Szent-Györgyi Albert Agóra

A SZEMÉLYES ADATOKRA VONATKOZÓ ADATVÉDELMI NYILVÁNOS SZABÁLYZAT

V 1.

Az EURÓPAI PARLAMENT ÉS A TANÁCS 2016. április 27-i (EU) 2016/679 RENDELETE (továbbiakban: GDPR) előírásainak alkalmazása céljából

v1. 2022. május

Dokumentum változáskövetés

Dátum	Verzió	A változás oka	A szerkesztést elvégezte
2022. május hó	V1.	Az EU Parlament és Tanács 2016/679. számú Rendelete (GDPR) és a 2011. évi CXII. törvénynek megfelelőség	RITEK Zrt.

Tartalom

I. A Szabályzat célja és hatálya.

1. **A Szabályzat célja**, hogy eleget tegyen a **Szent-Györgyi Albert Agóra** (továbbiakban: Adatkezelő) általi személyes adatok kezelése során irányadó adatvédelmi, adatkezelési és adatbiztonsági előírások meghatározása, a tevékenysége során a személyes adatok védelméhez fűződő jog érvényesülésének biztosítása.

2. **Adatkezelő megnevezése, elérhetősége:** Szent-Györgyi Albert Agóra (továbbiakban: Adatkezelő), székhelye: 6722 Szeged, Kálvária sugárút 23., E-mail címe: kapcsolat@agoraszeged.hu, telefonszáma: +36 62 563 480

3. **Az Adatkezelő területi hatálya kiterjed a mindenkor hatályos és az Alapító Okiratban szereplő központra és részlegekre, telephelyekre.**

Petőfi Sándor Művelődési Ház	6791 Szeged, Negyvennyolcas u. 12.
Heller Ödön Művelődési Ház	6753 Szeged-Tápé, Budai Nagy Antal u. 20.
Kecskési Művelődési Ház	6725 Szeged, Újvidéki u. 4/A.
Bálint Sándor Művelődési Ház	6726 Szeged, Temesvári krt. 42.
Móricz Zsigmond Művelődési Ház	6710 Szeged, Kapisztrán J. u. 52.
Tömörkény István Művelődési Ház	6771 Szeged-Szőreg, Magyar u. 16.
Petőfi-telepi Művelődési Ház	6727 Szeged, Szántó Kovács János u. 28.

4. **Az adatkezelés célja:** a szabadidő eltöltését célzó szolgáltatás megrendelésének előkészítése, abban való részvétel, a muzeális intézményekről, a nyilvános könyvtári ellátásról és a közművelődésről szóló 1997. évi CXL. törvényben foglalt lehetőségek biztosítása.

5. **Adatvédelmi tisztviselő neve, elérhetősége:** RITEK Zrt., székhelye: 6724 Szeged, Huszár utca 1., e-mail címe: dpo@ritek.hu, telefonszáma: +36 62 421-247.

6. **A Szabályzat 2022. június 01. napján lép hatályba.**

7. **A Szabályzat alanyi hatálya vonatkozik**
   a) a foglalkoztatásában, megbízásában álló természetes személyre,
   b) az adatfeldolgozókra, továbbá
   c) az Adatkezelő szolgáltatásában érintettre, aki különösen – de nem kizárólagosan – lehet
      - 18 év alatti fiatal, gyermek,
      - a szülői felügyeletet gyakorló szülő által megbízott személy,
      - felnőtt ügyfél, látogató,
      - jogi személy kapcsolattartója,

- szerződő ügyfél,
- rendezvényeken fellépő, szereplő személy,

d) adatfeldolgozóra

8. A **Szabályzat tartalma nyilvános.**

II. Az adatkezelés elvei

1. A törvényesség elve alapján: a személyes adatok kezelését jogszerűen, tisztességesen és átlátható módon kell végezni.

2. A célhoz kötöttség elve alapján:

   a) a foglalkoztatottak kizárólag a munkaköri leírásukban meghatározott feladataik ellátása céljából, a részükre biztosított jogosultságok rendeltetésszerű használatával kezelhetnek személyes adatot;
   b) a konkrét, vagy az érintett által adott hozzájárulásban megfogalmazott célhoz nem köthető adatkezelés tilos;
   c) amennyiben az adatkezelés célja teljesült vagy megszűnt, az adatkezelésre irányadó jogszabályban meghatározott tárolási határidőt követően az adatot elektronikusan törölni, a papíralapú adathordozót pedig selejtezni kell.

3. A pontosság és korlátozott tárolhatóság elve alapján:
   a) amennyiben a foglalkoztatott tudomást szerez arról, hogy az általa kezelt személyes adat hibás, hiányos, vagy időszerűtlen, köteles azt helyesbíteni, vagy az adat helyesbítését az adat rögzítéséért felelős munkatársnál kezdeményezni, és erről mindazokat értesíteni, akiknek az adat továbbításra került;

   b) a tárolásnak olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adat kezelése céljának eléréséhez szükséges ideig teszi lehetővé.

4. Az integritás és bizalmi jelleg elve alapján az adat kezelése során 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).

5. Az adattakarékosság elve alapján: az Adatkezelő kizárólag annyi és olyan személyes adatot kezelhet, amely az érintett egyértelmű azonosításához és ügyének elintézéséhez minimálisan szüksége és arra alkalmas.

III. Az Adatkezelő nyilvántartásában levő, működésével kapcsolatos különleges adatok és azok továbbítása

1. az érintett gyerek neve, neme, TAJ száma, állampolgársága, tartózkodási helye, állandó lakcíme, anyja neve, apja neve, születési helye, születési ideje, egészségügyi adatai (étel allergia, emésztési rendellenesség, allergia, tartós betegség),

2. a szülői felügyelet gyakorlására jogosult személy / törvényes képviselő adatai: neve, munkahelye, személyi igazolvány száma, elektronikus levélcíme, telefonszáma, bankszámla száma, IP-címe,

3. fiatal- és nagykorú ügyfél, látogató, web oldal látogató, regisztráló neve, elektronikus levélcíme, telefonszáma, IP-címe

4. az Adatkezelő munkavállalói, közalkalmazottai, közfoglalkoztatottai esetében, születési idő, születési ország, állampolgárság, édesanyja neve, személyi ig. szám, adott esetben gépjármű törzskönyv másolat és gépjármű forgalmi engedély másolat, bankszámlaszám, a társadalombiztosítási azonosító jel, adóazonosító szám, családi adókedvezményhez szükséges adatok, magán-nyugdíjpénztár neve, állandó lakcím, tartózkodási hely, e-mail cím, telefonszám

5. **A GDPR 4. cikk 10. pont szerinti harmadik fél részére történő adat átadás lehetséges**:

Központi, regionális szervezet neve:	**Elérhetőségek**	**Szervezet feladatai**
Nemzeti Adó- és Vámhivatal	telefonszáma: +36-1-250-9500, e-mail: nav.gov.hu/nav/e-ugyfsz/levelkuldes, honlap: https://nav.gov.hu/nav/kapcsolat	adózás és más befizetési kötelezettség nyilvántartása
OTP Mobil Kft. (Kizárólag a szolgáltatás ellenértékének a pénzügyi teljesítése, a SimplePay Interneten keresztüli online kártyás fizetési szolgáltatás elérése esetén)	Központi e-mail: ugyfelszolgalat@otpmobil.com, Telefonszám: +36-1-776-6901	az elektronikus fizetés lebonyolítása; a személyes adatokra a bankszámla terhelés és jóváírás céljából van szükség
Szegedi Tudományegyetem Juhász Gyula Pedagógusképző Kar	6725 Szeged, Boldogasszony sgt. 6., telefonszám: +36 62 546-051, http://www.jgypk.u-szeged.hu/kereses?searchStr=szakmai+gyakorlat&go=Keres	az oktatás érdekében szükséges és a szakmai gyakorlattal kapcsolatos adatkezelés

Webgalamb, E.N.S. Zrt.	dr. Koppány Julianna COO, Nádasdy-Nagy Balázs CEO, Székhely: 1106 Budapest, Fehér út 10., tel.: +36 20 222 0011, mailto:adatkezeles@ens.hu	hírlevél kiküldési szolgáltatás a regisztrált ügyfelek részére
INTROWEB Kft.	6724 Szeged, Gelei József u. 5. 1. em. 3., E-mail: info@introweb.hu	weboldal fejlesztés
Meta Platforms, Inc. (FB)	1601 Willow Road, Menlo Park, CA 94025, United States	közösségi internet oldal szolgáltatás
Google LLC, D/B/A YouTube	901 Cherry Ave. San Bruno, CA 94066, USA Fax: +1 650-253-0001	Globális internet szolgáltatás keretében az intézményi programok publikálása, azokról utólagos bemutató megjelentetése

IV. Az érintett adatkezeléssel kapcsolatos jogai

1. Tájékoztatás kéréshez, betekintéshez (hozzáféréshez) való jog. Az érintett az Adatkezelőtől kérheti, az adjon tájékoztatást, hogy róla milyen személyes adatot kezelnek, annak forrásáról, az adatkezelés céljáról, jogalapjáról, időtartamáról, az adattovábbítás jogalapjáról és címzettjéről.

2. A helyesbítéshez való jog. Az érintett helyesbítéshez való joga minden adatkezelési jogalap vonatkozásában megilleti. Az Adatkezelő a kérelmem esetén indokolatlan késedelem nélkül helyesbíti az érintettre vonatkozó pontatlanul kezelt személyes adatokat.

3. Adattörléshez (elfeledtetéshez) való jog. Az érintett kérheti, hogy az Adatkezelő törölje a személyes adatait. A törlési kérelmet az Adatkezelő különösen abban az esetben utasítja el, ha a jogszabály őt a személyes adatok tárolására és / vagy zárolásra kötelezi, pl. hatósági vagy bírósági eljárás során.

4. Zároláshoz való jog. Az érintett kérheti, hogy a személyes adatait az Adatkezelő zárolja, ami a tárolt személyes adatok megjelölését jelenti a jövőbeli kezelésük korlátozása céljából. A zárolás addig tart, amíg az érintett által megjelölt indok szükségessé teszi az adatok tárolását.

5. A tiltakozáshoz való jog. Az érintett írásban tiltakozhat az adatkezelés ellen. Így például, ha az Adatkezelő személyes adatot közvetlen üzletszerzés, ennek érdekében például a személyes adatára vonatkozó matematikai és statisztikai elemző eljárásokat alkalmazna, vagy közvélemény-kutatás vagy tudományos kutatás céljából továbbítaná, felhasználná.

6. Adathordozhatósághoz való jog. Az érintett jogosult kérni az Adatkezelőtől a személyes adatainak adatkezelők közötti, másik adatkezelőnek történő közvetlen továbbítását, ha ez technikailag megvalósítható és nem ütközik uniós vagy nemzeti jogszabály előírásába.

7. Önkéntes hozzájárulás esetén a visszavonáshoz való jog. Az érintett jogosult arra, hogy hozzájárulását bármikor visszavonja. A hozzájárulás visszavonása nem érinti a hozzájáruláson alapuló, a visszavonás előtti adatkezelés jogszerűségét.

8. Kérelem benyújtásának a joga. Az Adatkezelő köteles a kérelem benyújtásától számított legrövidebb idő alatt, legfeljebb azonban egy hónapon belül, közérthető formában, az érintett erre irányuló kérelmére írásban megadni a válaszát.

V. Információbiztonság az adatkezelésben

1. Az Adatkezelő információbiztonsági státusza: az Adatkezelő nem tartozik az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény hatálya alá, a védelmi intézkedésekről szóló döntést az Adatkezelő önállóan határozza meg.

2. Az Adatkezelő a papír alapú iratok kezelése és az elektronikus adatok használata során az információbiztonsági előírásai alapján, megfelelően gondoskodik arról, hogy ne forduljon elő adatvédelmi incidens.

3. Az Adatkezelő az adatokat megfelelő intézkedésekkel védi
   a) a jogosulatlan hozzáférés,
   b) megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a
   c) véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó
   d) hozzáférhetetlenné válás ellen.

4. Az Adatkezelő az adatbiztonság feltételeinek érvényesítése érdekében gondoskodik az érintett munkatársak megfelelő felkészítéséről.

5. Az Adatkezelő az adatok biztonságát szolgáló intézkedések meghatározásakor és alkalmazásakor tekintettel van a technika mindenkori fejlettségére. Az Adatkezelő több lehetséges adatkezelési megoldás közül azt választja, amely a személyes adatok magasabb szintű védelmét biztosítja, kivéve, ha az aránytalan nehézséget jelentene.

6. Az elektronikusan tárolt adatok esetében adatot csak a nyilvántartott hozzáférési jogosultsággal rendelkező adatkezelő kezelhet. Az adatkezelőnek egyéni, titkos jelszóval kell bejelentkeznie a rendszerbe. A rendszerben történt, jelszóval védett adatkezelésért az adatkezelő felel. Az esetleges visszaélések elkerülése érdekében az adatkezelő kötelezettsége, hogy egyéni jelszavak titkosságát biztosítsa. Az adatkezelés befejeztével az adatkezelőnek a rendszerből ki kell lépnie.

7. Az Adatkezelőnél alkalmazott információbiztonsági feltételek és adottságok:
   a) Az internetről letöltött programok nem futtathatóak felhasználói beavatkozás nélkül.
   b) Nem futtathatóak programok, melyek hitelességét az operációs rendszer nem tudta ellenőrizni.
   c) Otthoni munkavégzés esetében magáneszközök nem csatlakozhatnak a vállalati hálózathoz.
   d) A szoftverek telepítése a számítógépre csak adminisztrátori jogosultsággal lehetséges.
   e) A Microsoft Office csomagokat úgy állították be, hogy csak aláírt makrókat futtassanak.
   f) Az e-mail szerveren spam- és vírusszűrő van.
   g) Minden asztali számítógépet és laptopot úgy konfiguráltak, hogy az operációs rendszer szoftverfrissítései automatikusan telepítésre kerüljenek.
   h) Az operációs rendszer gyártójától származó biztonsági frissítéseket automatikusan betölti, és azonnal elérhetővé tegye az összes asztali számítógép és laptop számára.

8. Csak olyan operációs rendszerek van használatban, melyekhez a gyártó biztonsági frissítéseket biztosítja.

9. A kockázattal kapcsolatos fogalmak.

   a) kockázat: a fenyegetettség mértéke, amely egy fenyegetés bekövetkezése gyakoriságának (bekövetkezési valószínűségének) és az ez által okozott kár nagyságának a függvénye;

   b) A kockázatelemzés: az elektronikus információs rendszer értékének, sérülékenységének (gyenge pontjainak), fenyegetéseinek, a várható károknak és ezek gyakoriságának felmérése útján a kockázatok feltárása és értékelése.

   c) A kockázatkezelés: az elektronikus információs rendszerre ható kockázatok csökkentésére irányuló intézkedésrendszer kidolgozása.

10. **A GDPR Praeambulum (77) bekezdése alapján, a kockázatok felmérését el kell végezni a személyes adatok kezelése során**:
    a. „ *... megfelelő intézkedéseknek az adatkezelő vagy adatfeldolgozó általi végrehajtásához, valamint a megfelelés általuk való bizonyításához - különösen ami az adatkezeléssel kapcsolatos kockázat beazonosítását, valamint a kockázat forrásának, jellegének, valószínűségének és súlyosságának a felmérését illeti -, továbbá a kockázat mérséklésével kapcsolatos bevált gyakorlatoknak”* az ismerete szükséges

11. **A GDPR Praeambulum (78) bekezdése** kötelezettségi kapcsolatban van a fizikai, adminisztratív és logikai védelmi intézkedések megszervezésével és végrehajtásával:
    a. „*A természetes személyeket személyes adataik kezelése tekintetében megillető jogok és szabadságok védelme megköveteli az e rendelet követelményeinek teljesítését biztosító megfelelő technikai és szervezési intézkedések meghozatalát.”*

12. A GDPR Praeambulum (83) bekezdése olyan előírásokat tartalmaz, amely átfedést jelent a **Bizalmasság-Sértetlenség-Rendelkezésre állás** követelményeivel és az adatvédelmi incidens megelőzési kötelezettségével:

    (83) A biztonság fenntartása és az e rendeletet sértő adatkezelés megelőzése érdekében az adatkezelő vagy az adatfeldolgozó értékeli az adatkezelés természetéből fakadó kockázatokat, és az e kockázatok csökkentését szolgáló intézkedéseket, például titkosítást alkalmaz. Ezek az intézkedések biztosítják a megfelelő szintű biztonságot - ideértve a bizalmas kezelést is -, figyelembe véve a tudomány és technológia állását, valamint a végrehajtás kockázatokkal és a védelmet igénylő személyes adatok jellegével összefüggő költségeit. Az adatbiztonsági kockázat felmérése során a személyes adatok kezelése jelentette olyan kockázatokat - mint például a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítése, elvesztése, megváltoztatása, jogosulatlan közlése vagy az azokhoz való jogosulatlan hozzáférés - mérlegelni kell, amelyek fizikai, vagyoni vagy nem vagyoni károkhoz vezethetnek.

13. **A GDPR 32. cikk Az adatkezelés biztonsága** című tényállásában, az előbb ismertetett kötelezettségeket a következő előírásokkal erősíti meg:

Az adatkezelő és az adatfeldolgozó a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja, ideértve, többek között, adott esetben:

a. *a személyes adatok álnevesítését és titkosítását;*
b. *a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítását, integritását, rendelkezésre állását és ellenálló képességét;*
c. *fizikai vagy műszaki incidens esetén az arra való képességet, hogy a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását kellő időben vissza lehet állítani;*
d. *az adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedések hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárást.*

(2) A biztonság megfelelő szintjének meghatározásakor kifejezetten figyelembe kell venni az adatkezelésből eredő olyan kockázatokat, amelyek különösen a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítéséből, elvesztéséből, megváltoztatásából, jogosulatlan nyilvánosságra hozatalából vagy az azokhoz való jogosulatlan hozzáférésből erednek.

VI. Fontosabb fogalmak.

különleges adat: a) a faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviseleti szervezeti tagságra, a szexuális életre vonatkozó személyes adat, b) az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat, valamint a bűnügyi személyes adat;

adatkezelő: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely önállóan vagy másokkal együtt az adat kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja;

adatfeldolgozó: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely szerződés alapján - beleértve a jogszabály rendelkezése alapján kötött szerződést is - adatok feldolgozását végzi;

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

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;

biometrikus adat: egy természetes személy testi, fiziológiai vagy viselkedési jellemzőire vonatkozó minden olyan sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását, ilyen például az arckép vagy a daktiloszkópiai adat;

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;

biztonsági esemény: nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül;

biztonsági esemény kezelése: az elektronikus információs rendszerben bekövetkezett biztonsági esemény dokumentálása, következményeinek felszámolása, a bekövetkezés okainak és felelőseinek megállapítása, és a hasonló biztonsági események jövőbeni előfordulásának megakadályozása érdekében végzett tervszerű tevékenység;

egészségügyi adat: egy természetes személy testi vagy pszichikai egészségi állapotára vonatkozó személyes adat, ideértve a természetes személy számára nyújtott egészségügyi szolgáltatásokra vonatkozó olyan adatot is, amely információt hordoz a természetes személy egészségi állapotáról;

elektronikus információs rendszer biztonsága: az elektronikus információs rendszer olyan állapota, amelyben annak védelme az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos;

elektronikus információs rendszer: az adatok, információk kezelésére használt eszközök (környezeti infrastruktúra, hardver, hálózat és adathordozók), eljárások (szabályozás, szoftver és kapcsolódó folyamatok);

megelőzés: a fenyegetés hatása bekövetkezésének elkerülése;

MTPD (Maximum Tolerable Period of Disruption): Maximálisan tolerálható megszakadási időtartam, az a legnagyobb idő intervallum, ameddig a szervezet tolerálni képes az általa nyújtandó szolgáltatás kiesését;

nyilvántartási rendszer: a személyes adatok bármely módon - centralizált, decentralizált vagy funkcionális vagy földrajzi szempontok szerint - tagolt állománya, amely meghatározott ismérvek alapján hozzáférhető;

reagálás: a bekövetkezett biztonsági esemény terjedésének megakadályozására vagy késleltetésére, a további károk mérséklésére tett intézkedés;

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

rendkívüli esemény: minden olyan esemény, amely az Adatkezelő és Adatkezelői tevékenységének folyamatosságát támogató informatikai rendszerek folyamatos, üzemzavar mentes működőképességét veszélyezteti, vagy akadályozza;

részleges működőképesség: az az állapot, amikor az informatikai architektúra valamely elemének meghibásodása miatt az informatikai rendszerek bizonyos funkciói, vagy egésze jelentős ideig működésképtelenné válnak;

sértetlenség: az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanságát) is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható;

súlyos biztonsági esemény: olyan informatikai esemény, amely bekövetkezése esetén az állami működés szempontjából kritikus adat bizalmassága, sértetlensége vagy rendelkezésre állása sérülhet, emberi életek kerülhetnek közvetlen veszélybe, személyi sérülések nagy számban következhetnek be, súlyos bizalomvesztés következhet be az állammal vagy az érintett szervezettel szemben, alapvető emberi, vagy a társadalom működése szempontjából kiemelt jogok sérülhetnek;

teljes körű működésképtelenség: az az állapot, amikor az informatikai architektúra valamely elemének meghibásodása miatt az informatikai rendszerek még a minimális, erősen korlátozott rendszer funkciókat sem tudják ellátni, az ügyviteli folyamatok többségének informatikai támogatása megszűnik, és ennek helyreállítása jelentős időt vesz igénybe;

üzemzavar: az az állapot, amikor az informatikai rendszerek működésében rövid idejű zavar keletkezik, s így a rendszer néhány funkciójának átmeneti meghibásodása következik be, a zavar elhárítását az informatikai üzemeltető a napi rutinja alapján rövid idő alatt képes elvégezni;

védelmi feladatok: megelőzés és korai figyelmeztetés, észlelés, reagálás, eseménykezelés

VII. Általános tájékoztatás.

Az érintett kérelemre adott válasz felülvizsgálatának kezdeményezésére vonatkozó jogok:

1. Ha az érintettnek nem sikerült a személyes adatával kapcsolatos tiltakozását, panaszát, kérelmét az Adatkezelőnél megnyugtató módon rendeznie és / vagy úgy ítéli meg, hogy személyes adatai kezelésével kapcsolatban jogsérelem következett be vagy annak közvetlen veszélye fennáll, úgy
2. a Nemzeti Adatvédelmi és Információszabadság Hatóságnál jogosult bejelentést tenni és / vagy
3. jogosult polgári peres eljárásban bírósághoz fordulni, amelynek elbírálása a Szegedi Törvényszék hatáskörébe tartozik. Az érintett választása szerint a per a lakóhelye szerinti törvényszék előtt is megindítható.

A Nemzeti Adatvédelmi és Információszabadság Hatóság elérhetőségei:
Székhely: 1055 Budapest, Falk Miksa utca 9-11.
Postacím: 1363 Budapest, Pf. 9.
E-mail: ugyfelszolgalat@naih.hu
Telefon: +36 (1) 391 1400, +36 (30) 683-5969 és +36 (30) 549-6838
Ügyfélszolgálati idő: hétfő - csütörtök 9:00 – 16:00 óra között, péntek: 9:00 – 14.00 óra között
Honlap: www.naih.hu

S z e g e d, 2022. május 31.

Orbán Hedvig
igazgatónő