Debreceni Vagyonkezelő
Zártkörűen Működő Részvénytársaság

| | | |
|---|---|---|
| Folyamatszponzor: | Marossy Virág | vezérigazgató |
| Folyamatgazda: | dr. Molnár Péter | adatvédelmi tisztviselő |
| Ellenőrizte: | dr. Puskás Ágnes | megfelelési és szabályozási igazgató |

# DEBRECENI VAGYONKEZELŐ ZRT. ADATVÉDELMI INCIDENSEK KEZELÉSÉRŐL SZÓLÓ SZABÁLYZATA

Ezen szabályzatot jóváhagyta:

Marossy Virág s.k.
vezérigazgató

| Kiadások sorszáma | Iktatószáma | Hatály (-tól -ig) |
|---|---|---|
| 1. | DV-315-1/2025. | A Vezérigazgató általi ellenjegyzés napján lép hatályba és visszavonásig érvényes |
| 2. | | |
| | | |
| | | |
| | | |
| | | |

# TARTALOMJEGYZÉK

# 1. BEVEZETŐ RENDELKEZÉSEK

## 1.1 A SZABÁLYZAT CÉLJA

Jelen szabályzat (a továbbiakban: Szabályzat) célja, hogy meghatározza a Debreceni Vagyonkezelő Zártkörűen Működő Részvénytársaság (a továbbiakban: DV Zrt.) tevékenysége során esetlegesen bekövetkező adatvédelmi incidensek meghatározására, kezelésére, a megakadályozására vagy enyhítésére, az adatvédelmi hatóság részére történő bejelentés megtételére, és az adatvédelmi incidens nyilvántartásának vezetésére.

## 1.2 A SZABÁLYZAT HATÁLYA

### 1.2.1 Tárgyi hatály

Jelen szabályzat tárgyi hatálya kiterjed a DV Zrt. valamennyi szervezeti egységénél esetlegesen bekövetkezett adatvédelmi incidensre.

### 1.2.2 Személyi hatály

Jelen szabályzat személyi hatálya kiterjed a DV Zrt.-vel munkaviszonyban álló természetes személyekre (továbbiakban együtt: munkatársak), valamint mindazon természetes személyekre, akiknek jogait vagy jogos érdekeit az adatvédelmi incidens érinti.

### 1.2.3 Időbeli hatály

Jelen szabályzat a záró rendelkezésben meghatározott időponttól visszavonásig hatályos.

### 1.2.4 Alkalmazandó legfontosabb jogszabályok

- Az Európai Parlament és a Tanács (EU) 2016/679 Rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (a továbbiakban: GDPR)
- Magyarország Alaptörvénye,
- Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény,
- Az Európai Adatvédelmi Testület (EDPB, korábban WP29-es munkacsoport) Iránymutatásai, valamint a Nemzeti Adatvédelmi és Információszabadság Hatóság által kiadott vélemények, ajánlások, tájékoztatók, vélemények

# 2. ÉRTELMEZŐ RENDELKEZÉSEK

E szabályzat alkalmazásában (FOGALOM MEGHATÁROZÁSOK)

**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.
**adatkezelési folyamat:** az adatkezelő szervezeti egység egy konkrét feladatával összefüggésben, a személyes adatokon egy meghatározott adatkezelési célból végzett adatkezelési művelet vagy műveletek összessége.

**adatkezelő:** az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki, vagy amely önállóan vagy másokkal együtt az adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajttatja (a továbbiakban: DV Zrt.)
**adatkezelő szervezeti egység:** a DV Zrt. mindenkor hatályos Szervezeti és Működési Szabályzata szerinti szervezeti egysége, amely az adatkezelést a DV Zrt. nevében és érdekében végzi.
**adatfeldolgozó:** az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, aki, vagy amely szerződés alapján – beleértve a jogszabály rendelkezése alapján kötött szerződést is – az adatkezelő nevében személyes adatokat kezel, adatfeldolgozást végez.
**adatmegsemmisítés:** az adatok vagy az azokat tartalmazó adathordozó teljes fizikai megsemmisítése.
**adattörlés:** az adatok felismerhetetlenné tétele oly módon, hogy a helyreállításuk többé nem lehetséges.
**adatfeldolgozás:** az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől, feltéve, hogy a technikai feladatot az adatokon végzik.
**adatvédelmi felügyeleti hatóság:** a nemzeti jog által kijelölt illetékes adatvédelmi felügyeleti hatóság. A jelen utasítás kiadásakor az adatvédelmi felügyeleti hatóság feladatait a Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: **NAIH**) látja el.
**adattovábbítás:** az adat meghatározott harmadik fél számára történő hozzáférhetővé tétele.
**profilalkotás:** személyes adatok automatizált kezelésének bármely olyan formája, amelynek során a személyes adatokat valamely természetes személyhez fűződő bizonyos személyes jellemzők értékelésére, különösen a munkahelyi teljesítményhez, gazdasági helyzethez, egészségi állapothoz, személyes preferenciákhoz, érdeklődéshez, megbízhatósághoz, viselkedéshez, tartózkodási helyhez vagy mozgáshoz kapcsolódó jellemzők elemzésére vagy előrejelzésére használják.
**személyes adat:** 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.
**személyes adatok különleges kategóriája**: a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a természetes személyek egyedi azonosítását célzó genetikai és biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok.

## 3. ALKALMAZANDÓ RENDELKEZÉSEK

### 3.1 AZ ADATVÉDELMI INCIDENS FOGALMA, AZONOSÍTÁSA, JELLEMZŐI

**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.

A személyes adat *megsemmisítése* azt jelenti, hogy a személyes adat már nem létezik, legalábbis nincs meg olyan formátumban, amelyben az adatkezelő számára bármilyen módon felhasználható lenne.

A személyes adatok *elvesztéséről* akkor beszélhetünk, ha a személyes adat továbbra is létezik, de az adatkezelő nem fér hozzá, nincs a birtokában.

A személyes adatok *megváltoztatásáról* akkor beszélhetünk, ha a személyes adat állapotában, tartalmában, illetve megjelenésében módosulás történik.

*Jogosulatlan közlés* akkor következik be, ha arra illetéktelen személyekkel a személyes adatot megosztják, míg jogosulatlan hozzáférésről akkor beszélhetünk, ha illetéktelen személy képes a személyes adatot megismerni. A személyes adatok *károsodásáról* pedig akkor beszélhetünk, ha az eredeti adatállományt megváltoztatták, az nem teljes.

Az adatvédelmi incidenseket jellegük szerint különösen az alábbi kategóriákba sorolhatjuk:

- *Bizalmassági incidens:* személyes adatok véletlen vagy felhatalmazás nélküli közlése vagy az ezekhez való jogosulatlan hozzáférés. A bizalmassági incidenst bekövetkezettnek kell tekinteni abban az esetben is, ha a személyes adatokhoz való jogosulatlan hozzáférés lehetősége fennáll, de az adatvédelmi incidens körülményeinél fogva nem igazolható a személyes adatokhoz arra nem jogosult személyek által történő tényleges hozzáférés.
- *Sértetlenséggel kapcsolatos incidens:* személyes adatok véletlen vagy jogosulatlan megváltoztatása.
- *Hozzáférhetőséggel kapcsolatos incidens:* személyes adatok véletlen vagy jogosulatlan megsemmisítése vagy a személyes adatok elvesztése.

Az adatvédelmi incidens megfelelő és kellő idejű intézkedés hiányában fizikai, vagyoni vagy nem vagyoni károkat okozhatnak a természetes személyeknek, különösen ha az adatkezelésből

a) hátrányos megkülönböztetés,
b) személyazonosság-lopás, vagy személyazonossággal való visszaélés,
c) pénzügyi veszteség,
d) a jó hírnév sérelme,
e) a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülése,
f) álnevesítés engedély nélkül történő feloldása, vagy
g) bármely egyéb jelentős gazdasági vagy szociális hátrány fakadhat, vagy
h) az érintettek nem gyakorolhatják jogaikat és szabadságaikat, vagy
i) nem rendelkezhetnek a saját személyes adataik felett, vagy ha
j) olyan személyes adat kezelése történik, amelyek
    - faji, vagy etnikai származásra,
    - politikai véleményre,
    - vallási vagy világnézeti meggyőződésre, vagy szakszervezeti tagságra utalnak, valamint ha
    - személyes jellemzők értékelésére, így különösen munkahelyi teljesítménnyel kapcsolatos jellemzők, gazdasági helyzet, egészségügyi állapot, személyes preferenciák vagy érdeklődési körök,
    - megbízhatóság vagy viselkedés,

- tartózkodási hely vagy mozgás elemzésére vagy előrejelzésére kerül sor személyes profil létrehozása vagy felhasználása céljából, vagy
- ha kiszolgáltatott személyek – különösen, ha gyermek – személyes adatainak a kezelésére kerül sor, vagy
- ha az adatkezelés nagy mennyiségű személyes adat alapján zajlik, és nagyszámú érintettre terjed ki.

### 3.2 AZ ADATVÉDELMI INCIDENSEK MEGELŐZÉSÉVEL ÉS KEZELÉSÉVEL KAPCSOLATOS FELELŐSSÉGEK

A személyes adatok biztonságát sértő események megelőzése és kezelése (eljárásrend kialakítása, a szükséges intézkedések elrendelése) a DV Zrt. képviseletében eljáró Vezérigazgató felelőssége, akinek ezen feladata a DV Zrt. Adatvédelmi szabályzatban meghatározott hatáskörei gyakorlásán keresztül a DV Zrt. szervezeti struktúrájában meghatározott vezetői számára adatvédelemmel és adatbiztonsággal kapcsolatos további feladatokat és beszámolási kötelezettségeket határoz meg.
Ennek érdekében a DV Zrt. valamennyi adatkezelő szervezeti egysége vezetőjének alapvető kötelezettsége

a) a szervezeti egységét érintő adatvédelmi és adatbiztonsági szabályozottságot, valamint a szabályok betartását figyelemmel kísérni, amely elsődleges feltétele az adatvédelmi incidensek megelőzésének,
b) az adatbiztonságot sértő nem várt esemény észlelése esetén indokolatlan késedelem nélkül intézkedést kezdeményez illetve foganatosít annak érdekében, hogy az adatbiztonságot sértő nem várt esemény megszüntetésre, a hibás vagy hiányos belső szabályozás helyesbítésre illetőleg kiegészítésre kerüljön,
c) a helytelen alkalmazási gyakorlat megszüntetése mellett indokolt esetben személyi felelősség megállapításának kezdeményezése a Vezérigazgatónál.

Továbbá a DV Zrt. valamennyi dolgozójának feladata és kötelessége az észlelt adatbiztonságot sértő esemény jelzése a szolgálati út betartásával és a megszüntetésük érdekében az elrendelt intézkedések megvalósítása.

### 3.3 AZ ADATVÉDELMI INCIDENS KEZELÉSÉRE VONATKOZÓ SZABÁLYOK

A DV Zrt., vagyis az adatkezelő akár belső, akár külső jelzés alapján értesülhet a nemvárt eseményről.
Belső jelzésnek minősül, ha a DV Zrt.-vel munkaviszonyban, munkavégzésre irányuló egyéb jogviszonyban álló személy, vagy a DV Zrt.-vel kötött szerződés alapján eljáró adatfeldolgozó észleli a nemvárt eseményt.
Amennyiben a DV Zrt.-vel munkaviszonyban, munkavégzésre irányuló egyéb jogviszonyban álló személy észleli a nemvárt eseményt, köteles haladéktalanul, legfeljebb azonban az észleléstől számított 2 órán belül tájékoztatni az adatkezelő szervezeti egység vezetőjét illetve a Vezérigazgatót, valamint az adatvédelmi tisztviselőt.
Amennyiben a DV Zrt.-vel kötött szerződés alapján eljáró adatfeldolgozó észleli a nemvárt eseményt, köteles az említett szerződésben meghatározott kapcsolattartó útján haladéktalanul, legfeljebb azonban az észleléstől számított 2 órán belül tájékoztatni a Vezérigazgatót, valamint a DV Zrt. adatvédelmi tisztviselőjét.

Külső jelzésnek minősül, ha a fentieken meghatározott személyek körén kívül eső bármely személy észleli a nemvárt eseményt, és erről – szóban, írásban vagy elektronikus úton – tájékoztatja a DV Zrt.-t.
Amennyiben a külső jelzés az adatkezelővel munkaviszonyban, munkavégzésre irányuló egyéb jogviszonyban álló személyhez érkezik, e személy köteles haladéktalanul, legfeljebb azonban az észleléstől számított 2 órán belül tájékoztatni az adatkezelő szervezeti egység vezetőjét illetve a Vezérigazgatót, valamint az adatvédelmi tisztviselőt.
Amennyiben a DV Zrt.-vel kötött szerződés alapján eljáró adatfeldolgozóhoz érkezik a tájékoztatás, köteles az említett szerződésben meghatározott kapcsolattartó útján haladéktalanul, legfeljebb azonban az észleléstől számított 2 órán belül tájékoztatni a Vezérigazgatót, valamint az adatvédelmi tisztviselőt.
A NAIH DV Zrt.-nek küldött megkeresése minden esetben külső jelzésnek minősül.
Amennyiben a tájékoztatás valamilyen okból kizárólag a Vezérigazgatóhoz érkezik be, az haladéktalanul, legfeljebb a beérkezéstől számított 2 órán belül továbbítja a nem várt eseményről szóló tájékoztatást az adatvédelmi tisztviselő részére.
Az adatvédelmi tisztviselő az értesítést követően haladéktalanul, de legkésőbb a tudomására jutástól számított 2 órán belül összehívja az incidenskezelő csoportot.
Az incidenskezelő csoport feladata az adatvédelmi incidens körülményeinek feltárása, az adatvédelmi incidens kockázatainak felmérése, elemzése és kezelése, valamint az adatvédelmi incidenssel kapcsolatos további intézkedések megtételére vonatkozó döntéshozatal.
Az incidenskezelő csoport vezetését és irányítását az adatvédelmi tisztviselő látja el.
Az incidenskezelő csoport az adatvédelmi incidens kezelésének lezárásáig folyamatosan ülésezik az adatvédelmi tisztviselő által meghatározott rendszerességgel.
Az incidenskezelő csoport az adatvédelmi incidens kezelésének lezárásával szűnik meg, ideértve a NAIH esetleges eljárása keretében hozott döntéseket is.

Az incidenskezelő csoport tagjai:

a) az adatvédelmi tisztviselő;
b) megfelelési és szabályozási igazgató,
c) az érintett munkatárs és az adatkezelő szervezeti egység vezetője;
d) a Vezérigazgató vagy az általa megbízott személy,
e) amennyiben az adatvédelmi incidens olyan személyes adatot érint, amelynek kezelése során az adatkezelő szervezeti egység adatfeldolgozót vesz igénybe, úgy az adatfeldolgozó által kijelölt személy.

Az incidenskezelő csoport tagja lehet egyéb személy is szükség esetén.

*Az adatvédelmi incidens azonosítása az előzetes vizsgálat során:*
Az adatvédelmi tisztviselő az incidenskezelő csoport első ülésén ismerteti az lehetséges adatvédelmi incidenssel kapcsolatban rendelkezésre álló információkat, tényeket, különös tekintettel az adatvédelmi incidens bekövetkezésének körülményeire és az incidens kategorizálására.

Ezt követően az incidenskezelési csoport előzetes vizsgálatot folytat le annak érdekében, hogy megállapításra kerüljön, hogy az adatvédelmi incidens bizonyossággal bekövetkezett e. Az előzetes vizsgálatról feljegyzést kell készíteni, amelyben rögzíteni kell:

- az incidensre vonatkozó körülményeket (kitérve arra is, hogy az incidens érinti-e a DV Zrt. által alkalmazott bármely informatikai rendszert, illetve fennáll-e az esélye az

érintettek szélesebb körének személyes adatainak szivárgására, jogosulatlan személyek általi hozzáférésre),
- a vizsgálat időpontját,
- a vizsgálat helyét,
- a vizsgálatban résztvevő személyek nevét, munkakörét és
- annak megállapítását, hogy adatvédelmi incidens történt-e.

Az incidenskezelő csoport elvégzi az adatvédelmi incidens kockázatainak felmérését és elemzését, azok valószínűségének és súlyosságainak figyelembevételével. A kockázatok tekintetében azok forrását, a kiszolgáló környezetet, a személyes adatokat, illetve az incidens lehetséges hatásait kell vizsgálni.

A kockázatok forrása tekintetében figyelembe vehető tényezők:

a) az incidens véletlen belső magatartás vagy tevékenység eredménye;
**b) az incidens szándékos belső magatartás vagy tevékenység eredménye;**
**c) az incidens véletlen külső magatartás vagy tevékenység eredménye;**
**d) az incidens szándékos belső magatartás vagy tevékenység eredménye.**

A kiszolgáló környezet szempontjából figyelembe vehető tényezők:

a) az adatkezelés eszközei (papír alapú vagy automatizált módszerekkel történő adatkezelés);
b) az incidenssel érintett rendszer (levelező rendszer, adathordozó stb.);
c) a kiszolgáló környezet biztonságát védő intézkedések (pl. titkosítás, elnevesítés, tűzfal);
d) a kiszolgáló környezet ellenállóképessége;
e) az incidens elhárítása érdekében előzetes tett intézkedések hatékonysága;
f) az incidens bekövetkeztét lehetővé tevő tényezők;
g) az incidens bekövetkeztét befolyásoló egyéb tényezők;
h) a rendszerszerű működés helyreállításának valószínűsége.

A személyes adatok szempontjából figyelembe vehető tényezők:

**a) a személyes adatok kategóriái, különös tekintettel a különleges adatokra,**
b) a személyes adatok száma,
**c) az érintettek kategóriái, különös tekintettel az érintettek kiszolgáltatott helyzetére (az érintett gyermek, vagy munkavállaló)**
d) az érintettek azonosíthatósága,
**e) az érintettek száma.**

Az incidens várható hatásai szempontjából figyelembe vehető tényezők:

a) fizikai kár vagy veszély,
**b) vagyoni kár,**
c) nem vagyoni kár.

Az incidenskezelő csoport köteles az adatvédelmi incidenst egyedileg, kockázati szint szerint besorolni a következők szerint: alacsony kockázatú, (közepes)kockázattal járó vagy magas kockázatú incidens.

A fenti kategóriákban vastag betűvel jelölt esetek – ideértve az érintettek nagyobb számát is – közepes kockázatot, vagy magasabb kockázatot jelentenek.

Szintén valószínűsíthetően magasabb kockázattal jár az adatvédelmi incidens a természetes személyek jogaira és szabadságaira nézve, ha annak eredménye:

a) az érintett hátrányos megkülönböztetése;
b) személyazonosság-lopás;
c) személyazonossággal való visszaélés;
d) pénzügyi veszteség;
e) az érintett jó hírnevének sérelme;
f) a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülése;
g) álnevesítés engedély nélkül történő feloldása;
h) bármilyen egyéb jelentős gazdasági vagy szociális hátrány;
i) alapvető jogai vagy szabadságai gyakorlásának ellehetetlenülése;
j) az érintett saját személyes adatai feletti önrendelkezési jogának megszűnése;
k) személyes jellemzők értékelésére személyes profil létrehozása vagy felhasználása céljából.

Amennyiben az előzetes vizsgálat során megállapításra kerül, hogy nem következett be adatvédelmi incidens, a vizsgálat lezárható.
Amennyiben az adatvédelmi incidens bekövetkezett, de az alacsony kockázatú, úgy kell tekinteni, hogy az **valószínűsíthetően nem jár kockázattal** a természetes személyek jogaira és szabadságaira nézve. Ebben az esetben az adatvédelmi incidenst az adatvédelmi tisztviselő nyilvántartásba veszi, továbbá tájékoztatja a Vezérigazgatót. Amennyiben az adatvédelmi incidens olyan személyes adatokat érint, amelyeket a DV Zrt. adatfeldolgozóként kezel, úgy haladéktalanul értesíteni szükséges az e személyes adatok tekintetében adatkezelőnek minősülő szerződött partnert is.

Amennyiben az adatvédelmi incidens közepes kockázatú, úgy kell tekinteni, hogy az – a GDPR 33. cikk (1) bekezdése szerint – **valószínűsíthetően kockázattal** jár a természetes személyek jogaira és szabadságaira nézve.

Amennyiben az adatvédelmi incidens magas kockázatú, úgy kell tekinteni, hogy az – a GDPR 34. cikk (1) bekezdése szerint – **valószínűsíthetően magas kockázattal** jár a természetes személyek jogaira és szabadságaira nézve.

### 3.3.1 Az adatvédelmi incidenssel kapcsolatos intézkedési terv

Az incidenskezelési csoport az adatvédelmi incidens kivizsgálása során feltárt információk alapján meghatározza az adatvédelmi incidens következményeinek elhárításához vagy enyhítéséhez, valamint a további adatvédelmi incidens bekövetkezésének elkerüléséhez szükséges intézkedéseket, megjelölve az intézkedés végrehajtásáért felelős szervezeti egységet és a végrehajtás határidejét. Az intézkedési tervet az adatvédelmi tisztviselő útján jóváhagyásra meg kell küldeni a DV Zrt. Vezérigazgatójának.
Az intézkedési terv végrehajtásáért felelős szervezeti egység az intézkedési terv végrehajtására nyitva álló határidőt követő 15 napon belül írásos jelentést készít az intézkedési terv végrehajtásának eredményéről. A jelentést meg kell küldeni az adatvédelmi tisztviselő részére, aki azt véleményezésre megküldi az intézkedési terv készítésében részt vevő incidenskezelési csoport tagjai részére. Az intézkedési terv végrehajtásának eredményéről az adatvédelmi tisztviselő a jelentés kézhezvételét követő 15 napon belül beszámol a Vezérigazgatónak, amelyben ismertetni kell az incidenskezelési csoport tagjainak véleményét is.

### 3.3.2 Az adatvédelmi incidens bejelentése

Amennyiben az adatvédelmi incidens **valószínűsíthetően kockázattal jár** a természetes személyek jogaira és szabadságaira nézve, az adatvédelmi incidens nyilvántartásba vétele mellett a DV Zrt. köteles indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, bejelentést tenni a NAIH-hoz.
A bejelentési kötelezettség határideje az adatvédelmi incidensről való tudomásszerzéstől kezdődik. Tudomásszerzésnek az az időpont számít, amikor az DV Zrt., mint Adatkezelő ésszerű bizonyossággal rendelkezik arról, hogy olyan biztonsági esemény történt, amely adatvédelmi incidensnek tekintendő.
Amennyiben az adatvédelmi incidens körülményeinek feltárása, kockázatainak felmérése indokolttá teszi, a bejelentés részletekben is történhet.
A DV Zrt. nevében a bejelentési kötelezettséget az adatvédelmi tisztviselő teljesíti. Az adatvédelmi tisztviselő a bejelentési kötelezettségét papír alapon, vagy a NAIH honlapján a https://www.naih.hu/adatvedelmi-incidensbejelento-rendszer linken elérhető elektronikus bejelentési rendszer útján teljesíti.

A NAIH részére tett bejelentésnek tartalmaznia kell:

a) az Adatkezelő adatait;
b) az adatvédelmi incidens időpontját;
c) az adatvédelmi incidensről való tudomásszerzés időpontját;
d) az adatvédelmi incidens észlelésének módját;
e) esetleges késedelmes tájékoztatás indokait;
f) az adatvédelmi incidens jellegét;
g) az adatvédelmi incidenssel érintett személyes adatokat;
h) az adatvédelmi incidenssel érintett személyes adatok becsült számát;
i) az érintettek kategóriáit;
j) az adatvédelmi incidens előtt alkalmazott intézkedéseket;
k) az adatvédelmi incidens következményeinek a megjelölését;
l) az érintetteket ért fizikai, anyagi vagy nem vagyoni károkat, vagy egyéb jelentős következményeket, valamint a valószínűsíthető következmények súlyosságát;
m) a megtett intézkedéseket;
n) az adatvédelmi incidens orvoslására tett intézkedéseket;
o) egyéb bejelentéseket;
p) az adatvédelmi tisztviselő nevét és elérhetőségeit;

Az adatvédelmi tisztviselő köteles együttműködni a NAIH-hal az adatvédelmi incidensek kezelésével összefüggésben indult eljárások során.
Az adatvédelmi tisztviselő köteles a NAIH rendelkezésére bocsátani az adatvédelmi incidensek kezelésével összefüggésben indult eljárások lefolytatásához szükséges további információkat.
Annak érdekében, hogy az adatvédelmi tisztviselő teljesíteni tudja a fenti kötelezettségét, jogosult az Adatkezelővel munkaviszonyban, munkavégzésre irányuló egyéb jogviszonyban álló személytől, valamint az Adatkezelővel kötött szerződés alapján eljáró adatfeldolgozótól információt, tájékoztatást kérni.
Az incidenskezelő csoport tagjai kötelesek közreműködni az adatvédelmi tisztviselővel a fenti kötelezettség teljesítése során.

### 3.3.3 Az érintettek tájékoztatása

Amennyiben az adatvédelmi incidens **valószínűsíthetően magas kockázattal jár** a természetes személyek jogaira és szabadságaira nézve, az adatvédelmi incidens nyilvántartásba vétele, és a NAIH részére történő bejelentés mellett DV Zrt. köteles indokolatlan késedelem nélkül tájékoztatni az érintettet az adatvédelmi incidensről.
A tájékoztatási kötelezettséget a DV Zrt. nevében az adatvédelmi tisztviselő teljesíti.
Amennyiben – az érintettek nagy számára tekintettel – a személyes tájékoztatás lehetetlen lenne vagy aránytalan költséggel járna a DV Zrt.-re nézve, a tájékoztatás helyi vagy országos sajtótermékekben megjelentetett figyelemfelhívó jelzés útján is megadható. Ebben az esetben a DV Zrt. honlapján figyelemfelhívó jelzést kell elhelyezni, amely általános tájékoztatást nyújt az incidens jellegéről, az érintett személyes adatok, illetve az érintettek kategóriáról.

Az érintett vagy érintettek részére nyújtott tájékoztatásnak tartalmaznia kell legalább:

a) az adatvédelmi incidens jellegének leírását;
b) az adatvédelmi tisztviselő nevét és elérhetőségeit;
c) az adatvédelmi incidens valószínűsíthető következményeinek ismertetését;
d) az adatvédelmi incidens orvoslására tett vagy tervezett intézkedések ismertetését, beleértve adott esetben az incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket is;
e) az érintettek által az adatvédelmi incidens orvoslására tehető intézkedések ismertetését, beleértve adott esetben az incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket is.

Nem kell tájékoztatni az érintetteket, ha az alábbi feltételek bármelyike teljesül:

- a személyes adatok tárolása olyan titkosított módszerrel történt, amely miatt a személyes adatok harmadik személyek számára nem értelmezhetőek.
- a DV Zrt. az incidens bekövetkezése után olyan hatékony intézkedést tett az adatvédelmi incidens következményeinek elhárítására, amelyek eredményeként az érintett jogaira és szabadságaira jelentett magas kockázat a továbbiakban valószínűsíthetően nem valósul meg.
- aránytalan erőfeszítés lenne az érintettek közvetlen tájékoztatása. Ebben az esetben a DV Zrt. nyilvánosan közzétett közleményt adhat ki a bekövetkezett adatvédelmi incidensről.

Amennyiben az adatvédelmi incidensben az érintettekkel való kapcsolattartást lehetővé tevő csatorna érintett, úgy az érintettek tájékoztatására ez a csatorna nem alkalmazható. Amennyiben annak feltételei rendelkezésre állnak, az érintetteket az alábbi kommunikációs csatornákon lehet tájékoztatni:

- postai levélben,
- elektronikus levélben (e-mail),
- SMS-ben,
- a DV Zrt. honlapján,
- sajtóközleményben.

Az incidensről szóló tájékoztatás egyértelmű és átlátható jellegének biztosítása érdekében az nem küldhető ki más jellegű tájékoztatással együtt. A tájékoztatás az adatvédelmi tisztviselő véleményezése után a Vezérigazgató jóváhagyásával küldhető meg az érintett számára.

### 3.3.4 Korrekciós intézkedések

Az adatvédelmi tisztviselő az adatvédelmi incidens következményeként szükség esetén állásfoglalást ad ki arról, hogy az adatkezelő szervezeti egységeknek milyen további intézkedések megtételét javasolja az adatvédelmi incidensek megelőzése érdekében.

Ilyen intézkedés lehet:

- az adatkezelési folyamatra irányadó szabályozás felülvizsgálata, szükség szerinti módosítása, vagy annak hiányában szabályozás kialakítása,
- az adatkezelési folyamatra irányadó szabályozás betartásának fokozott ellenőrzése,
- képzések, oktatások szervezése, ideértve a múltban bekövetkezett adatvédelmi incidensek tapasztalatainak összegzését is.

Az adatvédelmi tisztviselő korrekciós intézkedésre vonatkozó állásfoglalását megküldi az adatkezelő szervezeti egység vezetőjének. A korrekciós intézkedés végrehajtásáról az adatkezelő szervezeti egység tájékoztatja az adatvédelmi tisztviselőt.

### 3.3.5 Az adatvédelmi incidens kezelésének lezárása

Az adatvédelmi tisztviselő az adatvédelmi incidens kezelésének folyamatát az intézkedési terv vagy – amennyiben korrekciós intézkedés megtételére került sor – a korrekciós intézkedés végrehajtásáról szóló tájékoztatás kézhezvételét követően lezárja és erről feljegyzést készít. Az adatvédelmi incidens kezelési folyamatának lezárásáról az adatvédelmi tisztviselő tájékoztatja a Vezérigazgatót.

### 3.3.6 Az adatkezelési incidensek nyilvántartása

A DV Zrt. köteles nyilvántartani az adatvédelmi incidenseket, tekintet nélkül azok kockázati besorolására. Az adatvédelmi incidensek nyilvántartásának tartalmát a DV Zrt. Adatvédelmi és Adatbiztonsági Szabályzatának 6. melléklete határozza meg.

A DV Zrt. nevében az adatvédelmi incidensek nyilvántartásának kötelezettségét az adatvédelmi tisztviselő teljesíti. Az adatvédelmi tisztviselő gondoskodik az adatvédelmi incidensek nyilvántartásának naprakészen tartásáról, frissítéséről.

Az adatvédelmi tisztviselő köteles a nyilvántartást a NAIH ez irányú kérésére rendelkezésre bocsátani.

## 4. ZÁRÓ RENDELKEZÉSEK

A Szabályzat a Vezérigazgató általi ellenjegyzés napján lép hatályba és visszavonásig érvényes.