SZIGETVÁRI TÁVHŐ
SZOLGÁLTATÓ NONPROFIT
KORLÁTOLT FELELŐSSÉGŰ TÁRSASÁG
7900 Szigetvár, Szent István lakótelep 7.

SZABÁLYZAT
AZ ADATVÉDELMI INCIDENSEK KEZELÉSÉRŐL

A **Szigetvári Távhő Szolgáltató Nonprofit Korlátolt Felelősségű Társaság (székhely: 7900 Szigetvár, Szent István lakótelep 7., cégjegyzékszám: Cg.02-09-076277)**, mint Adatkezelő az Európai Parlament és a Tanács (EU) 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 2016/679. rendelete (általános adatvédelmi rendelet, a továbbiakban: GDPR) szerinti kötelezettségeinek teljesítése érdekében minden lehetséges technikai és szervezési intézkedést megtesz, melyek alkalmasak arra, hogy az adatvédelmi incidensek bekövetkezését meggátolja, a kockázatok súlyosságát és valószínűségét a lehető legalacsonyabb szinten tartsa.

Ugyanakkor felelős adatkezelőként tisztában van azzal, hogy a bekövetkezett adatvédelmi incidens megfelelő és kellő idejű intézkedés hiányában fizikai, vagyoni vagy nem vagyoni károkat okozhat a természetes személyeknek, többek között személyes adataik feletti rendelkezés elvesztését vagy a jogaik korlátozását, hátrányos megkülönböztetést, pénzügyi veszteséget, jó hírnév sérelmét, a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülését, illetve az érintetteket sújtó egyéb jelentős gazdasági vagy szociális hátrányt.

E következmények megakadályozására és mérséklésére vonatkozó kötelezettségére tekintettel a Szigetvári Távhő Nonprofit Kft. az alábbi szabályzatot alkotja:

1.§ A szabályzat hatálya

A szabályzat hatálya kiterjed a **Szigetvári Távhő Szolgáltató Nonprofit Korlátolt Felelősségű Társaság (székhely: 7900 Szigetvár, Szent István lakótelep 7., cégjegyzékszám: Cg.02-09-076277)** által folytatott valamennyi adatkezelési tevékenységre, és minden munkavállalójára beleértve a munkavégzésre irányuló egyéb jogviszonyban foglalkoztatott személyeket is.

2.§ Fogalmak

Adatvédelmi incidens: a biztonság olyan sérülése, mely a kezelt személyes adatok véletlen, vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését, vagy az azokhoz való jogosulatlan hozzáférést eredményezi.

Bizalmasság: az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról.

Bizalmassággal kapcsolatos incidens: a személyes adatok jogosulatlan (felhatalmazás nélküli) közlése vagy az ezekhez való jogosulatlan hozzáférés.

Sértetlenség: az adat azon tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek.

Sértetlenséggel kapcsolatos incidens: a személyes adatok véletlen vagy jogtalan megváltoztatása.

Rendelkezésre állás: annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek.

Rendelkezésre állással kapcsolatos incidens: személyes adatok véletlen vagy jogtalan megsemmisítése vagy ezek elvesztése.

Kockázat: az adatvédelmi incidens hatásainak súlya és bekövetkezésük valószínűsége.

3.§ Adatvédelmi incidens észlelése és jelentése

(1) Az Adatkezelő minden munkavállalója – beleértve az munkavégzésre irányuló egyéb jogviszonyban foglalkoztatott személyeket is – köteles az adatvédelmi incidenst a tudomására jutást követően haladéktalanul jelenteni a közvetlen munkahelyi vezetőjének, aki a bejelentést köteles haladéktalanul továbbítani az ügyvezetőnek, távolléte esetén a helyettesítésére kijelölt vezetőnek. A bejelentés tartalmazza a bejelentő nevét, beosztását, szervezeti egységének megnevezését, valamint az incidens tárgyát, rövid leírását.

(2) Az ügyvezető a bejelentés kézhezvételét követő lehető legrövidebb időn belül, legkésőbb 24 órán belüli időpontra összehívja az Incidenskezelő munkacsoportot, melynek állandó tagjai: ügyvezető, informatikai vezető, az adatvédelmi tisztviselő, szükség szerinti tagok: az érintett szervezeti egység vezetője, a bejelentő, az adatfeldolgozó, továbbá mindazon személyek, akik az incidens körülményeinek feltárásában, következményeinek enyhítésében közreműködhetnek.

(3) Amennyiben az Incidenskezelő munkacsoport a fenti határidőre nem hívható össze, úgy az egyeztetést e-mailen, vagy telefonon kell lefolytatni.

(4) Az Incidenskezelő csoport egyeztetéséről emlékeztetőt kell felvenni, mely tartalmazza az az incidens leírását, az egyeztetés eredményét, és amennyiben véleményeltérés van, úgy annak rövid összefoglalását.

4.§ Adatvédelmi incidens kivizsgálása, értékelése

(1) Az Incidenskezelő csoport megvizsgálja a bejelentést és feltárja az adatvédelmi incidens bekövetkezésének időpontját, helyét, az adatvédelmi incidens egyéb körülményeit, az adatvédelmi incidens által érintett adatok körét, mennyiségét, az adatvédelmi incidenssel érintett személyek körét és számát, az adatvédelmi incidens várható hatásait, az adatvédelmi incidens megelőzésére, következményeinek enyhítésére megtett és megtehető intézkedéseket.

(2) A vizsgálatnak ki kell terjednie arra, hogy az adatvédelmi incidens milyen szintű kockázattal jár az érintettek jogaira és kötelezettségeire, milyen jellegű kockázatról van szó és szükséges-e a Hatóság, és/vagy az érintettek tájékoztatása az incidensről. Amennyiben a tájékoztatás nem szükséges, úgy a vizsgálatnak tartalmazni kell ennek indokait is. A kockázatértékelés módszertanát jelen szabályzat **1. sz. melléklete** tartalmazza.

(3) A vizsgálatot legkésőbb az incidensről való tudomásszerzést követő 72 órán belül be kell fejezni.

(4) A vizsgálat eredményei alapján az adatvédelmi tisztviselő javaslatot tesz az ügyvezetőnek az incidenskezeléshez szükséges intézkedések megtételére.

(5) A megvalósítandó további intézkedésekről a vizsgálat alapján feltárt tények, a kockázatértékelés eredményei és az adatvédelmi tisztviselő javaslata alapján az ügyvezető dönt.

5.§ Az adatvédelmi incidens nyilvántartása

(1) Az adatvédelmi incidensekről – függetlenül azok súlyától - az Adatkezelő nyilvántartást vezet, melynek mellékletét képezik a feltárt incidensekről felvett egyedi nyilvántartó lapok.

(2) Az adatvédelmi nyilvántartás mintáját a jelen szabályzat **2. számú melléklet** az egyedi nyilvántartó lapok mintáját a **3. számú melléklet** tartalmazza.

6.§ Az adatvédelmi incidens bejelentése a Hatóság részére

(1) Az Adatkezelő adatvédelmi tisztviselője az adatvédelmi incidenst az Adatkezelő tudomására jutását követően haladéktalanul, de legkésőbb 72 órán belül bejelenti a Hatóság részére, kivéve, ha az incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve.

(2) Az adatvédelmi tisztviselő a felügyeleti hatóság által erre a célra rendszeresített elektronikus felületen teszi meg a bejelentést.

(3) A Hatósági bejelentésnek tartalmaznia kell:
- az adatvédelmi incidenssel érintett adatok körét és hozzávetőleges számát,
- az adatvédelmi incidenssel érintett személyek körét és hozzávetőleges számát,
- az adatvédelmi incidens jellegét, körülményeit,

- az adatvédelmi incidens valószínűsíthető következményeit és
- az adatvédelmi incidens orvoslására és enyhítésére megtett intézkedéseket
- továbbá minden egyéb szükséges információt.

(4) A bejelentés megtételével kapcsolatban az adatvédelmi tisztviselő nem utasítható.

7.§ Az érintettek tájékoztatása adatvédelmi incidensről

(1) Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságára nézve és az érintettek tájékoztatása szükséges, az Adatkezelő haladéktalanul értesíti az érintetteket. Az érintettek tájékoztatása független a Hatóság felé irányuló tájékoztatási kötelezettségtől.

(2) Nem kell az érintetteket tájékoztatni:
- ha az Adatkezelő olyan technikai, szervezési, védelmi intézkedéseket hajtott végre az érintett adatokra vonatkozóan, amelyek megakadályozzák az illetéktelen személyek számára való hozzáférést az adatokhoz vagy megakadályozzák az adatok értelmezhetőségét;
- ha az adatvédelmi incidens bekövetkezését követően az Adatkezelő olyan intézkedéseket tett, amelyek biztosítják, hogy a feltárt adatkezelési kockázat valószínűsíthetően nem valósul meg;
- ha a tájékoztatás aránytalan erőfeszítést tenne szükségessé. Ebben az esetben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, mely tájékoztatás elektronikus úton is megtörténhet.

8.§ Rendszeres tréningek

Az Adatkezelő jelen szabályzattal kötelezettséget vállal az adatvédelmi tudatosság növelése céljából adatvédelmi incidensekkel kapcsolatos legalább évenként egyszeri munkavállalói oktatásra, mely során a múltban bekövetkezett adatvédelmi incidensek tapasztalatait, vagy a lehetséges adatvédelmi incidensek veszélyeit ismerteti, elemzi, a kockázatok csökkentésével, megelőzésével kapcsolatosan tájékoztatást ad, illetve az ismereteket ellenőrzi.

1. számú melléklet: A kockázatértékelés módszertana

Az incidensről való tudomásszerzést követően – természetesen az elhárítás érdekében tett azonnali intézkedések mellett – az adatkezelőnek haladéktalanul értékelnie kell az incidens által jelentett kockázatot, hiszen 72 óra áll rendelkezésére ahhoz, hogy döntsön a szükséges bejelentési, és értesítési kötelezettségről. Az azonnali kockázatértékelés segít az adatkezelőnek abban is, hogy megfelelő védelmi intézkedéseket tegyen az incidens hatásainak enyhítésére.

Az incidensek kockázatértékelése során a következő tényezőket kell figyelembe venni:

- Egyfelől az incidens típusát - hiszen például más kockázata van az okos mérő által rögzített adat véletlen megsemmisülésének, és azok illetéktelen személyek általi megszerzésének – másfelől a személyes adatok köre, jellege és mennyisége határozza meg az incidens által jelentett kockázat mértékét.
- Az adatok köre, érzékenysége, mennyisége szintén meghatározó tényező. Általában véve minél érzékenyebb adatok az incidens tárgyai, az annál nagyobb kárt okozhat. Ugyanakkor figyelembe kell venni azt is, hogy az érintettről milyen egyéb adat áll rendelkezésre, hiszen bizonyos adatok csak az érintettről már meglévő más adatokkal kontextusban jelenthetnek hátrányos következményt rejtő kockázatot.
- Az érintettek azonosíthatósága kiemelt jelentőségű tényező, mely kapcsolódik az incidens által érintett adatok köréhez.
- A következmények súlyossága, mely nyilvánvalóan az incidens kockázatának legfontosabb faktora, lényegében a többi tényező eredője. Meghatározásánál a GDPR (75) preambulum-bekezdésében található károk – fizikai, vagyoni, nem vagyoni károk, jó hírnév sérelme stb. - bekövetkezésének lehetőségeit kell felmérni. A következmények tekintetében jelentősége van annak is, hogy azok milyen hosszan állnak fenn, egyszeri hatásnak vagy állapotnak tekinthetők.
- Az érintettek köre befolyásolhatja az incidens súlyát, ha például a tárgyát képező adatok esetleg gyermekekre, vagy olyan személyekre vonatkoznak, akik számára jogaik gyakorlása akadályba ütközik.
- Az adatkezelő jellemzői szintén meghatározhatják a következmények lehetséges súlyát, bár ez nyilván összefügg azzal, hogy az adatkezelők általában a tevékenységükkel összefüggő adatokat kezelik, így lényegében az adatkezelő jellemzői részben meghatározzák az adatok körét és az érintettek lehetséges kategóriáit.
- Az érintettek száma jelenős a következmények szempontjából, hiszen multiplikálja a következményeket.

A fenti tényezők figyelembevételével kell értékelni az incidenst, a következményeknek az egyén jogaira és szabadságaira jelentett hatás súlya és e következmény valószínűsége alapján

A kockázatértékelés folyamata

Az Adatkezelő az Európai Unió Hálózati és Információs Biztonsági Ügynöksége (ENISA) által megfogalmazott módszertant követi az incidensek kockázatainak értékelésekor, melynek eredeti – angol

nyelvű – szövege az irányadó abban az esetben, ha a jelen szabályzatban foglalt fogalmak jelentésével, alkalmazhatóságával kapcsolatban kétely merül fel.[1]

Az incidens kockázatának súlya három szempont összefüggéséből származtatható:

Adatkezelési sajátosságok (A), ideértve az incidens által érintett adatok kategóriáit, és az adatkezelés általános jellemzőit. Ez a módszertan központi eleme, mert a személyes adatokat meghatározott adatkezelési környezetben értékeli.

Azonosíthatóság (B): Meghatározza, hogy az egyén személyazonossága milyen könnyen állapítható meg az incidenssel érintett adatokból. Ez az adatkezelés jellemzőinek korrekciós tényezője, bármilyen súlyú is az előbbi, az azonosíthatóság mértéke képes a kockázat mértékét megváltoztatni.

Az incidens körülményei (C), melynek körében értékelni kell az incidens típusát, annak esetleg súlyosító és enyhítő tényezőivel együtt. Amennyiben e körülmények fennállására derül fény az incidens értékelése során, a megfelelő értékkel növelni kell az előző összefüggés eredményét.
A fenti három tényező összefüggése matematikai képlettel kifejezve:

Az incidens kockázatának mértéke= AxB+C

A fenti képletbe történő behelyettesítéshez mindhárom fenti tényezőt számszerűsíteni kell, azt követően a végeredmény ezúttal is négyfokú skálán helyezhető el: alacsony, közepes, magas és nagyon magas kockázati besorolással

A kritériumok pontozása a következőképpen történik:

A) Adatkezelési sajátosságok
Az Adatkezelési sajátosságok pontszámának meghatározásához első lépésként az alábbi táblázat segítségével meg kell határozni a személyes adatok típusait, majd be kell sorolnia a következő négy kategória közül legalább egybe: alapadat, viselkedésre vonatkozó, pénzügyi és érzékeny adat.
Második lépésként kell figyelembe venni az adatkezeléssel összefüggő tényezőket, melyek módosíthatják az előző értéket (adatok mennyisége, pontossága, esetleg nyilvános hozzáférhetősége stb.) E tényezők növelhetik vagy csökkenthetik az alap pontszámot, oly módon, hogy a végeredmény minden esetben 1-4 pontos osztályozási rendszerben helyezkedik el. (1. sz. táblázat)

Ha az adatok egynél több kategóriába is sorolhatók, úgy a fenti lépéseket minden kategóriára el kell végezni, és a legmagasabb kapott érték lesz az irányadó a végeredmény számításánál.

sorszám	adatkategóriák	pontszám	gyakorlati példa

[1] Recommendations for a methodology of the assessment of severity of personal data breaches https://www.enisa.europa.eu/publications/dbn-severity

I.	**Egyszerű személyes adatok**		
I/1.	Egyszerű személyes adatok, pl. név, cím, születési adatok, képzettség, szakmai tapasztalat.	1 (alapérték)	egy futárszolgálat adott napi címzettjeinek neve és telefonszáma
I/2.	Ha az egyszerű adatok mennyisége és / vagy az adatkezelő jellemzői olyanok, hogy lehetővé teszik az érintettre vonatkozó profilalkotást, társadalmi-pénzügyi státuszára vonatkozó következtetések levonását	2	egy luxusórákat forgalmazó kereskedő vevőinek neve és telefonszáma
I/3.	Ha az egyszerű adatok mennyisége, természete és / vagy az adatkezelő jellemzői olyanok, hogy lehetővé teszik az érintett egészségi állapotával, szexuális preferenciáival, politikai vagy vallási meggyőződésével kapcsolatos következtetések levonását.	3	cukorbetegeknek szánt készítményeket forgalmazó üzlet vevőinek neve és telefonszáma
I/4.	Ha az egyszerű adatok olyan érintettekre vonatkoznak, amelyek bizonyos jellemzői (például hátrányos helyzetű csoportok, kiskorúak) miatt az információ kritikus lehet személyes biztonságuk vagy fizikai / pszichológiai körülményeik szempontjából.	4	örökbefogadott gyermekek neve és telefonszáma
II.	**Viselkedésre vonatkozó adatok**		
II/1.	Viselkedésre vonatkozó adatok, pl. helymeghatározási adatok, személyes preferenciákra, szokásokra vonatkozó adatok.	2 (alapérték)	közösségi médiában az érintett által csak az ismerősi köre részére megjelenített információ
II/2.	Ha a viselkedésre vonatkozó adat nem nyújt tényleges, lényegi betekintést az érintett viselkedésébe, vagy egyébként az adatok – az incidenstől függetlenül - nyilvános forrásból is könnyen hozzáférhetők	1	közösségi médiában az érintett által bárki számára hozzáférhetően közzétett adat
II/3.	Ha a viselkedésre vonatkozó adatok mennyisége, vagy az adatkezelő jellemzői alapján az érintett olyan profilja alkotható meg, mely tájékoztatást ad a mindennapi életvitelről, szokásokról.	3	közösségi médiában az érintett által csak az ismerősi köre részére az elmúlt egy évi tevékenységére, preferenciáira vonatkozóan megjelenített információ
II/4.	Ha a viselkedésre vonatkozó adatok az érintett szenzitív tulajdonságai szerinti profil megalkotását is lehetővé teszi	4	közösségi médiában folytatott kommunikáció (pl. üzenetváltás, komment)

			mely információt ad az érintett betegségéről
III	**Pénzügyi, vagyoni adatok**		
III/1.	Bármilyen pénzügyi adat (pl. bevétel, jövedelem, pénzügyi tranzakciók, bankszámlakivonatok, befektetések, hitelkártyák, számlák stb.), ideértve a pénzügyi információkon alapuló szociális jóléti adatokat, és a vagyoni helyzetet.	3 (alapérték)	banki egyenlegközlő, melyből az érintett havi számlaegyenlege megállapítható
III/2.	Ha a pénzügyi adat nem nyújt tényleges, lényegi betekintést az érintett pénzügyi, vagyoni helyzetébe	1	egy banki levélen szereplő adatokból mindössze annyi információ származik, hogy az érintett az adott bank ügyfele
III/3.	Ha a pénzügyi adatállomány konkrét pénzügyi információt tartalmaz, de az még mindig nem tesz lehetővé tényleges, lényegi betekintést az érintett pénzügyi helyzetére (pl. egyszerű bankszámlák további részletek nélkül).	2	egy banki levélen szereplő adatokból az érintett egy napi tranzakciói látszanak annak részletei nélkül (név, számlaszám, összegek)
III/4.	Ha a pénzügyi adatállomány jellegéből és / vagy mennyiségéből adódóan teljes pénzügyi (pl. hitelkártya) információ biztonsága sérül, amely az érintett sérelmére csalást eredményezhet, vagy alkalmas a részletes társadalmi / pénzügyi profiljának megalkotására.	4	banki egyenlegközlő, melyből az érintett egy évi egyenlegei és tranzakcióinak részletes története megállapítható
IV.	**Érzékeny (különleges) adatok**		
IV/1.	Bármilyen érzékeny adat (pl. egészségi állapot, politikai hovatartozás, vallás, szexuális élet)	4 (alapérték)	egy laborlelet, mely tartalmazza az érintett vérvizsgálatának eredményét
IV/2.	Ha az érzékeny adat jellege nem nyújt tényleges, lényegi betekintést az érintett viselkedésébe, vagy egyébként az adatok – az incidenstől függetlenül - nyilvános forrásból is könnyen hozzáférhetők.	1	egy laborjelentés, mely szerint az érintett komplex vérvizsgálaton vett részt
IV/3.	Ha az érzékeny adat természete általános feltételezést tesz lehetővé	2	a kórház sürgősségi osztályának irata arról, hogy az érintett vérvizsgálaton vett részt
IV/4.	Ha az érzékeny adat természete érzékeny információkra vonatkozó feltételezést tesz lehetővé	3	egy laborjelentés, mely szerint az érintett meghatározott betegség szűrésére vonatkozóan vérvizsgálaton vett részt

V.	**Azonosítók** (az alábbiak jellemző példák, az adott azonosító kompromittálódása miatti incidens súlya az azonosítóval védett információ jellegétől függ, és az I-IV. szerint besorolandó)		
V/1.	Egyszerű adattal összefüggő azonosító	1	elektronikus zenei áruház (pl. Spotify) fiókhoz tartozó felhasználói név és jelszó
V/2.	Viselkedési adattal összefüggő azonosító	3	közösségi média profil felhasználói neve és jelszava
V/3.	Pénzügyi adattal összefüggő azonosító	4	pénzügyi utalást lehetővé tevő elektronikus banki felhasználói név és jelszó
V/4.	Különleges adattal összefüggő azonosító	4	az érintett betegségével kapcsolatos online közösségi fórum felhasználói fiókjának azonosítói

B) Az azonosíthatóság meghatározása

Az azonosíthatóság meghatározása szintén négyfokú skálán történik, és az értékek az adatkezelési sajátosságok pontszámának szorzótényezői lesznek a kockázatértékelésnél.
A legalacsonyabb pontszám (0,25) akkor alkalmazható, ha az egyén azonosításának lehetősége elhanyagolható, vagyis rendkívül nehéz, a legmagasabb pontszám (1) akkor, ha az azonosítás minden további ráfordítás nélkül, pusztán az adatokból lehetséges. (2. sz. táblázat)

azonosíthatóság foka	**érték**	**gyakorlati példa 1. (fénykép)**	**gyakorlati példa 2. (e-mail cím)**
elhanyagolható	0,25	homályos, távoli fényképfelvétel az érintettről	az e-mail cím nem tartalmaz azonosításra alkalmas információt (pl. nevet), és nem azonosítható az interneten (pl. nem szolgál elsődleges belépési e-mail címnek bármely - pl. facebook - profilhoz)
korlátozott	0,5	homályos távoli fényképfelvétel az érintettről a gépkocsijában ülve	
jelentős	0,75	éles fényképfelvétel az érintettről	az e-mail cím nem tartalmaz azonosításra alkalmas információt (pl.nevet), de azonosítható az interneten (pl. elsődleges belépési e-mail címként szolgál az érintett facebook profiljához)

maximális	1	éles fényképfelvétel az érintettről a gépkocsijában ülve	az e-mail cím tartalmaz azonosításra alkalmas információt (pl. nevet), és azonosítható is az interneten (pl. elsődleges belépési e-mail címként szolgál az érintett facebook

C) Az incidens körülményeinek értékelése

Az incidens körülményeit is négy kategória szerint lehet csoportosítani: bizalmassággal, sértetlenséggel, rendelkezésre állással kapcsolatos incidensek, illetve ezen objektív besoroláson kívül itt értékelni kell azt is, hogy az előző három biztonsági kategóriát érintő incidens véletlen, vagy más személy rosszindulatú szándéka idézte-e elő. Ez utóbbinak a külön értékelésére azért kell sort keríteni, mert a rossz szándék olyan tényező, amely valószínűvé teszi az adatok jogellenes felhasználását is – amennyiben ez tehát megállapítható, úgy az incidens jellege mellett mindenképpen további 0,5 ponttal növeli az értéket.
Fontos rögzíteni, hogy C érték meghatározásánál – az A és B értékkel szemben, ahol mindig a maximális pontszámot kell választani - az egyes C értékeket – amennyiben több is felmerül adott incidens kapcsán – egytől-egyig pontokat hozzáadjuk a végső pontszám eléréséhez.

	érték	**leírás**	**gyakorlati példa**
Bizalmassággal kapcsolatos incidens	+0	bizalmasság feltételezett sérülése, jogellenes adatkezelésre utaló bizonyíték nélkül	akta elveszik költözés közben
	+0,25	bizalmasság bizonyítottan sérül, de az adat korlátozott körben válik ismertté	személyes adatot tartalmazó e-mail téves megküldése meghatározott számú ismert címzettnek
	+0,5	bizalmasság bizonyítottan sérül, és az adat nem meghatározható körben válik ismertté	személye adatot tartalmazó dokumentumot feltöltik egy korlátlan hozzáférésű internetes felületre
Sértetlenséggel kapcsolatos incidens	+0	az adat változott, de nem azonosítható pontatlanságot, vagy jogellenességet eredményező használat	az adatbázis frissítése hibás volt, de a hibás adatok felhasználását megelőzően az eredeti adatállomány helyreállítható volt
	+0,25	a megváltozott adatot valószínűleg pontatlan, vagy jogellenes helyzetet eredményező módon felhasználták, de az eredeti adat helyreállítható	pl. online egészségügyi szolgáltatás igénybevétele során a felvett adatot (pl. eredményt) megváltoztatják, így az érintett egészségügyi profilja pontatlan, de az ismételt vizsgálat alapján a pontos tartalom helyreállítható

	+0,5	a megváltozott adatot valószínűleg pontatlan, vagy jogellenes helyzetet eredményező módon felhasználták, és az eredeti adat nem állítható helyre	az előbbi példa, kiegészítve azzal, hogy az eredeti adat nem helyreállítható.
Rendelkezésre állással kapcsolatos incidens	+0	az elveszett adatok minden nehézség nélkül helyreállíthatók	az adatokról van biztonsági mentés, vagy másik adatbázisból nehézség nélkül helyreállíthatók
	+0,25	az ideiglenesen elveszett adatok helyreállíthatók, de erőfeszítéseket kell tenni ennek érdekében	az elveszett adatot ismételten elektronikus formában kell felvenni, vagy az érintettet ismételten meg kell keresni az adat felvétele érdekében
	+0,5	az adatok véglegesen elvesztek, és nincs lehetőség a helyreállításra	az elveszett adat semmilyen módon nem állítható helyre
Rosszindulatú, szándékos támadás	+0,5	az incidens rosszindulatú külső vagy belő támadás eredménye	zsarolóvírus titkosítja az adatokat

Fontos rögzíteni, hogy C érték meghatározásánál – az A és B értékkel szemben, ahol mindig a maximális pontszámot kell választani - az egyes C értékeket – amennyiben több is felmerül adott incidens kapcsán – egytől-egyig pontokat hozzáadjuk a végső pontszám eléréséhez. (pl. ha az adatok végleg törlődnek: az érték 0,5, ha zsarolóvírus miatt törlődnek, akkor további +0,5, vagyis összesen +1, ha a zsaroló az adatokat nyilvánosságra is hozza, akkor további +0,5 értéket kell hozzáadni, így az incidens kockázatértékelésénél mindösszesen +1,5.) Az e tényezőkre kapott 0, 0,25, 0,5 pontokat az adatkezelési sajátosságok és az azonosíthatóság pontszámainak szorzatához kell hozzáadni, és így alakul ki a képlet szerinti végső eredmény.

A kockázat értékelése a kapott értékek alapján

Az A, B, C értékeket a képletbe helyettesítve számszerűsíthető az incidens kockázata az alábbi skála szerint: Amennyiben a kapott érték kevesebb 2-nél, úgy az incidens kockázata **alacsony**, az érintettek legfeljebb kisebb kellemetlenségekre számíthatnak.

Ha az érték 2, vagy nagyobb, de kevesebb 3-nál, úgy az incidens **közepes** kockázatú, ekkor az érintettek jelentős nehézségeket tapasztalhatnak, de azokat viszonylag könnyen képesek leküzdeni.

Ha a kapott érték 3, vagy nagyobb, de kevesebb 4-nél, úgy az incidens **magas** kockázatú és az érintettek számára jelentős következményekkel járhat, amelyet komoly nehézségek árán lehet megoldani.

A 4, vagy annál nagyobb értéket kapó **maximális** kockázatú besorolás esetén az egyén akár visszafordíthatatlan következményekkel is szembesülhet.

INCIDENS SZÁMA: **[PL. 1/2020]**

INCIDENS NYILVÁNTARTÓ LAP

1. Az adatvédelmi incidens időpontja

Az adatvédelmi incidens tudomására jutásának időpontja:
Az adatvédelmi incidens elhárítása érdekében tett tevékenység időpontja: [-tól-ig]
Az adatvédelmi incidens időpontja:

2. Érintett személyes adatok köre

...

3. Az incidenssel érintettek köre és száma

...

4. Az adatvédelmi incidens körülményei leírása

...

5. Az adatvédelmi incidens hatásai

...

6. Hatások

...

7. Az elhárításra megtett intézkedések leírása

...

8. A kockázat szintje

...

9. Hatóság tájékoztatása megvalósult-e *(amennyiben igen, annak időpontja és módja; amennyiben nem, ennek oka)*

...

10. Érintettek tájékoztatása megvalósult-e *(amennyiben igen, annak időpontja és módja; amennyiben nem, ennek oka)*

...

Helyszín, dátum

.....

SZIGETVÁRI TÁVHŐ
SZOLGÁLTATÓ NONPROFIT
KORLÁTOLT FELELŐSSÉGŰ TÁRSASÁG
7900 Szigetvár, Szent István lakótelep 7.

ADATVÉDELMI INCIDENSEK NYILVÁNTARTÁSA

2020-as év

	Incidens időpontja	Adatkezelő tudomásszerzése	Bejelentés időpontja a NAIH-hoz:	Érintettek tájékoztatásának időpontja,	Az incidenssel érintett szervezeti egység:	Az érintett személyes adatok köre	Az adatvédelmi incidenssel érintettek köre és száma	Nyilvántartó lap sorszáma	Egyéb megjegyzés:
1.									
2.									
3.									
4.									
5.									
6.									
7.									
8.									
9.									
10.									
11.									
12.									
13.									
14.									
15.									
16.									
17.									
18.									
19.									
20									
21.									
22.									
23.									