Csapi-15 Vásárcsarnok és Piacfenntartó Kft.

1156 Budapest, Nyírpalota út 52. Tel.: 06-1-418-3188

csapi.info@t-online.hu - http://www.ujpalotapiaca.hu

MUNKAVÁLLALÓI ADATBIZTONSÁGI SZABÁLYZAT

Az Európai Parlament és Tanács 2016/679 Általános Adatvédelmi Rendelete – „GDPR”

- A természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról -

alapján

Hatályos: 2023. február 01. napjától

Készítette:	Ellenőrizte és jóváhagyta:
Dr. Miklós Péter	Szakály Kis Csilla Gabriella
adatvédelmi tisztviselő	ügyvezető
sk.	sk.

TARTALOMJEGYZÉK

TARTALOMJEGYZÉK 21. ÁLTALÁNOS TÁJÉKOZTATÁS 32. BIZTONSÁGRA TÖREKVŐ VISELKEDÉS A MUNKAHELYEN 43. A SZÁMÍTÓGÉPES MUNKAHELY BIZTONSÁGOS HASZNÁLATA 54. A HORDOZHATÓ SZÁMÍTÓGÉPEK BIZTONSÁGOS HASZNÁLATA 65. MOBIL INFORMATIKAI ADATHORDOZÓK BIZTONSÁGOS HASZNÁLATA 86. A TÁRSASÁG INFORMATIKAI HÁLÓZATÁNAK BIZTONSÁGOS HASZNÁLATA 97. JELSZÓ HASZNÁLATI SZABÁLYOK 108. MUNKAHELYI ELEKTRONIKUS LEVELEZÉS BIZTONSÁGOS HASZNÁLATA 119. MUNKAHELYI INTERNET BIZTONSÁGOS HASZNÁLATA 1210. VÍRUSVÉDELMI SZABÁLYOK 1311. TEENDŐK ADATVÉDELMI INCIDENS ÉSZLELÉSE ESETÉN 1412. ZÁRÓ RENDELKEZÉSEK 15

ÁLTALÁNOS TÁJÉKOZTATÁS

Az adatkezelő tevékenységét úgy végzi, hogy adatkezelési folyamatai összhangban állnak az Európai Parlament és Tanács 2016/679. számú Általános Adatvédelmi Rendeletének (a továbbiakban: "GDPR"), amely alapvetően szabályozza a természetes személyeknek a személyes adatok kezelése tekintetében történő védelmét és az ilyen adatok szabad áramlását.

1.1. A Szabályzat célja

A jelen szabályzat célja a Társaság általános működésében minden papír alapú adatkezelése és informatikai rendszer használata során előírni azokat az alapvető, minden munkatársra vonatkozó viselkedési, munkahelyi és informatikai eszközök használatára vonatkozó biztonsági szabályokat, amelyek az alapvető adatok (beleértve a személyes adatok) kezelésének adatbiztonsági feltételeit biztosítják.

A Társaság által kezelt adatok biztonságának kialakításához és fenntartásához – a jelen szabályzat előírásán, betartásán és számonkérésén túlmenően – szükség van még az Informatikai infrastruktúra üzemeltetésének megfelelően biztonságos és szabályozott működtetésére is, amelyre vonatkozó adatbiztonsági alapelveket a rendszergazda számára az „IT Üzemeltetés Adatvédelmi Szabályzata" c. szabályzat tartalmazza.

1.2. A szabályzat hatálya

A jelen szabályzat hatálya kiterjed a Társaság minden alkalmazottjára és szerződéses alvállalkozójára, akik a Társaság informatikai infrastruktúrájához hozzáférnek, azt használják, illetve a Társaság folyamataiban, tevékenységeiben részt vesznek, a Társaság számára (adatokkal történő) műveleteket, feladatokat látnak el.

1.3. A szabályzat használata

Jelen adatbiztonsági szabályok azokat általános, számítógépes munkahelyen dolgozó minden kolléga, munkatárs által betartandó adatbiztonsági célú szabályokat foglalják össze, amelyek alapvetőek és szükségesek a papír alapú és elektronikus formátumú adatok – különösen a személyes adatok – kezelésének alapvető biztonságos használatához.

2. FELELŐSSÉGTELJES VISELKEDÉS A MUNKAHELYEN

2.1. Személyes adatokat tartalmazó dokumentumok, iratok nem hagyhatók felügyelet nélkül az asztalon.

2.2. Munkavégzés során (lehetőleg) csak azok az iratok, illetve dokumentumok lehetnek elöl az asztalon, amelyek az adott munka végzéséhez akkor szükségesek.

2.3. Munkavégzés után minden személyes adatot tartalmazó dokumentumot, iratot és elektronikus adathordozót el kell tenni az asztalokról, és zárt, biztonságos helyen kell tárolni.

2.4. A zárható íróasztalokat és szekrényeket is (amennyiben kulcsra zárhatóak) kulcsra zárva kell tartani, és a kulcsokat biztonságos helyen kell őrizni.

2.5. Megbeszélések után a tanácskozóteremből (tárgyalóból) minden bizalmas tartalmú dokumentumot, különösen a személyes adatokat tartalmazó iratokat, papírokat, jegyzeteket el kell távolítani. (Ide beleértendők a használt flip-chart papírok eltávolítása, táblák letörlése, stb.)

2.6. Személyes adatokat tartalmazó dokumentumok, iratok másolásakor sem eredeti példány, sem másolat nem maradhat a másolóban.

2.7. Személyes adatokat tartalmazó dokumentumok, iratok csak olyan személyeknek adhatók át, akik munkaköri feladatuknál fogva vagy jogszabályi előírásnak megfelelve jogosultak azoknak az információnak a megismerésére vagy használatára, és az átadó személy erről meggyőződött.

2.8. Elektronikus átviteli út (pl. telefon, fax, e-mail) esetén a bizalmas információkat ajánlott, az üzleti titoknak minősített információkat kötelező titkosítva átvinni.

2.9. Amennyiben a személyes adatokat tartalmazó dokumentumok, iratok őrzésére, tárolása már nincs szükség, azokat papírdarálóval kell megsemmisíteni, vagy biztonságos gyűjtés, tárolás után eljuttatni a szabályozásnak megfelelő, felügyelt megsemmisítésre.

2.10. A személyes adatokat tartalmazó kézi feljegyzéseket, munkapéldányokat, másolati példányokat, stb. ugyanolyan biztonsággal kell kezelni, mint az azokat az információkat tartalmazó eredeti, hivatalos iratokat.

3. A SZÁMÍTÓGÉPES MUNKAHELY BIZTONSÁGOS HASZNÁLATA

3.1. Minden felhasználó köteles az általa használt számítógépet rendeltetésének megfelelően, kizárólag munkájának végzésére, illetve támogatására használni.

3.2. Minden felhasználó köteles az esetleges meghibásodásokat azonnal jelezni a rendszergazdának.

3.3. TILOS a számítógép (vagy egyéb informatikai eszköz) burkolatát megbontani, az eszköz belső részéhez hozzáférni, azon változtatásokat végezni. A garancia címke nem sérülhet meg!

3.4. TILOS a telepített (nem hordozható) számítógépet (vagy egyéb informatikai eszközt) a rendszergazda értesítése nélkül más munkahelyre áttelepíteni.

3.5. A felhasználó nem változtathatja meg a használatába kapott számítógép (vagy egyéb informatikai eszközök) konfigurációját. A perifériák cseréjét, a szoftverek telepítését csak a rendszergazda végezheti.

3.6. TILOS külső bootolást (számítógép külső egységről vagy perifériáról történő indítását) alkalmazni.

3.7. A felhasználó számítógépét csak saját azonosítójával és jelszavával belépve használhatja. A felhasználó számára büntetőjogi, illetve munkajogi felelősségre vonás terhe mellett TILOS más azonosítójának használata.

3.8. A felhasználó a számítógépeken csak azokat a szoftvereket használhatja, amelyeket a rendszergazda a munkája elvégzéséhez telepített.

3.9. A felhasználó a számítógépére semmilyen szoftvert nem telepíthet, nem törölhet, és nem módosíthat. E rendelkezés megszegéséért a felhasználó ellen felelősségre vonás kezdeményezhető.

3.10. A felhasználó semmilyen olyan szoftvert, amit nem a rendszergazda telepített, nem futtathat a számítógépén. (Ebbe beleértendők a telepítést nem igénylő, külső eszközről – pl. CD/DVD-ROM, USB Flash drive, stb. – indítható programok, valamint a freeware, shareware szoftverek, illetve bármilyen nem a Társaság tulajdonát képező szoftverek is.)

3.11. A számítógépes asztalon minél kevesebb alkalmazás, dokumentum legyen egyidejűleg megnyitva, lehetőleg csak azok, amelyek az adott munka végzéséhez akkor szükségesek.

3.12. Rövidebb idejű távollét esetén a számítógépet legalább zárolni kell.

3.13. Hosszabb idejű távollét esetén ki kell jelentkezni az alkalmazásokból, és a számítógépet ki kell kapcsolni.

4. A HORDOZHATÓ SZÁMÍTÓGÉPEK BIZTONSÁGOS HASZNÁLATA

4.1. A hordozható számítógépek biztonságos használatára érvényesek a számítógépek biztonságos használatára, az előző fejezetben előírt szabályok mind.

4.2. A hordozható számítógépet extrém hőmérséklet, mágneses tér, magas páratartalom vagy erős füstképződés hatásának kitenni TILOS.

4.3. A számítógépeket működő állapotban szállítani nem szabad. (Ez nem vonatkozik az utazás közbeni használatra.)

4.4. Repülőutak alkalmával hordozható számítógép kézipoggyászként szállítandó. Lehetőség szerint el kell kerülni a röntgenkészülékkel történő vizsgálatot.

Adatbiztonsági szabályok:

4.5. Személyes adatok csak titkosítva tárolhatók a hordozható számítógépeken.

4.6. A hordozható számítógépen lokálisan tárolt adatok rendszeres mentéséről a felhasználó maga köteles gondoskodni. A mentéseknek az adathordozón titkosítva kell tárolni, és az adathordozókat biztonságosan kell tárolni.

4.7. A külső munkahelyen történő feladat elvégzése után a hordozható számítógépeken keletkezett vagy tárolt adatokat a megfelelő a hálózati fájlszerverekre kell menteni, és ezt követően a hordozható számítógépről le kell őket törölni.

Jogosulatlanok általi, információhoz való hozzáférések megakadályozása:

4.8. Bel- és külföldi kiküldetésre vitt (munkahelyi és otthoni használaton kívül) utazó kollégák notebookjainak titkosítását el kell végezni, ennek alkalmazásáért a felhasználó felelős.

4.9. A hordozható számítógépet csak annak a rendszergazda által beállított felhasználója, a saját bejelentkezésével és jelszavával, a munkavégzés céljára használhatja.

4.10. TILOS a hordozható számítógépet más célra használni, illetve másoknak (pl. családtagoknak, barátoknak, ügyfeleknek) használatra átengedni.

4.11. Különösen ott kell a használatot követően a tárolt adatok törlésére odafigyelni, ahol a hordozható számítógépet megosztva használják.

4.12. Nyilvános helyeken történő használatnál ügyelni kell arra, hogy illetéktelenek ne olvashassák el a képernyő tartalmát.

4.13. A hordozható számítógép rövid idejű elhagyásakor is azonnal zárolni kell a számítógépet, ezzel megakadályozva azt, hogy kívülállók betekinthessenek rendszerbe.

4.1.4 A rendszergazda által installált jelszavas képernyővédő törlése vagy várakozási idejének megváltoztatása TILOS.

Hordozható számítógépek fokozott vírusveszélye kockázatainak csökkentése:

4.15. A rendszergazda által installált központi vírusvédelmi rendszer használata kötelező.

4.16. Az idegen külső adathordozók (pl. optikai adathordozók, külső merevlemezek, flash drive-ok) vírusmentességét felhasználásuk előtt kötelező megvizsgálni.

4.17. A hordozható számítógép külső hálózatra kapcsolódását (pl. szállodákban, vásárokon, beszállítóknál, otthon) követő használata előtt soron kívüli, teljes gépre vonatkozó vírusellenőrzést kötelező végrehajtani.

Intézkedések, ha a hordozható számítógépet már ellopták, vagy elveszítették:

4.18. Az ellopás, elveszítés tényét a lehető leggyorsabban jelenteni kell a rendszergazdának.

4.19. Tájékoztatni kell a közvetlen felettes vezetőt arról (előzetesen szóban, majd ahogyan lehetőség adódik erre, írásban is megerősítve), hogy a berendezés tartalmaz-e bárminemű személyes adatot, vagy a Társaság illetve ügyfelei rendszereihez távoli hozzáférési lehetőséget.

4.20. Ha a számítógépet a szállodai szobából vagy a szálloda ingatlanján álló kocsiból lopták el értesíteni kell a szálloda vezetését.

4.21. Rendőrségi jegyzőkönyvet kell felvetetni lopás esetén.

4.22. Hordozható számítógép ellopása esetén, hogyha az személyes adatot is tartalmazott, azt személyes adatvédelmi incidensnek kell minősíteni, és az annak megfelelő eljárást azonnal el kell indítani.

5. MOBIL INFORMATIKAI ADATHORDOZÓK BIZTONSÁGOS HASZNÁLATA

5.1. Munkavégzés céljaira csak a rendszergazda által kapott, céges adathordozó használható.

5.2. Az adathordozókat azok feldolgozása és tárolása alatt úgy kell kezelni, hogy biztosítva legyenek elvesztés, megsemmisülés, megsérülés és elcserélés, valamint jogosulatlan hozzáférés ellen.

5.3. Gondosan és elzárva kell a használaton kívüli adathordozókat is tárolni.

5.4. Azokat a mobil adathordozókat, amelyeket privát számítógéppel történő adatcserére használtak, újrafelhasználás előtt újra kell formázni.

5.5. A személyes adatokról készült másolatok érzékenysége – és adatvédelmi igénye – megegyezik az eredeti személyes adat érzékenységével, ezért ugyanúgy kell védeni a másolatokat is.

5.6. Személyes adatot tartalmazó elektronikus adathordozókat egyidejűleg más célra felhasználni TILOS.

5.7. Személyes adatok titkosított tárolása hordozható elektronikus adattárolón ajánlott, amennyiben a hordozható adathordozón a személyes adatok Társaság telephelyén kívüli szállítása vagy átadása szükséges, akkor viszont minden esetben kötelező.

5.8. A hordozható adathordozókon lévő adatok illetéktelenek általi hozzáféréséért a felhasználó a felelős.

5.9. Személyes adatot tartalmazó, meghibásodott háttértár egységet (merevlemezt) akár garanciális javítás keretében lecserélni, vagy bármely formában kiadni TILOS. (Ez vonatkozik a hálózati merevlemezes nyomtatók és multifunkcionális berendezések merevlemezeire is.)

5.10. Selejtezésre kijelölt, személyes adatokat tartalmazó elektronikus adathordozókat kidobni TILOS. Azt minden esetben dokumentált megsemmisítési eljárással, bizottság előtt kell selejtezni.

6. A TÁRSASÁG INFORMATIKAI HÁLÓZATÁNAK BIZTONSÁGOS HASZNÁLATA

6.1. A hálózaton csak a rendszergazda által biztosított és üzemeltetett informatikai eszközök lehetnek.

6.2. Számítógép-hálózati kábel szomszédos helyiségekbe történő áthúzása TILOS!

6.3. A hálózatba a felhasználók csak a saját belépési azonosítójukat használva jelentkeznek be.

6.4. TILOS a saját azonosító és jelszó átadása másnak.

6.5. A rendszergazda által biztosított eszközöket a vállalati hálózatra csatlakoztatás során egy másik, lokális (vezetékes vagy vezeték nélküli) hálózatra kötve megosztani SZIGORÚAN TILOS!

6.6. Az informatikai rendszer használata otthonról csak korlátozottan, felső vezetői engedéllyel, biztonságos VPN csatornán keresztüli bejelentkezéssel engedélyezhető.

6.7. Az informatika rendszerek távoli eléréssel történő használata során a rendszergazda által beállított biztonsági eljárások, eszközök és beállítások (pl. titkosított csatorna, VPN, stb.) használata kötelező.

7. JELSZÓ HASZNÁLATI SZABÁLYOK

A jelszó képzése:

7.1. A jelszónak olyannak kell lennie, hogy tulajdonosa könnyen megjegyezhesse, de a kívülállók nehezen találhassák ki.

7.2. Egy jelszónak, ha az technikailag lehetséges, minimum 8 karakterből kell állnia, nagy és kisbetűket, számokat kell tartalmaznia.

7.3. A korábban már alkalmazott jelszavakat nem szabad többször felhasználni.

7.4. Különböző rendszerekhez történő belépésekre különböző jelszavakat kell használni.

A jelszavak cseréje:

7.5. A jelszót a következő esetekben mindig azonnal meg kell változtatni:

- A jelszó tudatos továbbadása esetében, amennyiben az ok már nem áll fenn (pl. karbantartási munkák).
- Minden olyan esetben, amikor fennáll a gyanúja annak, hogy ismertté vált.
- A rendszerrel együtt kiszállított, előre beállított jelszavakat az üzembeállítást követően azonnal.

7.6. Minden egyéb esetben a javasolt jelszavakat rendszeresen cserélni.

A jelszó titokban tartása:

7.7. A felhasználónak titokban kell tartani jelszavait.

7.8. A jelszavakat még a közeli munkakapcsolatban álló, egymást jól ismerő kollégák sem közölhetik egymással.

7.9. A feltétlenül szükséges jelszó-feljegyzések csak úgy tárolhatók, hogy ahhoz csak és kizárólag maga a felhasználó férhet hozzá személyesen.

7.10. A jelszó-feljegyzések tárolására nem használhatók az ún. szabadon rendelkezésre álló „emlékezet-segítők”, mint pl. felragasztva monitorra, billentyűzet aljára, stb.

7.11. Jelszavak nem tárolható olvasható formátumú fájlokban (pl. txt, doc, xls, stb. fájl).

7.12. A jelszavakat és azonosítókat tartalmazó üzeneteket nem szabad üzenetrögzítőn megadni, FAX készülékkel, vagy nem titkosított csatornán elküldeni.

7.13. A jelszavak bevitelénél ügyelni kell arra, hogy azt begépelés közben mások ne olvashassák el, ne leshessék ki.

Különleges szabályok helyettesítések/vészhelyzetek esetére

7.14. Kivételes esetekben (pl. a jelszó elvesztése, elfelejtése esetén) a rendszergazdától, a megfelelő személyi azonosítás után egy új jelszó igényelhető. Az új jelszót a belépést követően azonnal le kell cserélni, erre a rendszer automatikusan felszólít.

7.15. Helyettesítés és távollét esetén az érintett helyettesítő személy rendszerbeli meghatalmazása, és ezen keresztül számára – a helyettesítés időtartamára – a szükséges jogosultságok központi (rendszergazda általi) beállítása a helyes, hivatalos eljárás.

8. MUNKAHELYI ELEKTRONIKUS LEVELEZÉS BIZTONSÁGOS HASZNÁLATA

8.1. A Társaság az elektronikus levelezési szolgáltatást (e-mailt) csak és kizárólag munkavégzés céljából, a munkaköri feladatok hatékonyabb ellátásának érdekében biztosítja. A szolgáltatást magán célra és egyéb, a munkavégzéssel nem összefüggő célokra használni TILOS.

8.2. Az elektronikus levelezés használati engedélye személyre szóló, azt kizárólag a felhasználó saját maga veheti igénybe.

8.3. A felhasználó saját azonosítójának és jelszavának átadása más felhasználók részére TILOS.

8.4. Helyettesítés és távollét esetén a levelezés továbbításának szabálya beállítható, a válaszlevelek küldése esetében az érintett helyettesítő személy rendszerbeli meghatalmazása a helyes, hivatalos eljárás.

8.5. TILOS a munkahelyi e-mail címmel magánjellegű regisztrációt tenni (pl. közösségi oldalak).

8.6. Az ingyenes levelezőrendszerek (pl. freemail.hu) munkahelyi célú használata TILOS.

8.7. Az elektronikus levelek és csatolmányok védelmi előírásai megegyeznek az egyéb dokumentumok védelmének előírásaival.

Az E-mailek küldésére vonatkozó irányelvek:

8.8. A feladó, mint tulajdonos felelős az E-mail tartalmáért.

8.9. TILOS más nevében e-mailt küldeni, kivéve meghatalmazottak (pl. titkárnő) esetében.

8.10. A leveleket mindig célzottan kell kiküldeni, sosem szükségtelenül nagy elosztási kör számára.

8.11. Nagy adatmennyiségeket lehetőleg csak tömörített formátumú csatolmányként szabad küldeni.

8.12. Személyes adatokat tartalmazó dokumentumok e-mail-en keresztül csak titkosított formában küldhetők.

8.13. Zavaró, félreinformáló levelek küldése, jogtalan megrendelések elindítása TILOS és eljárást vonhat maga után.

Az E-mailek fogadására vonatkozó irányelvek:

8.14. A címzett felelős az E-mail tovább-feldolgozásáért és továbbításáért.

8.15. Bizalmas információk (pl. különlegesen személyes adatok) továbbítását kérő elektronikus levelek esetében mindig meg kell győződni az információkérés hitelességéről.

8.16. Ismeretlen helyről származó e-mail-t (pl. a feladó ismeretlen, vagy a feladó e-mail gyanús) megnyitás nélkül, olvasatlanul törölni kell.

8.17. Külső vagy belső e-mail címről érkező, félrevezető tartalmú e-mail-ek esetén azonnal értesíteni kell a rendszergazdát.

8.18. A kapott E-mail mellékleteket először számítógépes víruskeresővel kell átvizsgálni, amennyiben azok pl. futtatható programokat tartalmaznak.

9. MUNKAHELYI INTERNET BIZTONSÁGOS HASZNÁLATA

9.1. A Társaság az Internet használatot munkavégzés céljából, a munkaköri feladatok hatékonyabb ellátásának érdekében biztosítja.

9.2. Az Internet használati engedély személyre szóló, azt kizárólag a felhasználó saját maga veheti igénybe.

9.3. Az Internetes oldalak elérése monitorozásra és naplózásra kerülhetnek, a munkával összefüggésbe nem hozható oldalak elérhetőségét a rendszergazda biztonsági okból jogosult korlátozni.

9.4. Egyértelműen munkához nem köthető témájú Internetes oldalak látogatása TILOS, különösen ha látogatásuk jogi következményekkel járó – akár BTK-ba ütköző – tevékenységet jelenthet. (Pl. szexuális és pornográf tartalmú oldalak, torrent oldalak, rasszizmust, gyűlöletet, erőszakot népszerűsítő oldalak, stb.)

10. VÍRUSVÉDELMI SZABÁLYOK

A központi vírusvédelmi szoftver alkalmazására vonatkozó szabályok

10.1. A rendszergazda által telepített vírusvédelem nélkül sem hálózati, sem önálló munkaállomás, sem hordozható számítógép nem használható.

10.2. A felhasználó nem akadályozhatja a vírusvédelmi program és részeinek folyamatos futását.

10.3. A felhasználónak kötelessége jelenteni a rendszergazdának, ha észleli, hogy a gépén a vírusvédelmi szoftver nem működik folyamatosan.

10.4. A hordozható számítógépek esetében a vírusminta frissítésről való gondoskodás a felhasználó kötelessége.

10.5. A számítógépen idegen adathordozót csak vírusvizsgálat után lehet használatba venni.

10.6. Aki az adatait és adathordozóit rendszeres vírus ellenőrzés vagy vírusvédelmi intézkedés (vírusirtás) alól kivonja, felelősségre vonható, illetve az abból eredő károkért felel.

10.7. Office dokumentumok esetében kerülni kell a makrók és aktív tartalmak megnyitását, külső forrásból érkező dokumentum esetében pedig nem szabad engedélyezni a makrókat.

Teendők vírusfertőzés gyanúja vagy biztos felismerése esetén:

10.8. Ha a felhasználó gépén vírus jelenlétére utaló működési zavarok jelentkeznek,– ezt a vírusvédelmi program akár jelzi, akár nem,– a következő lépéseket kell tenni:

- Ne használja tovább vírusos vagy vírusgyanús rendszert.
- Ne változtassa meg a rendszer-állapotot.
- Azonnal jelentse az esetet a rendszergazdának, és tartsa be annak utasításait.

10.9. A rendszergazda jogosult a vírusveszély elhárításáig a vírusos számítógépet a hálózatról leválasztani, azon a munkavégzést megtiltani.

11. TEENDŐK ADATVÉDELMI INCIDENS ÉSZLELÉSE ESETÉN

11.1. Adatvédelmi incidensnek minősülnek például:

- Személyes adatok dokumentumon, hordozható eszközön, adathordozón vagy informatikai rendszeren (pl. levelezéssel) történő illegális továbbítása.
- Illetéktelen hozzáférések személyes adatokat kezelő informatikai rendszerhez vagy alkalmazáshoz (pl. jelenlegi vagy volt alkalmazott vétlen vagy tudatos közreműködése által, vagy biztonsági lyuk kihasználásával).
- Személyes adatokat tartalmazó adatbázis részének vagy egészének sérülése vagy elvesztése.
- Az informatikai rendszer részének vagy egészének használhatatlanná válása vírus vagy egyéb rosszindulatú szoftver által.
- Stb.

11.2. Adatvédelmi incidens (esemény) észlelésekor az azt észlelő személy köteles azonnal tájékoztatni közvetlen munkahelyi vezetőjét, aki haladéktalanul köteles tájékoztatni az adatvédelmi tisztviselőt az adatvédelmi incidens körülményeinek, kockázatainak, az érintettekre nézve hátrányos következményeinek és a szükséges intézkedések meghatározása érdekében. Az adatvédelmi tisztviselőnek azonnal el kell kezdenie az eset kivizsgálását, a megfelelő védelmi és kárcsökkentő intézkedések megtételét, és eleget kell tennie a szükséges jelentéstételi kötelezettségének, az „Adatvédelmi incidenskezelési szabályzat” előírásai szerint.

12. ZÁRÓ RENDELKEZÉSEK

12.1. Hatálybalépés

Jelen szabályzat 2023. február 01. napján lép hatályba, a benne foglaltak munkavállalók és egyéb közreműködők részére történő megismertetése az adatkezelő ügyvezetőjének a feladata és felelőssége.