkezelés automatizált módon, gépi eszközzel történik.

7. Tiltakozás személyes adatok kezelése ellen:

Az érintett a saját helyzetével kapcsolatos okokból írásban tiltakozhat adatainak kezelése ellen, továbbá az érintett jogosult arra, hogy bármikor tiltakozzon a rá vonatkozó személyes adatok közvetlen üzletszerzés célból történő kezelése ellen.

A tiltakozás joga csak abban az esetben illeti meg az érintettet, ha az adatkezelés közérdekből vagy közhatalmi jogosultság gyakorlása keretében végzett feladat végrehajtásához, illetve az adatkezelő vagy egy harmadik fél jogos érdekei alapján szükséges. Ha az érintett tiltakozik a személyes adatok közvetlen üzletszerzés érdekében történő kezelése ellen, akkor a személyes adatok a továbbiakban e célból nem kezelhetők.

Ha az érintett úgy ítéli meg, hogy a Városliget Zrt. a személyes adatainak kezelése során megsértette a hatályos adatvédelmi követelményeket, akkor

a) panaszt nyújthat be a Hatósághoz, vagy

b) lehetősége van adatainak védelme érdekében bírósághoz fordulni, amely az ügyben soron kívül jár el.

Városliget Zrt.
dr. Gyorgyevics Benedek Tamás vezérigazgató,
munkáltatói jogkör gyakorlója

1. sz. Melléklet: Adatvédelmi incidens értékelése

A személyes adatokkal kapcsolatos jogsértések súlyának meghatározása

A személyes adatok megsértésének súlyosságát e módszer összefüggésében úgy definiálják, mint „az egyénekre az adatvédelmi incidensből származó potenciális hatás nagyságának becslése".

Az adatvédelmi incidens súlyosságának értékelése során három tényező pontos meghatározása és vizsgálata elengedhetetlen, ezek a következők:

- **Adatfeldolgozási kontextus** (DPC): a felhasználási környezethez igazítva meg kell határozni a sérült/károsodott/hozzáférhetetlenné vált adatok típusát. valamint a kapcsolódó tényezőket. Ez képezi a módszer alapját, és értékeli egy adott adatkészlet kockázatát
- **Azonosítás egyszerűsége** (EI): meg kell határozni, hogy a sérült/károsodott/hozzáférhetetlenné vált személyes adatok alanyának azonosítása milyen egyszerű a jogsértésben részt vevő adatok alapján. Ez a DPC korrekciós tényezője
- **A jogsértés körülményei** (CB): meg kell vizsgálni az incidens különleges körülményeit, amelyek további befolyást gyakorolnak a jogsértés súlyosságára.

Az adatvédelmi incidens súlyának értéke a következő képlet alapján számítható ki: **SE = DPC x EI + CB**

Mindhárom kritériumot pontozni kell. A végeredmény alapján négy súlyossági szintre lehet besorolni a jogsértéseket: alacsony, közepes, magas és nagyon magas.

A kritériumok pontozása:

DPC

1. lépés: A személyes adatok típusának meghatározása és osztályozása
- A jogsértésben részt vevő személyes adatok típusának meghatározása.
- Az adatokat besorolása a megfelelő kategóriába a következők közül: egyszerű, viselkedési, pénzügyi és szenzitív adatok. Így megkapjuk az előzetes DPC-pontszámot.

2. lépés: Az adatfeldolgozáshoz kapcsolódó kontextus egyéb tényezőkkel történő kiigazítása
- Értékelni kell bizonyos tényezők előfordulását, amelyek növelhetik vagy csökkenthetik az alappontszámot. Ilyen tényezők lehetnek például adatmennyiség, az adatkezelők vagy az egyének sajátosságai, az adatok érvénytelensége vagy pontatlansága.
- Ha van ilyen értékelendő tényező, akkor ennek megfelelően növelni vagy csökkenteni kell az alappontszámot. Az adatkategóriák szerinti kiigazítási skálákat az 1. táblázat tartalmazza. Ha az adat több kategóriába is beleillik, akkor az összes lehetséges módon el kell végezni a számítást és a legmagasabb pontszámot eredményező esetet kell figyelembe venni.

EI

Az azonosítás egyszerűségének vizsgálata során meg kell határozni, hogy az adat(ok)hoz hozzáférő felek milyen eséllyel tudják beazonosítani az adatok alanyát.

Négy szintet célszerű megkülönböztetni: elhanyagolható, korlátozott, szignifikáns és maximális. Szintenként a pontszám lineáris növekedik. A legalacsonyabb pontszám esetén az egyén azonosításának lehetősége elhanyagolható, ami azt jelenti, hogy lehetséges ugyan, de rendkívül nehéz az adatokat egy adott személyhez kapcsolni. A legmagasabb pontszámot akkor választják ki, ha az egyén

személyazonossága közvetlenül, kutatás nélkül a megsértett adatok alapján felfedezhető. Az EI meghatározásakor figyelembe kell venni, hogy az azonosítás közvetlenül (pl. név alapján) vagy közvetetten (pl. azonosítószám alapján) lehetséges az adatokból.

CB

E kritérium körében több tényező vizsgálandó.

- A bizalmasság elvesztése: ez akkor valósul meg, amikor az információkhoz olyan felek férnek hozzá, akik nem jogosultak arra, vagy akiknek nincsen jogalapja az adatkezeléshez. Mértéke a hozzáférhetővé vált adatok terjedelmétől és adatokhoz (akár csak potenciálisan) hozzáférő személyek számától függ.
- Integritás elvesztése: akkor fordul elő, amikor az eredeti információ megváltozik, és az adatok helyettesítése káros lehet az egyén számára. A legsúlyosabb helyzet az, amikor nagy esély van rá, hogy a megváltoztatott adatokat oly módon használják fel, hogy az egyén számára ártalmas legyen.
- Az elérhetőség elvesztése: az az állapot, amikor az eredeti adatok nem érhetők el. Lehet átmenti (az adatok helyreállíthatók), vagy állandó (az adatokat nem lehet helyreállítani).
- Rosszindulatú szándék: ez az elem azt vizsgálja, hogy a megsértést emberi vagy műszaki hiba okozta-e, vagy rosszindulatú szándékos fellépés áll-e a háttérben.
- A nem rosszindulatú jogsértések közé tartoznak a véletlen elvesztés, az emberi hibák és a szoftverhibák. A rosszindulatú jogsértések közé sorolhatók a lopások és a hackelés, amelyek célja az egyének károsítása, a személyes adatok harmadik félnek nyereség céljából történő átadását.

A jogsértés súlyossága

SE < 2	Alacsony	Az adatok alanyai az incidensben érintetté válhatnak, esetleg néhány kellemetlenséget tapasztalhatnak, de ezek nem okoznak számukra komolyabb kellemetlenséget.
2 ≤ SE <3	Közepes	Az egyének jelentős kellemetlenséget tapasztalhatnak, amelyeket néhány nehézség ellenére képesek leküzdeni (többletköltségek, üzleti szolgáltatásokhoz való hozzáférés megtagadása, félelem, stressz, kisebb testi megbetegedések stb.).
3 ≤ SE <4	Magas	Az egyéneknek jelentős következményekkel kell számolniuk, amelyeket súlyos nehézségekkel tudnak leküzdeni (pénzeszközök eltulajdonítása, bankok feketelistájára való felkerülés, ingatlankár, munkahely elvesztése, egészségromlás stb.).
4 ≤ SE	Nagyon magas	Az egyéneknek jelentős, sőt visszafordíthatatlan következményekkel kell számolniuk, amelyeket nem tudnak megoldani (pénzügyi nehézségek, munkaképtelenség, pszichológiai vagy fizikai betegségek, halál stb.).

Két további tényező figyelembevétele válhat még indokolttá. Ezek a következők:

- Az érintett személyek száma meghaladja a 100-at. Egy nagyobb esemény bekövetkeztével az érintett személyek adatai valószínűleg könnyebben hozzáférhetővé tehetők, valamint az érintett személyek nagy száma befolyásolja a jogsértés általános mértékét.
- Az adatok nem érthetők. A nem értelmezhetőség (például erős titkosítás) jelentősen csökkentheti az egyénekre gyakorolt hatást, mivel ez jelentősen csökkenti az illetéktelen felek számára az adatokhoz való hozzáférés lehetőségét.

DPC pontszámok meghatározása

egyszerű adat	életrajzi adat, elérhetőségek, teljes név, képzési adatok, családi életre vonatkozó adat, szakmai tapasztalatok stb.	
	Előzetes alappontszám: amikor a jogsértés „egyszerű adatokat" tartalmaz, és az adatkezelő nem ismer súlyosbító tényezőket.	1
	A 1-gyel növelhető, ha az „egyszerű adatok" mennyisége és/vagy az adatkezelő jellemzői olyanok, hogy engedélyezhető az egyén bizonyos profilozása, vagy feltételezések tehetők az egyén társadalmi, pénzügyi helyzetére.	2
	A pontszám 2-vel növelhető, ha az „egyszerű adatok" és/vagy az adatkezelő jellemzői feltételezésekhez vezethetnek az egyén egészségi állapotára, szexuális preferenciáira, politikai vagy vallási meggyőződésére vonatkozóan.	3
	A pontszámot 3-mal lehet növelni, ha az egyén bizonyos tulajdonságai miatt, az információ kockázatot jelentene az egyén személyes biztonságára vagy fizikai, pszichológiai állapotára.	4
viselkedési adat	hely, forgalmi adatok, személyes szokások és igények stb.	
	Előzetes alap pontszám: amikor a jogsértés magába foglal „viselkedési adatokat" és az adatkezelő nem ismer súlyosbító vagy enyhítő tényezőket.	2
	A pontszámot 1-gyel csökkenthetjük, ha az adatkészlet jellege nem nyújt lényeges betekintést az egyén viselkedésével kapcsolatos információkba, vagy az adatok nyilvános forrásokból begyűjthetők. (például az internetes keresésekből).	1
	A pontszám 1-gyel növelhető, ha a „viselkedési adatok" mennyisége és/vagy az adatkezelő jellemzői olyanok, hogy az egyén profilja létrehozható és az részletes információkat szolgáltat a mindennapi életéről és szokásairól.	3
	A pontszám 2-vel növelhető, ha az egyén érzékeny adatain alapuló profil létrehozható.	4
pénzügyi adat	bármilyen pénzügyi adat (pl. bevétel, financiális tranzakciók, bankszámlakivonatok, befektetések, hitelkártya adatok, számlák stb.), beleértve a szociális jóléthez kapcsolódó információkat.	
	Előzetes alap pontszám: amikor a jogsértés „pénzügyi adatokat" foglal magába és az adatkezelőnek nincs tudomása semmilyen súlyosbító vagy enyhítő tényezőről.	3
	A pontszámot 2-vel csökkenthetjük, ha az adatkészlet jellege nem nyújt lényeges betekintést az egyén pénzügyi adataival kapcsolatos információkba	1
	A pontszámot 1-gyel csökkenthetjük, ha az adott adatkészlet tartalmaz bizonyos pénzügyi információkat, de még mindig nem nyújt lényeges betekintést az egyén pénzügyi helyzetébe.	2
	A pontszámot 1-gyel lehet növelni, ha az adott adatkészlet természete és/vagy mennyisége miatt teljes pénzügyi információ kerül nyilvánosságra, így lehetővé tesz csalást, vagy részletes társadalmi, pénzügyi profil kialakítást.	4
szenzitív adat	bármilyen szenzitív adat (pl. egészségügyi adatok, politikai nézetek, szexuális életre vonatkozó adatok)	
	Előzetes alap pontszám: amikor a jogsértés „érzékeny adatokat" tartalmaz, és az adatkezelő nem ismer enyhítő tényezőt.	4
	A pontszámot 1-re csökkenthetjük, ha az adatkészlet jellege nem nyújt lényeges betekintést az egyén viselkedésével kapcsolatos információkba, vagy az adatok könnyen nyilvános forrásokon keresztül gyűjthetők.	1
	A pontszámot 2-vel csökkenthetjük, ha az adatok jellege általános feltételezésekhez vezethet.	2
	A pontszámot 1-gyel csökkenthetjük, ha az adatok jellege az érzékeny információkkal kapcsolatban feltételezésekhez vezethet.	3

Pontszámot növelő tényezők:

- A megsértett adatok mennyisége (ugyanazon egyén esetében): ez a tényező növelheti az alapvető DPC-pontszámot a megsértett információ mennyiségének növekedése miatt (azaz súlyosbító tényezőként szolgál). Figyelembe kell venni a hozzáférhetőség időtartamát és magát a hozzáférhetővé vált adatok tartalmát is.
- Az adatkezelő különleges tulajdonságai: ez a tényező az adatkezelő működési területére és tevékenységeire vonatkozik, amelyek növelhetik az adatok alapvető DPC-pontszámát, és további információkkal szolgálhatnak egy adott adatkészletre vonatkozóan.
- Az egyének sajátos jellemzői: egy adott adatkészlet alapvető DPC-pontszáma szintén növelhető abban az esetben, ha az egyének különleges szükségletekkel rendelkező társadalmi csoporthoz tartoznak.

Pontszámot csökkentő tényezők:

- Az adatok érvénytelensége, pontatlansága: egy adott adatkészlet alapvető DPC-pontszáma csökkenthető, ha az adat érvénytelensége vagy pontatlansága ismert az adatkezelő számára és így a jelentőségük csökken.
- Nyilvános hozzáférhetőség: az adatkészlet alapvető DPC-pontszáma szintén csökkenthető abban az esetben, ha a megsértett adatok a jogsértés előtt már nyilvánosan hozzáférhetők voltak, vagy könnyen összegyűjthetők és/vagy hozzáférhetők a nyilvánosan elérhető forrásokon keresztül.
- Az adatok jellege: egy másik csökkenő tényező bizonyos esetekben lehet egy adott adatkészlet természete, amely kevésbé fontos az információk szempontjából, amelyet az egyénről felfedhet.

EI pontszámok meghatározása

A következő azonosító adatok befolyásolják az EI pontszámának értékét:

- Teljes név (keresztnév, vezetéknév)

Ez a leggyakoribb közvetlen azonosító, de az EI pontszáma esetenként változhat, mivel a teljes név önmagában nem mindig jelöli ki az egyént.

Ha az azonosítást csak az egyén teljes nevével hajtják végre:

- EI = 0,25 (elhanyagolható) egy ország lakossága körében, ahol sokan ugyanazt a teljes nevet használják;
- EI = 0,5 (korlátozott) egy lakossága körében, ahol kevés az azonos névvel rendelkező egyén;
- EI = 0,75 (jelentős) egy kisváros lakossága körében;
- EI = 1 (maximális) egy ország lakosságában, a születési dátum és az e-mail cím megadásával is.

- Személyi igazolvány / útlevél / társadalombiztosítási szám

Mindegyik egyedi azonosítónak tekinthető, és felhasználható az egyén meghatározására.

Ha az azonosítást ezen számok közül csak az egyik segítségével hajtják végre:

- EI = 0,25 (elhanyagolható), ha nem adnak meg más információt az egyénről, vagy nem lehet további információt találni referencia-adatbázis használatának hiányában;
- EI = 0,75 (jelentős), ha az azonosító további azonosítási információkat derít fel az egyénről és más adatokhoz kapcsolódik;
- EI = 1 (maximális), ha referencia-adatbázisból is rendelkezésre állnak információk.

- Telefonszám / otthoni cím

Mindkettő közvetett azonosító, amely felhasználható az egyénnel való kommunikációra vagy elérhetőségére.

Ha az azonosítás csak a két azonosító egyikén alapszik:

- EI = 0,25 (elhanyagolható) egy ország lakosságában, ha a számot/címet nem vették nyilvános nyilvántartásba;
- EI = 0,5 (korlátozott) egy kisváros lakosságában, és a számot/címet nem vették a nyilvánosan elérhető nyilvántartásba;
- EI = 1 (maximális) egy ország lakosságában, és a szám/cím szerepel nyilvánosan elérhető nyilvántartásban.

- Email cím

Ez egy közvetett azonosító is, amelyet fel lehet használni az egyénnel való kommunikációra, és bizonyos esetekben információkat tartalmaz a nevére vonatkozóan.

Ha az azonosítás e-mail cím alapján történik:

- EI = 0,25 (elhanyagolható), ha az e-mail cím nem tár fel semmilyen más azonosítási információt, és nem használják az egyén elsődleges címeként internetes oldalakon, fórumokon vagy közösségi hálózatokon.
- EI = 0,75 (jelentős), ha az e-mail cím nem tár fel semmilyen más azonosítási információt, de az egyén elsődleges címeként használja az internetes oldalakon, fórumokon vagy közösségi hálózatokon (és így kereshető az interneten).
- EI = 1 (maximális), ha az e-mail cím feltárja az egyén nevét, és elsődleges címeként használja internetes oldalakon, fórumokon vagy közösségi hálózatokon (és így kereshető az interneten).

- Kép

Lehet közvetlen vagy közvetett azonosító, az esettől függően.
Ha az azonosítás csak egy képen alapszik:

- EI = 0,25 (elhanyagolható), ha a kép homályos;
- EI = 0,5 (korlátozott), ha a kép nem világos vagy homályos, de tartalmaz további információkat (például felismerhető környezet), amelyek az egyén azonosításához vezethetnek;
- EI = 0,75 (jelentős), ha a kép tiszta, de más azonosítási információ nem kapcsolódik hozzá;
- EI = 1 (maximális), ha a kép tiszta és valamilyen kiegészítő információ kapcsolódik hozzá.

- Kódolás/ álnevek / Monogram

Az egyedi azonosítókhoz hasonlóan, a kódok és álnevek is használhatók az egyén azonosításához, amennyiben lehetséges, hogy összekapcsolják őket egy referencia-adatbázissal.
Kódolás vagy álnevek használata alapján:

- EI = 0,25 (elhanyagolható), ha a kód/álnév nem tár fel az egyén más személyes adatai közül referencia-adatbázishoz való hozzáférés nélkül;
- EI = 0,75 (Jelentős), ha az álnév valamilyen adatot tár fel az egyénről és más személyes adatokhoz kapcsolódik;
- EI = 1 (maximális), ha az álnév feltárja az egyén teljes nevét vagy adatait a referencia-adatbázisból.

CB pontszámok meghatározása

- A bizalmasság elvesztése
  - 0 – a bizalmassági kockázatnak kitett adatokra vonatkozik, de nincs arra bizonyíték, hogy illegális adatkezelés történt
    - ✓ A papír vagy a laptop eltűnik;
    - ✓ A berendezésektől a személyes adatok megsemmisítése nélkül megszabadultak
  - +0,25 – ismert számú címzett rendelkezésére bocsátott adatok esetén
    - ✓ Ismert számú címzettnek küldtek helytelenül e-mailt személyes adatokkal;
    - ✓ Néhány ügyfél hozzáférhet más ügyfelek fiókjaihoz egy online szolgáltatás révén.
  - +0,5 – nem ismert számú címzettek számára eljuttatott adatok esetén
    - ✓ Az adatokat egy internetes üzenőfalon közzéteszik;
    - ✓ Az adatokat egy P2P webhelyre töltik fel;
    - ✓ Az alkalmazott elad egy CD-ROM-ot vagy egyéb adathordozót az ügyféladatokkal;
    - ✓ A helytelenül konfigurált webhely nyilvánosan elérhetővé teszi a belső felhasználók internetes adatait.
- Az integritás elvesztése
  - 0 - adatváltoztatás esetén, de helytelen vagy illegális felhasználás fennállása nélkül:
    - ✓ A személyes adatokkal rendelkező adatbázis nyilvántartásait helytelenül frissítették, de az eredeti adatok megszerzése megtörtént a megváltozott adatok bármilyen felhasználása előtt.
  - +0.25 – adatváltoztatás esetén, valószínűleg helytelen vagy illegális felhasználás történt vagy történhet, de helyreállítási lehetőséggel:
    - ✓ Megváltozott az online szociális szolgáltatás nyújtásához szükséges rekord, és az egyénnek egy adott szolgáltatásban kell kérnie a szolgáltatást. offline módon.
    - ✓ Megváltozott egy olyan rekord, amely fontos az egyén fájljának pontossága szempontjából az online orvosi szolgálatban.
  - +0,5 – adatváltoztatás esetén, valószínűleg helytelen vagy illegális felhasználására anélkül, hogy helyreállítanák:

- ✓ Az előző példák + az eredeti adatok nem állíthatók helyre.

- Az elérhetőség elvesztése
  - ➢ 0 – az adatok bármilyen nehézség nélkül helyreállíthatók
    - ✓ A fájl másolata elveszett, de más másolatok rendelkezésre állnak;
    - ✓ Az adatbázis sérült, de könnyen rekonstruálható más adatbázisokból.
  - ➢ +0,25 – az adatok ideiglenesen elérhetetlenek
    - ✓ Az adatbázis sérült, de rekonstruálható más adatbázisokból némi feldolgozás útján;
    - ✓ Egy fájl elveszik, de az információ az egyén részéről ismét szolgáltatható.
  - ➢ +0.5 – az adatok teljesen elérhetetlenek
    - ✓ Egy fájl elveszett vagy az adatbázis megsérült és az adatokról nincs biztonsági másolat, és az egyén nem tudja azokat szolgáltatni.
- rosszindulatú szándék
  - ➢ +0,5 – a jogsértés szándékosan történt
    - ✓ Egy vállalat alkalmazottja szándékosan megosztja az ügyfelek személyes adatait egy közösségi média nyilvános webhelyén;
    - ✓ Egy vállalat alkalmazottja ügyfelek magánadatait ad el egy másik társaságnak;
    - ✓ A közösségi hálózat egyik tagja szándékosan küld információt a többi tagról azok családtagjai számára, azzal a céllal, hogy ártson nekik.