Adatvédelmi szabályzat

Azonosító: IB11
Érvényesség: 2025. április 29.

Dokumentációs adatlap

Dokumentum jellemzők – IB11	
Szerző	Kolovics Márk
Besorolás	Belső
Verzió	v1.1
Státusz	kiadva

Dokumentum történet

Dátum	**Név**	**Verzió**	**Leírás**
2023.04.05	Kolovics Márk	v0.1	Dokumentum létrehozása
2024.02.29	Sárközi Zoltán	v1.1	Változások átvezetése, auditra történő felkészülés

Jóváhagyások

Dátum	**Név**	**Verzió**	**Szerepkör**
2023.08.30	Katona István	v1.0	Vezérigazgató
2024.04.29	Katona István	v1.1	Vezérigazgató

Tartalomjegyzék

1. Szabályzat célja

Jelen szabályzat célja, hogy általános szabályozási környezetet biztosítson az Innopay Zrt. (továbbiakban Társaság) tulajdonában lévő, illetve általa üzemeltetett informatikai rendszerekben tárolt vagy papír alapon rendelkezésre álló adatok kezelésével kapcsolatban, rögzítse az érzékeny személyes adatok kezelésének, tárolásának és továbbításának feltételeit, és előírja az adat- és információvédelemmel kapcsolatos követelményeket.

Szabályozza a személyes adatok bizalmasságát, hitelességét, sértetlenségét, rendelkezésre állását és funkcionalitását.

A szabályzat összefoglalja a Társaság által a működése, tevékenységének ellátása, szolgáltatásának nyújtása során gyűjtött, rendelkezésre bocsátott vagy egyéb módon tudomására jutott személyes adatok kezelésével kapcsolatos egyes lényeges rendelkezéseket, különösen az adatvédelmi tevékenység ellátásában résztvevő szervezeti egységek feladatait és együttműködésük kereteit.

A szabályzat továbbá biztosítja az aktuális jogszabályoknak, előírásoknak és iparági szabványoknak való megfelelést.

Jelen szabályzat a vezetés által jóváhagyott, minden munkavállaló számára elérhető és a külső érdekelt felek számára ismertetett követelményeket tartalmaz.

2. Szabályzat hatálya

2.1. Szabályzat személyi hatálya

A szabályzat személyi hatálya kiterjed a Társaság valamennyi munkavállalójára, valamint a Társaság informatikai rendszerével, szolgáltatásaival szerződéses, vagy más módon kapcsolatba kerülő természetes és jogi személyekre, jogi személyiséggel nem rendelkező szervezetekre (továbbiakban: külső személy) a velük kötött szerződésben rögzített mértékben, illetve titoktartási nyilatkozat alapján.

2.2. Szabályzat tárgyi hatálya

A szabályzat tárgyi hatálya kiterjed a Társaság tulajdonában lévő valamennyi informatikai rendszerre, azok teljes életciklusában.

2.3. Szabályzat időbeni hatálya

Jelen szabályzat érvényes a hatálybalépés napjától, visszavonásig. A dokumentum aktualitását, alkalmasságát, hatékonyságát minden nagyobb változáskor, de legalább évente az Informatikai vezető felülvizsgálja, az Információbiztonsági Felelőssel (továbbiakban: IBF) egyeztetve.

A Szabályzatot a Vezérigazgató hagyja jóvá, adja ki és lépteti hatályba.

Az Informatikai vezető feladata, hogy a működési környezetben bekövetkezett jelentősebb változás esetén is elvégezze a szabályzat felülvizsgálatát. A felülvizsgálat a legutolsó felülvizsgálat óta bekövetkezett jogszabályi, funkcionális, biztonsági, technológiai vagy egyéb változásokra kell kiterjedjen.

A szabályzatot minden érintettnek meg kell ismernie, de gondoskodni kell arról, hogy a szabályzat jogosulatlanok számára ne legyen megismerhető.

2.4. Kapcsolódó szabályzatok

Jelen dokumentum az alábbi szabályzatokhoz kapcsolódik, amely a Társaság szabályzatai között fellelhető:

a) Informatikai Biztonsági Szabályzat
b) Változáskezelési Szabályzat
c) Incidenskezelési Szabályzat
d) Jogosultságkezelési Szabályzat

A Társaság szabályzatain túl jelen dokumentum az alábbi jogszabályoknak és előírásoknak felel meg:

a) Az Európai Parlament és a Tanács 2016. április 27-i (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 (általános adatvédelmi rendelet) (továbbiakban: GDPR)
b) 2009. évi CLV. törvény a minősített adat védelméről (továbbiakban: Mavtv.)
c) 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (továbbiakban: Infotv.)
d) 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (továbbiakban: Ibtv.)
e) 2/2015. (III. 12.) Korm. rendelet a pénzügyi intézmények, a biztosítók és a viszontbiztosítók, továbbá a befektetési vállalkozások és az árutőzsdei szolgáltatók informatikai rendszerének védelméről
f) Magyar Nemzeti Bank 8/2020. (VI.22.) számú ajánlása az informatikai rendszer védelméről
g) Magyar Nemzeti Bank 4/2019. (IV.1.) számú ajánlása a közösségi és publikus felhőszolgáltatások igénybevételéről
h) A Magyar Nemzeti Bank 12/2020. (XI.6.) számú ajánlása a távmunka és távoli hozzáférés informatikai biztonsági követelményeiről
i) A Magyar Nemzeti Bank 11/2020. (X.20.) számú ajánlása a pénzügyi szervezetek működésének fizikai biztonsági és humánkockázatkezelési feltételeiről
j) Magyar Nemzeti Bank 7/2020. (VI.3.) számú ajánlása a külső szolgáltatók igénybevételéről
k) Magyar Nemzeti Bank 12/2022. (VIII.11.) számú ajánlása a belső védelmi vonalak kialakításáról és működtetéséről, a pénzügyi szervezetek irányítási és kontroll funkcióiról
l) NIST 800-53 szabvány moderate szint
m) ISO/IEC 27001 IEC:2013 Információbiztonsági szabvány
n) ISO/IEC 27002 IEC:2013 Információbiztonsági szabvány

3. Fogalmak, meghatározások, rövidítések

Adatcsoport	A Társaság működése és/vagy a folyamatok szempontjából összetartozó, magas szinten csoportosított adatok halmaza, amely logikailag egységesen kezelendő (eltekintve a megjelenési formátumban, a tárolási helyben, illetve a védelmi igényekben rejlő eltérésektől).
Adatfeldolgozás	Az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől.
Adatfeldolgozó	Az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely az adatkezelő megbízásából - beleértve a jogszabály rendelkezése alapján történő megbízást is - személyes adatok feldolgozását végzi.
Adatfeldolgozó rendszer	Információ meghatározott célú, módszeres gyűjtésére, tárolására, feldolgozására (bevitelére, módosítására, rendszerezésére) továbbítására, fogadására, megjelenítésére, megsemmisítésére stb. alkalmas rendszer.
Adatgazda	Annak a szervezeti egységnek a vezetője, ahová jogszabály vagy közjogi szabályozó az adat kezelését rendeli, illetve ahol az adat keletkezik, vagy ahol azt a szervezet egészére nézve központosítottan kezelik. Kötelessége a kezelésébe rendelt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának minősítését biztosítani, az adatkezelés ügyviteli folyamatát megszervezni, és egyben jogosult az adatok minősítésére, a javasolt minősítés jóváhagyására, az adatkörök, adatcsoportok osztályba sorolásának elvégzésére, illetve az adatok hozzáférését szabályozására (jogosultak köre). Jelen utasításban fogalma alatt minden esetben az Adatgazda helyettese is értendő.
Adathordozhatóság	Hozzájáruláson [GDPR 6. cikk (1) bek. a) pont, 9. cikk (2) bek. a) pont] vagy szerződésen [GDPR 6. cikk b) pont alapuló, automatizált módon történő adatkezelés esetén az érintett azon joga, hogy a rá vonatkozó, általa az adatkezelő rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja, továbbá azokat egy másik adatkezelőnek továbbítsa.
Adatkezelés	Az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása, a fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése is.
Adatkezelések nyilvántartása	Jelen utasítás 4.3.4 fejezetében meghatározott adattartalmú, folyamatosan karbantartott nyilvántartás.
Adatkezelési cél	Az a pontosan meghatározott, jogszerű cél, amelynek elérése érdekében a személyes adatokon az adatkezelő az adatkezelési műveleteket végzi.
Adatkezelő	Az a természetes, vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely – törvényben vagy az Európai Unió kötelező jogi aktusában meghatározott keretek között – önállóan vagy másokkal együtt az adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az általa megbízott adatfeldolgozóval végrehajtja.

Adatkör	Az adatkezelés szempontjából funkcionálisan összetartozó, egy adott adatcsoporton belül tovább bontható, de az adatmezők szintjénél magasabban csoportosított adatok halmaza, amely még logikailag egységesen kezelendő, fizikai megjelenési formátuma (papír, illetve elektronikus), valamint tárolási helye megegyezik, és a halmaz elemeinek védelmi igénye azonos. (példa: születési hely – adatmező, ügyfél azonosító adat – adatkör, ügyféladat - adatcsoport)
Adatmegsemmisítés	Az adatok vagy az azokat tartalmazó adathordozó visszaállíthatatlan, teljes fizikai megsemmisítése.
Adattovábbítás	Az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele. A szervezet egyes szervezeti egységei közötti, illetve az adatfeldolgozónak történő adatátadás nem minősül adattovábbításnak.
Adattörlés	Az adatok felismerhetetlenné tétele oly módon, hogy a helyreállításuk többé nem lehetséges.
Adatvagyon	A Társaság kezelésében lévő adatok összessége.
Adatvédelem	A személyes adatok jogszerű kezelését és feldolgozását, az adatok biztonságát, valamint az érintett személyek magánszférájának és személyhez fűződő jogainak védelmét biztosító alapelvek, szabályok, eljárások, adatkezelési eszközök, technikai és szervezeti intézkedések és módszerek összessége.
Adatvédelmi Csoport	Az adatvédelmi tisztviselő (továbbiakban: DPO) feladatai ellátásának támogatására rendelt, az egyéb szervezeti egység állományába tartozó munkavállalók.
Adatvédelmi esemény	Az adatvédelmi rendellenesség és az adatvédelmi incidens.
Adatvédelmi felügyeleti hatóság	A Nemzeti Adatvédelmi- és Információszabadság Hatóság, illetve a GDPR 56. cikke szerinti fő felügyeleti hatóság.
Adatvédelmi hatásvizsgálat	Olyan vizsgálat, amelyet az adatgazda köteles elvégezni, amennyiben valamely tervezett adatkezelés – figyelemmel annak jellegére, hatókörére, körülményeire és céljaira, ideértve különösen az új technológiák alkalmazásának esetét – valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, és amelynek célja annak megállapítása, hogy a tervezett adatkezelés a személyes adatok védelmét hogyan érinti. Az adatvédelmi hatásvizsgálat egy olyan eljárás, amelynek során az adatkezelő a tervezett adatkezelési műveletet vagy műveleteket áttekinti, megvizsgálja az adatkezelés érintettekre gyakorolt esetleges hatását, felméri annak kockázatait, a kockázatok kezelésének módját, és mindezt megfelelően dokumentálja.
Adatvédelmi incidens	Az adatbiztonság 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.
Adatvédelmi rendellenesség	Az adatbiztonság olyan megsértése, amelynél nem következik be az adatvédelmi incidenssé minősüléshez szükséges eredmény (a kezelt személyes adatok véletlen vagy jogellenes megsemmisítése, elvesztése, megváltoztatása, jogosulatlan közlése vagy az azokhoz való jogosulatlan hozzáférés).

Adatvédelmi tisztviselő	Az adatvédelmi jog és gyakorlat szakértői szintű ismeretével bíró személy, akit az adatkezelő és az adatfeldolgozó köteles kijelölni a GDPR 37. cikkében nevesített esetekben (így pl. abban az esetben, ha az adatkezelő vagy az adatfeldolgozó fő tevékenységei olyan adatkezelési műveleteket foglalnak magukban, amelyek jellegüknél, hatókörüknél és/vagy céljaiknál fogva az érintettek rendszeres és szisztematikus, nagymértékű megfigyelését teszik szükségessé, vagy különleges adatok nagy számban történő kezelését foglalják magukban), aki feladatai ellátása körében nem utasítható, és munkaviszony vagy szolgáltatási szerződés keretén belül végzi tevékenységét.
Alkalmazott	A Társasággal munkavégzésre irányuló jogviszonyban álló személyek.
Álnevesítés	A személyes adatok olyan módon történő kezelése, amelynek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik, feltéve, hogy az ilyen további információt külön tárolják, és technikai és szervezési intézkedések megtételével biztosított, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni.
Auditálás	Egy független IT auditor a jogszabályokban, az adat- és titokvédelmi szabályzatokban, a rendszerszintű informatikai biztonsági utasításokban foglaltaknak, valamint a nemzetközi szabványok és ajánlások szerint vizsgálja a rendszer megfelelését.
Belső információ	A Társaság vagy ügyfele pénzügyi, gazdasági vagy jogi helyzetével, vagy ezek várható változásával összefüggő – nyilvánosságra még nem került – olyan információ, amely nyilvánosságra kerülése esetén a Társaság vagy ügyfele megítélésének jelentős befolyásolására alkalmas.
Bizalmas adat	Olyan adat (információ), amelynek esetében jogszabály írja elő, illetve a Társaság érdeke, hogy csak meghatározott személyek köre (jogosultak) számára legyen hozzáférhető, mindenki más számára nem.
Bizalmasság	Az adat tulajdonsága, amely arra vonatkozik, hogy az adatot csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhessék meg, használhassák fel, illetve rendelkezhessenek a felhasználásáról.
Biztonsági monitoring	Figyelemmel kíséri a behatolási pontokon végzett rendszeres felderítési és felülvizsgálati tevékenységet. Folyamatosan vizsgálja az informatikai biztonság területén történt visszaéléseket, vagy ennek alapos gyanúja esetén az egyes eseményeket. Riasztási rendszer alkalmazásával megvalósul az IT biztonság azonnali reagáló képességének fokozása.
Biztonságtudatosság	A veszélyforrások felismerése, a védelmi intézkedések szükségességének elfogadása, és rendeltetésszerű végrehajtására való törekvés.
Deperszonalizálás (anonimizálás)	A nyilvántartási rendszerben tárolt személyes adatok közül a személyazonosításra alkalmas adatok eltávolítása olyan, visszafordíthatatlan módon, hogy a nyilvántartási rendszerben megmaradó adatok a továbbiakban semmilyen körülmények között nem teszik lehetővé egy természetes személy azonosítását.
Egyéb személyazonosító adatok	A személyes adatok bármely olyan kombinációja, amely alkalmas egy természetes személy azonosítására, vagyis más természetes személyektől való egyértelmű megkülönböztetésére.
Érdekmérlegelési teszt	Jogos érdeken alapuló adatkezelés tervezett bevezetése esetén annak írásbeli dokumentálása, hogy az adatkezelő számba vette az adatkezelést megalapozó érdekeket, érveket, valamint az érintettek személyes adatok védelméhez fűződő – a tervezett adatkezelés ellen ható – jogait és érdekeit, és ezen érdekek és érvek összevetésével megalapozza az adatkezelés bevezetését vagy a bevezetés elutasítását.

Érintett	Azonosított vagy azonosítható természetes személy. azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy egy, vagy több tényező alapján azonosítható.
Érzékeny adat	Bármely olyan üzleti-, személyes- vagy QR-adat, amely bizalmasságának, hitelességének vagy rendelkezésre állásának kompromittálódása a Társaság jogszabályi kötelezettségnek való nem megfelelőségét, piaci vagy pénzügyi kárt okozhat.
Folyamatfelelős	Olyan szakértő, aki felügyeli az adott (üzleti) folyamatot.
Harmadik fél	Az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely nem azonos az érintettel, az adatkezelővel, az adatfeldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére felhatalmazást kaptak.
Harmadik ország	Minden olyan állam, amely nem tagja az Európai Gazdasági Térségnek (EGT). i
Hitelesség	Az adat tulajdonsága, amely arra vonatkozik, hogy az adat bizonyítottan vagy bizonyíthatóan az elvárt forrásból származik.
Hozzájárulás	Az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez.
Illetéktelen személy	Olyan személy, aki nem az Társaság alkalmazásában áll, illetve olyan külsős felhasználó, akinek az adott bizalmas információ tekintetében - jogosultsági szempontból - legális hozzáférési lehetősége nincs, illetve nem biztosított, valamint aki az intézményi vagyontárgy kezelésével nincsen megbízva.
Információ	Információnak nevezünk mindent, amit a rendelkezésünkre álló adatokból nyerünk. Bizonyos tényekről, tárgyakról vagy jelenségekről hozzáférhető formában megadott megfigyelés, tapasztalat vagy ismeret, amely valakinek a tudását, ismeretkészletét, annak rendezettségét megváltoztatja, átalakítja, alapvetően befolyásolja, bizonytalanságát csökkenti vagy megszünteti.
Információbiztonság	Az információ minden formájának, és az azt kezelő infrastruktúra, és az információszolgáltatás védelme. Bővebb az informatikai biztonság fogalmánál, mivel elektronikus információk mellett az információ minden megjelenési formájára vonatkozik.
Információbiztonsági program	Az információbiztonsági kockázatok csökkentésére tervezett intézkedések összehangolt megvalósítási terve, mely felelőshöz és határidőhöz rendelten tartalmazza az intézkedéseket, az elvárt célokat, a célok mérési módszerét.
Információbiztonsági stratégia	A biztonsági célok, alapelvek és a Társaság vezetői elkötelezettségének bemutatása az Informatikai Biztonsági Szabályzatban (továbbiakban IBSZ) meghatározott biztonsági feladatok irányítására és támogatására.
Információs vagyontárgy	Ez a kifejezés általánosságban jeleníti meg azon információk tömegét, amelyre egy szervezetnek szüksége van küldetésének eléréséhez és feladatainak elvégzéséhez. Az információ a nem materiális javak közé tartozik és elkülönül az őt hordozó médiától.
Információvédelem	Az informatikai rendszerekben kezelt adatok által hordozott információk bizalmasságának, hitelességének és sértetlenségének védelme.
Informatikai biztonság	Az informatikai biztonság a védelmi rendszer olyan, a szervezet számára kielégítő mértékű állapota, amely az informatikai rendszerekben kezelt adatok bizalmassága, hitelessége, sértetlensége és rendelkezésre állása, illetve a rendszerelemek rendelkezésre állása és funkcionalitása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos.

Informatikai Biztonsági Irányítási Rendszer / Biztonság felügyelet	Rendeltetése az informatikai rendszerek által kezelt adatok bizalmasságának, hitelességének és sértetlenségének védelmének, kialakítás az adatvédelmi osztályonként specifikus biztonsági követelmények meghatározásán és a biztonsági események monitorozásán, vizsgálatán keresztül. Az informatika biztonsággal kapcsolatos szakfeladatokat az IBF munkatárs végzi.
Informatikai vezető	Megtervezi, vezeti, koordinálja és ellenőrzi a számítástechnikai, informatikai szolgáltatásokat, valamint a szervezeten belüli kommunikációs, távközlési és egyéb adatkommunikációs, hálózati szolgáltatásokat, infrastrukturális rendszereket, ide értünk minden – az informatikai- vagy telekommunikációs szakterületen - vezető beosztású személyt, függetlenül a vezetői szinttől, melyet a szervezetnél képvisel.
Intézkedés	A kockázatkezelés eszközei, beleértve a szabályzatokat, eljárásokat, irányelveket, gyakorlatokat, képzést vagy egyéb intézkedést, amelyek lehetnek adminisztratív, műszaki, irányítási vagy jogi természetűek. Az intézkedést a kontroll, a biztonsági ellenintézkedés vagy válaszlépés szinonimájaként is használják.
Jogosultságkezelés	A személyes adatokhoz, informatikai rendszerekhez vagy egyéb erőforrásokhoz való hozzáférés kezelésének folyamata és módszere, beleértve különösen a jóváhagyásokat, szerepköröket, összeférhetetlenségi kontrollokat.
Kezelési utasítások	Az iratokhoz a kiadmányozó döntése alapján az alábbi kezelési utasítások alkalmazhatók: – „Saját kezű felbontásra!”, – „Más szervnek nem adható át!”, – „Nem másolható!”, – „Kivonat nem készíthető!”, – „Elolvasás után visszaküldendő!”, – „Zárt borítékban tárolandó!” (a kezelésére vonatkozó utasítások megjelölésével.), – valamint más, az adathordozó sajátosságától függő egyéb szükséges utasítás.
Kockázat	A Társaság céljainak elérését veszélyeztető bizonytalanság és annak hatása. A működési kockázatokat minőségi és mennyiségi skálán is lehet értékelni. A negatív kockázat meghatározható egy fenyegetés bekövetkezése gyakoriságának (bekövetkezési valószínűségének) és az ez által okozott kár nagyságának a függvényével.
Kockázatelemzés	Információ módszeres felhasználása az erőforrások azonosítására és a kockázat becslésére. Az elektronikus információs rendszer értékének, sérülékenységének (gyenge pontjainak), fenyegetéseinek, a várható károknak és ezek gyakoriságának felmérése útján a kockázatok feltárása és értékelése.
Kockázatkezelés	Összehangolt tevékenységek a szervezet kockázati szempontból történő irányítására és ellenőrzésére. A kockázatkezelés rendszerint magában foglalja a kockázatfelmérést (azonosítás és becslés, értékelés), a kockázatjavítást (kockázatok csökkentése intézkedések által), a kockázatelfogadást (ld. maradványkockázat) a kockázatok nyomon követését, és a kockázatokra vonatkozó tájékoztatás megtételét.
Kockázattal arányos védelem	A kockázatokkal arányos a védelem, ha egy kellően nagy időintervallumban a védelem költségei arányosak a potenciális kárértékkel.
Különleges adat	Az Info tv. értelmében különleges adatnak minősül a személyes adatok különleges kategóriáiba tartozó minden adat, azaz a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre

	vagy szakszervezeti tagságra utaló személyes adatok, valamint a genetikai adatok, a természetes személyek egyedi azonosítását célzó biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok.
Magatartási kódex	A GDPR 40. cikke alapján a GDPR rendelkezései hatékony és helyes alkalmazásának az elősegítése érdekében létrehozott, és az esettől függően a Nemzeti Adatvédelmi- és Információszabadság Hatóság vagy az Európai Bizottság által jóváhagyott előírások összessége, amely figyelembe veszi az ágazaton belüli adatkezelés sajátosságait.
Megbízható működés	Az informatikai rendszerek, és az általuk kezelt adatok által hordozott információk rendelkezésre állásának és funkcionalitásának védelme.
Minősítés	Az a döntés, amelynek meghozatala során az arra felhatalmazott személy megállapítja, hogy egy adat megfelel a minősítési kategóriák egyikénél felsorolt valamennyi feltételnek, és megállapítja a minősítési jelölést.
Minősítési jelölés	Az adathordozón, illetve iraton elhelyezett, annak információvédelmi minősítése feltüntetésére szolgáló (szöveges) jelzés.
Minősített adat	– **külföldi minősített adat** megjelenési formájától függetlenül az Európai Unió valamennyi intézménye és szerve, továbbá az Európai Unió képviseletében eljáró tagállam, a külföldi részes fél vagy nemzetközi Társaság által készített és törvényben kihirdetett nemzetközi szerződés vagy megállapodás alapján átadott olyan adat, amelyhez történő hozzáférést az Európai Unió intézményei és szervei, az Európai Unió képviseletében eljáró tagállam, más állam vagy külföldi részes fél, illetve nemzetközi Társaság minősítés keretében korlátozza.
	– **nemzeti minősített adat** a minősítéssel védhető közérdekek körébe tartozó, a minősítési jelölést a Mavtv.-ben, valamint a Mavtv. felhatalmazása alapján kiadott jogszabályokban meghatározott formai követelményeknek megfelelően tartalmazó olyan adat, amelyről – a megjelenési formájától függetlenül – a minősítő a minősítési eljárás során megállapította, hogy az érvényességi időn belüli nyilvánosságra hozatala, jogosulatlan megszerzése, módosítása vagy felhasználása, illetéktelen személy részére hozzáférhetővé, valamint az arra jogosult részére hozzáférhetetlenné tétele a minősítéssel védhető közérdekek közül bármelyiket közvetlenül sérti vagy veszélyezteti (a továbbiakban együtt károsítja), és tartalmára tekintettel annak nyilvánosságát és megismerhetőségét a minősítés keretében korlátozza.
Munkavégzésre irányuló jogviszony	A munkaviszony, a munkavégzési kötelezettséggel járó szövetkezeti tagsági viszony, a vállalkozási és megbízási szerződés, a gazdasági társaság vezető tisztségviselői vagy felügyelő bizottsági tagsági tevékenység ellátására irányuló jogviszony és az egyéni vállalkozás.
Nyilvánosságra hozatal	Minősített adatnak a titokbirtokos hatásköréből kikerülő, meghatározhatatlan körben, mindenki részére biztosított megismerhetővé, hozzáférhetővé tétele.
Nyilvántartási rendszer	A személyes adatok bármely módon – centralizált, decentralizált vagy funkcionális vagy földrajzi szempontok szerint – tagolt állománya, amely meghatározott ismérvek alapján hozzáférhető, amely lehet elsődleges nyilvántartási és származtatott nyilvántartási rendszer.
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.
Rendelkezésre állás	Az informatikai rendszerelem – ideértve az adatot is – tulajdonsága, amely arra vonatkozik, hogy az informatikai rendszerelem az arra jogosult számára a szükséges időben és időtartamra használható.
Rendszergazda	Rendszergazdának nevezzük azt a szükséges számítástechnikai ismeretekkel rendelkező személyt, akit ezzel a feladattal az informatikai rendszert használó illetékes szervezeti egység, vagy a felhatalmazott szervezeti egység vezetője írásban megbíz. A rendszergazda végzi az informatikai rendszer hardver és szoftver karbantartását, fejlesztését, hibáinak feltárását és – ha lehetséges – javítását.
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.
Személyazonosító adat	A személyes adatok közül azok, amelyek szükségesek és elégségesek egy természetes személy más természetes személytől való egyértelmű megkülönböztetésére (azonosítására), melyen belül megkülönböztetünk természetes és egyéb személyazonosító adatokat.
Személyes adat	Azonosított vagy azonosítható természetes személyre („érintett”) vonatkozó bármely információ.
Tárolási hely	Az a fizikai hely, ahol az adat rendeltetésszerűen fellelhető, ahol az tárolása, őrzése megvalósul.
Teljes körű védelem	Teljes körű a védelem, ha az az informatikai rendszer összes elemére kiterjed.
Természetes személyazonosító adatok	A személyazonosító jel helyébe lépő azonosítási módokról és az azonosító kódok használatáról szóló 1996. évi XX. törvény 4. § (4) bekezdése szerinti adatok (az érintett családi és utóneve, születési családi és utóneve, születési helye, születési ideje és anyja születési családi és utóneve).
Titkosítás	Az adatok olyan transzformációja, melynek során az adat értelmezhetetlenné válik a megfelelő kulcs ismerete nélkül.
Titokbirtokos	Az a személy, aki felelős az adott bizalmas adat (a vonatkozó jogszabályok értelmében személyes adat vagy üzleti titok) titkosításáért.
Titoktartási kötelezettség	A munkavállalók, valamint a szervezettel munkavégzésre irányuló egyéb jogviszonyban álló magánszemélyek és szervezet alkalmazottainak azon kötelezettsége, hogy a munkavégzés során tudomásukra jutott üzleti titkot, bizalmas információt a jogviszony fennállása alatt és után is megőrzik.
Törlés	Az adat felismerhetetlenné tétele oly módon, hogy a helyreállítása a továbbiakban már nem lehetséges, amely megvalósulhat adat szintjén, adatcsoport szintjén, egy személyhez kapcsolódó valamennyi adat szintjén, adatbázis/nyilvántartási rendszer része vagy egésze szintjén. A törlés célja megvalósítható deperszonalizálással (anonimizálással) [(37) bekezdés] is.

Üzleti titok (védett ismeret) (az üzleti titok védelméről szóló 2018. évi LIV. törvény)	1. § (1) Üzleti titok a gazdasági tevékenységhez kapcsolódó, titkos – egészben, vagy elemeinek összességeként nem közismert vagy az érintett gazdasági tevékenységet végző személyek számára nem könnyen hozzáférhető –, ennélfogva vagyoni értékkel bíró olyan tény, tájékoztatás, egyéb adat és az azokból készült összeállítás, amelynek a titokban tartása érdekében a titok jogosultja az adott helyzetben általában elvárható magatartást tanúsítja. 2 Védett ismeret (know-how) az üzleti titoknak minősülő, azonosításra alkalmas módon rögzített, műszaki, gazdasági vagy szervezési ismeret, megoldás, tapasztalat vagy ezek összeállítása.
	Jelen dokumentumban az „Üzleti titok” minősítés a partner cég/szervezet üzleti titkára utal. A Társaság üzleti titkot képező adatai „KIEMELT” minősítés alatt szerepelnek (ez utóbbi meghatározását lásd később).
Zárt védelem	Zárt a védelem, ha az az összes releváns fenyegetést figyelembe veszi.

Rövidítés	**Magyarázat / Leírás**
NIST	National Institute of Standards and Technology
CVSS	Common Vulnerability Scoring System

4. Adatkezelés általános szabályai

4.1. Adatok érzékenységének besorolása

A Társaságnál kezelt és tárolt adatok érzékenységük mértékétől függően az alábbi csoportok valamelyikébe sorolhatók be:

a) **„NYILVÁNOS” (1. biztonsági osztályba)** lehet sorolni a közérdekű gazdasági és egyéb adatokat.
b) **„ALAP” (2. biztonsági osztályba)** lehet sorolni a szervezeti és nyílt, a tevékenységhez, működéshez tartozó adatokat.
c) **„FOKOZOTT” (3. biztonsági osztály)** olyan adatokat tartalmazzon, amelyek a Társaság mindennapi feladataihoz szükségesek, azaz belső adatnak számítanak. Ide tartoznak a Társaság napi normál tevékenységéhez tartozó adatok, a Társaság egyéb belső szabályozásában hozzáférés-korlátozás alá eső (pl. egyes feladatok végrehajtása érdekében bizalmas), valamint a nagy tömegű személyes adatok.
d) **„KIEMELT” (4.-5. biztonsági osztályba)** kell sorolni az üzleti titkot, valamint a különleges személyes adatokat.

Minden be nem sorolt adatot **„FOKOZOTT”** biztonsági osztályba soroltnak kell tekinteni a tényleges besorolás megtörténtéig.

A **"FOKOZOTT”** vagy **„KIEMELT”** védelmi osztályba sorolt adat, dokumentum, információ akár a jog által védelemben részesített is lehet, így azok védelmére büntetőjogi, polgári jogi és munkajogi szabályok is vonatkozhatnak.

4.2. Személyi követelmények

4.2.1. Adatvédelmi tevékenység ellátásában résztvevők

Az adatvédelmi tevékenység irányításában és ellátásában a Társaságnál a Vezetői Fórum tagjai vesznek rész.

4.2.2. Irányítás

Információbiztonsággal foglalkozó Vezetői Fórum

A Társaság Vezérigazgatója hívja össze az Információbiztonsági Vezetői Fórumot, amelynek feladata az információbiztonsági (beleértve az adatvédelmet is) feladatok és tevékenységek áttekintése, az adatgazdák kijelölése és a kijelölések felülvizsgálata.

Az adatvagyonnal kapcsolatosan a szerepek és felelősségek felülvizsgálatát évenként vagy változáskor, minden esetben (pl.: új rendszer- vagy meglévő rendszer új moduljának bevezetése, fejlesztése) végre kell hajtani.

Ki kell jelölni az új rendszerekhez, funkciókhoz tartozó adatgazdákat, valamint ezzel párhuzamosan, szükség szerint módosítani a meglévő kijelöléseket.

Az Információbiztonsági Vezetői Fórum fő feladatai az adatvédelemmel összefüggésben az Információbiztonság területén adatvédelmi szempontból alkalmazandó rendszerek, szakértők és adatgazdák kijelölése, kijelölések felülvizsgálata.

Információbiztonsági Vezetői Fórum állandó tagjai

a) Vezérigazgató
b) Informatikai vezető
c) Kereskedelmi vezérigazgató-helyettes
d) Biztonsági vezető
e) IBF
f) DPO
g) Adatgazdák

Információbiztonsági Vezetői Fórum meghívott tagjai

a) Rendszergazda
b) Belső ellenőr

A fórum évente, illetve jelentősebb információ biztonsági változások és incidensek esetén ülésezik az Informatikai vezető moderálásával, állandó és meghívott tagokkal.

Vezérigazgató

Az információbiztonsági Társaság és azon belül az adatvédelem személyi és tárgyi kialakításáért, biztosításáért, illetve azzal kapcsolatos alapkövetelmények megfogalmazásáért a Társaság Vezérigazgatója a felelős.

Informatikai vezető

A stratégia szerint kitűzött beszerzések és fejlesztések adatvédelmi-, valamint biztonsági követelményeinek betartatásáért felelős a rendszerek teljes életciklusa során.

Adatgazda

Az adatgazda **felméri és minősíti** a szabályzatban foglaltak alapján azokat **az adatköröket**, amelyeket az általa képviselt szervezeti egység kezel (létrehoz, rögzít, felhasznál stb.), meghatározza az adatkörrel kapcsolatban az adatkezelés módját (beleértve a felhasznált informatikai rendszert), meghozza a vonatkozó döntéseket (például biztonsági besorolások).

Az adatgazda az adatkörök felmérésekor és biztonsági osztályba történő besorolásuk során egyeztethet az adatkörben érintett belső folyamatfelelősökkel (vagy szakértőkkel, funkciógazdákkal, kulcsfelhasználókkal), továbbá az adatkört feldolgozó informatikai rendszer alkalmazás-, valamint rendszergazdájával és az Adatvédelmi tisztviselővel.

Az adatgazda az adatkör **felméréssel és minősítéssel kapcsolatos tevékenységet delegálhatja** az általa kijelölt folyamatfelelősnek az összeférhetetlenségi szabályok figyelembe vételével (vagy szakértőnek, kulcsfelhasználónak), de az adatkörök biztonsági besorolása (minősítése) csak az ***adatgazda jóváhagyásával*** tekinthető véglegesnek, mivel az adatgazda felelős a hozzárendelt adatvagyon kezeléséért, az azokhoz történő hozzáférés szabályainak jóváhagyásáért, betartatásáért és az elszámoltathatóságáért.

Rendszergazda

A **rendszergazda a hatáskörébe rendelt rendszerek, alkalmazások tekintetében**

a) Ellátja a rendszerek felügyeletét,
b) Elvégzi az üzemeltetési feladatokat,
c) Biztosítja a rendszerek rendelkezésre állását, valamint
d) Beállítja a rendszerekben a jóváhagyott jogosultságokat (amennyiben az alkalmazás erre nem biztosít lehetőséget az alkalmazásgazdának),
e) Technológiailag kikényszeríti az adatgazda által támasztott védelmi intézkedéseket.

Az adatvagyon felmérés során információt szolgáltat(hat) az adott alkalmazásban, rendszerben kezelt adatokról (adatkörökről, adatcsoportokról), a rendszerekben végzett adatkezelés technikai, fizikai jellemzőiről, a tárolás, mentés (archiválás) módjáról és helyéről.

Adatvédelmi tisztviselő (DPO)

Az Adatvédelmi tisztviselő a hatáskörébe tartozó személyes adatokat tartalmazó adatkörökre vonatkozóan **támogatást nyújt a besorolás végrehajtásában**. Az adatvédelmi tisztviselő véleményének kikéréséhez olyan dokumentumot/leírást kell benyújtani hozzá, amely kellő részletességgel meghatározza az adatkezelés célját, az adatkezelés jogalapját, a kezelendő adatok körét, az adatkezelés egyéb feltételeit.

Az adatvédelmi tisztviselő nyilvántartást vezet:

a) a hozzájárulásokról,
b) az érintettek tájékoztatásáról,
c) az adatkezelésekről,
d) az adatvédelmi incidensekről.

Az adatvédelmi tisztviselő tárolja:

a) a végrehajtott hatásvizsgálatok,
b) a jogos érdeken alapuló adatkezelések érdekmérlegelési tesztjeinek dokumentációját.

Az Adatvédelmi tisztviselő szerepkör összeférhetetlen a fenti (folyamatfelelősei rendszergazdai, valamint az IBF) szerepkörökkel.

Információbiztonsági Felelős (IBF)

Az IBF feladata az adatok jogosulatlan megszerzése, módosítása és tönkretétele elleni műszaki és szervezési intézkedések és eljárási szabályok rendszerének (biztonsági kontroll környezet) feletti kontroll ellenőrzésének kialakítása. Az IBF – az adatvagyon leltár összeállítása során – támogatást nyújt az adatgazdáknak, folyamatfelelősöknek vagy alkalmazásgazdáknak az adatkörökkel kapcsolatos minősítési/előminősítési folyamatban, és felel az adatköri besorolás véleményezéséért, továbbá javaslatokat tehet a biztonság hatékony javítása érdekében és az adatvédelmi és adatbiztonsági szabályzatok módosítására.

Az IBF szerepkör összeférhetetlen a fenti (funkciógazdai, folyamatfelelősi, alkalmazásgazdai, rendszergazdai, valamint Adatvédelmi tisztviselő) szerepkörökkel.

Az adatvédelem és az Információbiztonság területén gondoskodni kell a hatályos jogszabályoknak megfelelő működésről, ennek érdekében pontosan meg kell határozni minden munkakörhöz, hogy milyen jogok, kötelezettségek és felelősségi körök kapcsolódnak hozzá, melyet rögzíteni kell a munkaköri leírás részeként.

Biztosítani kell a fentieken túl azt is, hogy az adatmentéssel kapcsolatos munkakört csak olyan személyek tölthessék be, akiknek a munkakör betöltéséhez szükséges befolyásmentességet és szakértelmet szakmai gyakorlattal, végzettséggel és szakképesítéssel igazolta.

Kommunikációért felelős vezető

a) adatvédelmi incidens esetén közreműködik az érintettek tájékoztatásának módjáról és a tájékoztatás tartalmáról való döntés előkészítésében,
b) adatvédelmi incidens esetén – az adatvédelmi tisztviselő közreműködésével – szükség esetén sajtóközleményt bocsát ki és kizárólagos kapcsolatot tart a sajtó képviselőivel.

A Társaság adatvédelmi kérdésekben eljáró jogi képviselője (a továbbiakban: a Társaság Jogi képviselője)

a) szakmai támogatást nyújt az adatkezeléssel összefüggő, nem adatvédelmi jogszabályok értelmezésében;
b) véleményezi az adatvédelmi tisztviselő hatáskörébe tartozó egyes döntések tervezeteit;
c) biztosítja a Társaság képviseletét az érintett által a Társaság ellen az érintett adatvédelmi jogainak megsértése miatt indított, illetve a Társaság által a Nemzeti Adatvédelmi és Információszabadság Hatóság határozatainak felülvizsgálata iránt indított perekben.

Az adatvédelem és az Információbiztonság területén gondoskodni kell a hatályos jogszabályoknak megfelelő működésről, ennek érdekében pontosan meg kell határozni minden munkakörhöz, hogy milyen jogok, kötelezettségek és felelősségi körök kapcsolódnak hozzá, melyet rögzíteni kell a munkaköri leírás részeként.

Biztosítani kell a fentieken túl azt is, hogy az adatmentéssel kapcsolatos munkakört csak olyan személyek tölthessék be, akiknek a munkakör betöltéséhez szükséges befolyásmentességet és szakértelmet szakmai gyakorlattal, végzettséggel és szakképesítéssel igazolta.

4.3. Dokumentálási kötelezettség

A Társaság felelős a személyes adatok kezelésére vonatkozó alapelvek [GDPR 5. cikk (1) bek.] betartásáért.

A Társaságnak képesnek kell lennie a személyes adatok kezelésére vonatkozó alapelvek betartásának igazolására. A megfelelőség igazolása különösen az adatkezeléshez kapcsolódó döntéseket megalapozó körülmények és a döntések, az érintetteknek szóló tájékoztatások és nyilatkozatok, az érintettől származó nyilatkozatok, továbbá a személyes adatokat tartalmazó (elektronikus vagy papír alapú) dokumentumok szervezeten belüli vagy azon kívüli mozgásának megfelelő dokumentálásával történik.

4.3.1. Adatkezelés bevezetése, módosítása, megszüntetése

A Társaság az adatkezelést érintő minden tevékenységről, beleértve az adatkezelés megkezdésére, megváltoztatására irányuló bármely igényt, szándékot, az adatkezelést érintő valamennyi döntést írásban, dokumentálható és visszakereshető formában rögzíti és tárolja. Ennek során rögzíteni kell az adatkezelés megkezdésére és megváltoztatására irányuló igény, szándék felmerülésének, valamint az adatkezelést érintő valamennyi és bármely döntés, illetve az adatkezelést érintő minden további tevékenység időpontját, célját és annak a szakterületnek és a szakterület adatgazdájának a megnevezését, amely szakterületen az adott igény felmerült, illetve aki az adott döntést meghozta.

Amennyiben adatkezelésre érdekmérlegelési teszt elvégzését követően jogos érdek alapján kerül sor, a Társaság írásban, dokumentálható és visszakereshető formában rögzíti és eredményét és az arról készült egyéb dokumentációt.

Amennyiben adatkezelésre hatásvizsgálat elvégzését követően kerül sor, a Társaság írásban, dokumentálható és visszakereshető formában rögzíti és tárolja a hatásvizsgálat megállapításait, eredményét és az arról készült egyéb dokumentációt.

4.3.2. Hozzájárulások dokumentálása és tárolása

A Társaságnak képesnek kell lennie annak igazolására, hogy az érintett a személyes adatainak kezeléséhez hozzájárult. Ennek érdekében az érintetteknek a Társaság egyes adatkezelési tevékenységeihez hozzájáruló valamennyi – írásban, online felületen, elektronikus üzenet, illetve videóchat útján és egyéb úton tett – nyilatkozatát, továbbá a Társaság minden ezzel kapcsolatos nyilatkozatát a Társaság dokumentálható és visszakereshető formában rögzíti, nyilvántartja és tárolja. Amennyiben a hozzájárulás megadására szóban telefonos úton került sor, úgy a Társaság köteles az érintett e módon tett nyilatkozatát hangfelvétel útján rögzíteni, illetve a rögzített hangfelvételt dokumentálható és visszakereshető formában nyilvántartani, valamint tárolni. A hozzájáruló nyilatkozatok fentiek szerinti dokumentálásának és tárolásának részletes szabályait az adott tevékenységet szabályozó belső szabályozók tartalmazzák.

Amennyiben az adatkezelés jogalapja az érintett hozzájárulása, úgy a hozzájárulás visszavonása esetén a Társaság a hozzájárulás alapján kezelt adatokat a GDPR 17. cikke figyelembevételével törli.

4.3.3. Érintettek tájékoztatásának dokumentálása

A Társaság megfelelő intézkedéseket hoz annak érdekében, hogy az érintett részére a személyes adatok kezelésére vonatkozó valamennyi szükséges információt és minden egyes tájékoztatást tömör, átlátható, érthető és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva nyújtsa, különösen a gyermekeknek címzett bármely információ esetében.

Az érintettnek címzett tájékoztatás megtörténtét és annak az érintett általi megismerését dokumentálható és visszakereshető formában rögzíteni kell.

4.3.4. Adatkezelések nyilvántartása

A DPO valamennyi adatkezelési tevékenységéről és adatfeldolgozási tevékenységéről elektronikus formában nyilvántartást vezet.

4.3.5. Érdekmérlegelési teszt elvégzésének módszertana

Jogos érdek az a törvényes, kellően pontosan megfogalmazott, valós és fennálló, illetve elérhető előny, amelyet az adatkezelő származtat – vagy a társadalom származtathat – az adatkezelésből.

Érdekmérlegelési tesztet kell elvégezni, ha a tervezett adatkezelés jogalapja jogos érdek. Az érdekmérlegelési tesztet a tervezett adatkezelésért felelős adatgazda végzi el a DPO bevonásával. Az érdekmérlegelési tesztet írásban kell elvégezni. Az elkészült dokumentumot az Adatvédelmi tisztviselőnek kell megküldeni, aki azt szakmai szempontból véleményezi. A jogos érdeken alapuló adatkezelés kizárólag az érdekmérlegelési teszt elvégzését és az adatvédelmi tisztviselő véleményének beszerzését követően kezdhető meg.

A teszt módszertanát, a megválaszolandó kérdéseket minden esetben a tervezett adatkezelés figyelembevételével kell megválasztani, a kérdések köre csak orientáló, a tervezett adatkezelés szempontjából releváns egyéb kérdésekkel bővíthető. Abból kell kiindulni, hogy bármilyen adatkezelés beavatkozás az érintett magánszférájába és e beavatkozás jogosságát, szükségességét és arányosságát kell bizonyítani.

4.3.6. Adatvédelmi hatásvizsgálat elvégzésének módszertana

Ha az adatkezelés valamely, különösen új technológiákat alkalmazó típusa valószínűsíthetően magas kockázattal jár a természetes személyek jogaira nézve, az adatkezelést megelőzően hatásvizsgálatot kell végezni. Olyan egymással hasonló típusú adatkezelési műveletek, amelyek egymáshoz hasonló kockázatokat jelentenek, egyetlen adatvédelmi hatásvizsgálat (továbbiakban hatásvizsgálat) keretei között is értékelhetők.

A hatásvizsgálat elvégzésének szükségességéről a tervezett adatkezelésért felelős adatgazda szükség esetén kikéri az adatvédelmi tisztviselő véleményét.

A hatásvizsgálat elvégzését a tervezett adatkezelésért felelős adatgazda koordinálja. A hatásvizsgálat megállapításait írásban kell rögzíteni. Az elkészült hatásvizsgálati dokumentációt az Adatvédelmi tisztviselőnek kell megküldeni, amely azt szakmai szempontból véleményezi és beszerzi az Informatikai vezető véleményét is. Ha az adatgazda úgy ítéli meg, hogy az adatkezelés nem jár magas kockázattal, úgy meg kell indokolnia és dokumentumokkal igazolnia a mellőzés okait. A bevezetendő adatkezelés kizárólag a hatásvizsgálat elvégzését követően kezdhető meg.

4.4. Érintettől származó kérelmek, panaszok megválaszolásának rendje

4.4.1. Adatvédelmi bejelentések típusai

Az érintettől a következő, személyes adatai a Társaság általi kezelését érintő beadványok (a továbbiakban együtt: adatvédelmi bejelentések) érkezhetnek:

a) bejelentheti a Társaság által nyilvántartott adatok megváltozását,
b) tájékoztatást kérhet személyes adatai kezeléséről [milyen személyes adatokat milyen célból, milyen jogalapon, milyen forrásból szerezve meddig kezeli a Társaság, alkalmaz-e automatizált döntéshozatalt és/vagy profilalkotást az adatkezelés során, és a személyes adatokat kinek, milyen jogalapon továbbítja)] – hozzáféréshez való jog (GDPR 15. cikk),
c) kérheti pontatlanul nyilvántartott személyes adatai helyesbítését, illetve vitathatja a nyilvántartott személyes adatok pontosságát – helyesbítéshez való jog (GDPR 16. cikk),
d) kérheti nyilvántartott személyes adatai törlését – törléshez való jog (GDPR 17. cikk),
e) kérheti személyes adatai kezelésének korlátozását (a pontatlan adat helyesbítéséig terjedő időre; a jogellenesen kezelt személyes adatok törlése helyett; jogszerűen kezelt, de szükségtelenné vált adatok törlése helyett az érintett kérésére az érintett jogi igényének előterjesztéséhez, érvényesítéséhez vagy védelméhez; jogos érdeken alapuló adatkezelés elleni tiltakozás elbírálásáig) – az adatkezelés korlátozásához való jog (GDPR 18. cikk),
f) kérheti, hogy a rá vonatkozó, általa a Társaság rendelkezésére bocsátott és elektronikus adatbázisban kezelt adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja – adathordozhatósághoz való jog (GDPR 20. cikk),
g) tiltakozhat személyes adatai kezelése ellen, ha az adatkezelés jogalapja az adatkezelő vagy harmadik személy jogos érdeke (pl. direkt marketing célú adatkezelés), illetve közérdekű feladat vagy közfeladat ellátása, beleértve mindkét esetben a profilalkotást is – tiltakozási jog gyakorlása (GDPR 21. cikk),
h) automatizált döntéshozatal alkalmazása esetén az adatkezelő részéről emberi beavatkozást kérhet, közölheti álláspontját [GDPR 22. cikk (3) bek.],
i) kifogást nyújthat be az automatizált döntéshozatal alkalmazásával meghozott döntéssel szemben [GDPR 22. cikk (3) bek.],
j) az Adatvédelmi Tisztviselőhöz fordulhat a személyes adatok kezelését, illetve a GDPR szerinti jogai gyakorlását érintően [GDPR 38. cikk (4) bek.].

Adatvédelmi bejelentések előzetes vizsgálata

Az Adatvédelmi tisztviselő a beérkezett adatvédelmi bejelentéseket haladéktalanul megvizsgálja abból a szempontból, hogy az érintett kérte-e az adatkezelés korlátozását [zárolás, GDPR 18. cikk – 0e), és megalapozott kérés esetén az adatvédelmi tisztviselő intézkedik a Társaságnál annak az informatikai rendszerekben történő megvalósításáról. Az adatkezelés korlátozásának (zárolásának) feloldásáról az adatvédelmi tisztviselő külön tájékoztatja az érintett informatikai rendszereket üzemeltető szervezet egységeket.

Az Adatvédelmi tisztviselő a beérkezett bejelentéseket, kérelmeket megvizsgálja abból a szempontból, hogy egyértelműen megalapozatlan vagy túlzó-e, és javaslatot tesz a Vezérigazgatónak díj felszámítására vagy a kérelem elutasítására. A felszámítható díj mértékének

megállapításánál figyelembe veendő költségelemeket a Társaság Adatkezelési Tájékoztatója tartalmazza.

4.4.2. Adatvédelmi bejelentések kivizsgálása

Az adatvédelmi bejelentéseket Adatvédelmi Csoport – önállóan vagy a Társaság egyéb szervezeti egységeinek közreműködésével – kivizsgálja, illetve előkészíti az adatvédelmi tisztviselő válaszát vagy intézkedését:

a) az Informatikai vezető közreműködik az adatkezelés korlátozásának végrehajtásában, a válaszadáshoz szükséges személyes adatok különböző informatikai rendszerekből történő összegyűjtésében az IBF-fel együttműködve,
b) az Adatgazda az Adatvédelmi tisztviselő által meghatározott – legalább 5, sürgős esetben legalább 1 munkanapos – határidőn belül az Adatvédelmi tisztviselő rendelkezésére bocsátja az adatvédelmi bejelentés elbírálásához szükséges adatokat, információkat, felvilágosítást, magyarázatot, illetve az adatvédelmi tisztviselő által kért egyéb módon közreműködik a bejelentéssel kapcsolatos döntések előkészítésében,
c) az IT az Adatvédelmi tisztviselő rendelkezésének megfelelően elvégzi az adatkezelés korlátozását (zárolását), az adatok helyesbítését/módosítását, törlését.

4.4.3. Adathordozhatósághoz való jog gyakorlása

Az adathordozhatósághoz való jog gyakorlására irányuló kérelmet az érintett az erre szolgáló formanyomtatványon, e-mailben vagy az Adatkezelési Tájékoztatóban meghatározott módon nyújthat be.

Amennyiben az érintett nem az Adatkezelési Tájékoztatóban meghatározott módon nyújtja be az adathordozhatósághoz való jog gyakorlására irányuló kérelmét, az ilyen kérelmet fogadó szervezeti egység tájékoztatja az érintettet a megfelelő benyújtás szükségességéről és módjáról.

Az adathordozhatósághoz való jog gyakorlására irányuló kérelmet az Adatvédelmi tisztviselő – a kérelem beérkezését követő 3 munkanapon belül – átadja az Informatikai vezetőnek a szükséges adatok összegyűjtése és az abban való közreműködés céljából, hogy a kérelem teljesíthető-e, illetve mely adatokra nézve teljesíthető.

Amennyiben az adathordozhatósághoz való jog gyakorlására irányuló kérelem nem teljesíthető, az Adatvédelmi tisztviselő javaslatot tesz a kérelem elutasítására és erről a Társaságot tájékoztatja. Az adathordozhatóság részbeni teljesíthetősége esetén az Adatvédelmi tisztviselő a döntését a kiadható adatok rendelkezésre bocsátásával egyidejűleg közli a kérelmezővel.

4.5. Személyes adatot tartalmazó, papír alapú adathordozók nyilvántartása

Személyes adatot tartalmazó dokumentumnak a Társaságon belüli és azon kívüli továbbítását a hozzáféréshez való jogosultság nyomon követhetősége érdekében dokumentálni kell.

4.6. Elektronikus adathordozók kezelése

4.6.1. Adathordozók azonosítása

Az adathordozók kezelése, átadása és átvétele, valamint adminisztrációja a papíralapú és gépi adathordozókra egyaránt csak szabályozottan (nyomon követhetően) történhet, ezek megfelelőségét az IBF ellenőrizheti.

Valamennyi adathordozót, a tárolás során nyilvántartásba kell venni. A nyilvántartást napra készen kell vezetni, úgy, hogy a média tárolási helyszíne pontosan beazonosítható legyen.

Valamennyi adathordozót egységes azonosítással meg kell jelölni (minősítés, informatikai rendszer megnevezése /vagy tulajdonos személy/ a készítés időpontja, a készítő).

A védelem mértékét az adathordozók minősítésére tekintettel kell meghatározni, az adathordozókat védeni kell a jogosulatlan hozzáféréstől.

Évente média leltárt kell készíteni, az adatokat rögzíteni a nyilvántartásban (adatvagyon leltár) az Adatvagyon felmérési módszertan -ban foglaltaknak megfelelően.

A média leltár elkészítéséért az Informatikai vezető a felelős. A nyilvántartásnak minimálisan tartalmaznia kell:

a) Az adathordozó fizikai helyét (pl., személyhez kötött hordozható eszköz stb.)
b) Az adathordozó azonosítóját vagy iktatószámát
c) A tárolt adatok jellegét
d) A tárolt adatok érzékenységi besorolását

4.7. Adathordozók tárolása

Az eltávolítható adathordozók és fizikai eszközök tárolására – amennyiben ez lehetséges –a műszaki-, tűz- és vagyonvédelmi előírásoknak megfelelő helyiséget kell kijelölni, illetve kialakítani, ahol az eltávolítható adathordozókat és fizikai eszközöket káros külső hatásoktól védett (pl. por, nedvesség, napsugárzás stb.), kulccsal zárható szekrényben kell elhelyezni úgy, hogy tárolás közben ne sérüljenek vagy károsodjanak.

Az adathordozók tárolásánál az Infrastrukturális követelmények 4.7.2. pontban megfogalmazott követelményeknek kell megfelelni. A fentieken kívül rendszeresen ellenőrizni kell az adathordozók elöregedését is.

4.7.1. Adathordozók szállítása

Az eltávolítható adathordozók és fizikai eszközök szállítása közben az adatoknak, illetve maguknak a fizikai adathordozóknak a védelme érdekében fokozott figyelmet kell fordítani a megfelelő körülmények biztosítására.

Az adathordozók szállítása csak az Informatikai vezető által jóváhagyott szállítólevéllel lehetséges. A szállítólevélnek tartalmaznia kell a szállítást megrendelő/átadó, a szállítást kivitelező/átvevő megnevezését, az adathordozó megnevezését a szállítás időpontját, a jóváhagyó nevét, a jóváhagyás időpontját és a szállítás megtörténésének dátumát és az igazoló személy nevét. (1. Melléklet – Adathordozó mozgatása/megsemmisítése)

Az adathordozó szállításának nyilvántartását évente minimum egyszer ellenőrizni, az ellenőrzést dokumentálni kell.

Az épületen kívüli szállítás esetén a legrövidebb és leggyorsabb útvonalat kell választani.

Tömegközlekedési eszközön – lehetőség szerint – ne történjen az adathordozó szállítása.

Papíralapú adathordozók szállítása esetén biztosítani kell, hogy a szállítók ne férhessenek hozzá az adattárolók tartalmához.

Az adathordozókat tilos őrizetlenül hagyni.

4.7.2. Adatok és adathordozók megsemmisítése

Az adatok megsemmisítése az adatok elévülése, az adathordozó selejtezése vagy megsemmisítése, illetve törvényileg és/vagy rendeletileg meghatározott adattörlési kötelezettség miatt válhat szükségessé. Megsemmisítésük a következők szerint történik:

a) A papír alapú anyagok esetében iratmegsemmisítőt kell alkalmazni, úgy, hogy az adat abból ne legyen többé előállítható. Tárolási konténer alkalmazása esetén biztosítani kell, hogy a konténer biztonságosan le legyen zárva.
b) Az adatokat tartalmazó elektronikus médiákat úgy kell megsemmisíteni, hogy abból ne lehessen adatokat visszaállítani.
c) A megsemmisítéshez olyan biztonságos megsemmisítő, törlő programot kell alkalmazni, amelyet az iparág támogat, de megengedett más fizikai megsemmisítő eljárás is, például a demagnetizálás.

A selejtezendő anyagot helyben és szállításnál is védeni kell a jogosulatlan hozzáférés ellen. Amennyiben a megsemmisítendő adatokat tartalmazó adathordozók fizikailag is megsemmisítésre kerülnek, és a megsemmisítést külső, harmadik fél végzi, az adathordozók megsemmisítését mindenképpen meg kell előznie az adatok megsemmisítésének, ezzel biztosítva, hogy a megsemmisítendő adatok az adathordozók harmadik fél kezébe kerülése esetén semmilyen módon ne legyenek visszaállíthatóik. Az adatok megsemmisítéséről a sérült adathordozók esetén is gondoskodni kell!

Optikai vagy mágneses adathordozók (winchester, mágnesszalag) esetén az adatok megsemmisítését az Informatikai vezető végzi speciális, optikai adatmegsemmisítő berendezés vagy megfelelően erős mágneses terű eszköz segítségével.

Az adatok megsemmisítése után az adathordozó szükség esetén újra felhasználható, vagy amennyiben javíthatatlan fizikai károsodás érte, a megsemmisítéséről vagy újra hasznosításáról az Informatikai vezető gondoskodik.

Az adatmegsemmisítés tényéről minden esetben jegyzőkönyvet kell készíteni és amennyiben az adatmegsemmisítés törvényileg vagy rendeletileg előírt okokból történik, akkor tételesen meg kell jelennie a megsemmisített adatok listájának.

A megsemmisítés jóváhagyását az Informatikai vezető végzi el.

4.8. Adatmentés

A megtervezett mentési és visszaállítási eljárásokra üzemeltetési előírásokat kell készíteni, és azok betartását rendszeresen ellenőrizni kell.

A mentések nyilvántartását az előírásoknak megfelelően kell vezetni.

Az időszakos, archiválandó (pl. éves) mentéseket a jogszabályokban meghatározott ideig, de legalább tíz évig, bármikor visszakereshetően, helyreállíthatóan kell megőrizni.

A biztonsági mentéseket tartalmazó médiákat biztonságos helyen kell tárolni, amely lehet egy alternatív telephely vagy back-up helyszín. A biztonsági mentések tárolási helyére ugyanazok a biztonsági előírások vonatkoznak, mint az éles környezet egyéb fizikai helyszíneire.

A tárolási helyszín biztonságosságát legalább évente egyszer az Informatikai vezetőnek és az IBF-nek ellenőrizni kell, és azt dokumentálni kell.

4.8.1. Adatmentési stratégia kialakítása

Az Eszközök adatmentési stratégiáját az Informatikai vezető az eszközök üzemeltetőinek igénye alapján az üzletmenetfolytonossági terv (BCP), a katasztrófa utáni helyreállítási terv (DRP) és a rendelkezésre álló erőforrások együttes figyelembevételével alakítja ki és állíttatja be.
A kialakított és beállított adatmentési stratégiáról a mentésért felelős adminisztrátor minden esetben tájékoztatja a rendszergazdákat és üzemeltetésben résztvevőket.

4.8.2. Infrastrukturális követelmények

A mentett és archivált adatok tárolására szolgáló helyiségek fizikai védelmét biztosítani kell a jogosulatlan hozzáféréstől – lehetőleg a MABISZ és a Rendőrség ajánlásai szerint –, kizárva ezzel a jogosulatlan személyek bejutását; a belépésre jogosultak belépésének időpontját, tartózkodásának célját, időtartamát, kilépésének időpontját pedig naplóban kell rögzíteni.
Ugyancsak biztosítani kell a fizikai és környezeti biztonság komplex kezelését, amely magába foglalja az élet- és vagyonvédelem alábbi területeit is: tűz, árvíz, elárasztás, fizikai behatolás, áramellátás-kimaradás elleni megfelelő szintű védelem. A védelemnek az alkalmazások rendelkezésre állásának értékével, a hardver és a szoftver beszerzési értékével, az adatok pótlásának költségével kell arányban lennie.

A hibatűrő rendszerek üzemeltetése során biztosítani kell a karbantartó és üzemeltető személyzet rendszeres oktatását és továbbképzését olyan szinten, hogy az előírt kiesési időn belül meg tudják valósítani a rendszerek visszaállítását normál üzemállapotra. A szolgáltatás minőségének folyamatos javítása érdekében a hibajelenségeket utólagosan elemezni és értékelni kell tudnia az üzemeltetésnek.

4.8.3. Adatmentő rendszerek beállítása, üzemeltetése

A mentőrendszert az Informatikai vezető felelőssége úgy beállíttatni, hogy az Eszközök mentendő adatait a kialakított adatmentési stratégia szerint teljesen automatizált módon mentse.
Amennyiben az adott mentőrendszernél megoldható, az adatbiztonság növelése érdekében a mentőrendszert a mentésért felelős üzemeltetőnek úgy kell beállítania, hogy az adatmentések indulása előtt automatikusan ellenőrizze a sikeres mentés körülményeinek meglétét (mentőegység és média állapota, mentendő rendszer elérhetősége stb.), és annak eredményéről, vagy hiba esetén e-mailben tájékoztassa a mentésért felelős üzemeltetőt.

Az adatmentés eredményét a rendszergazdának rendszeresen ellenőriznie kell. Amennyiben lehetőség van, a mentőrendszert úgy beállítani, hogy az adatmentés eredményéről e-mailben küldjön jelentést a mentésért felelős üzemeltetőnek, a mentés eredményének ellenőrzése az e-mailben kapott jelentések átvizsgálását jelenti. Amennyiben ez a megoldás nem kivitelezhető, vagy a nagyszámú mentés miatt ennek gyakorlatban való alkalmazása nehézkes, a mentésért felelős üzemeltetőnek közvetlenül a naplóállományok átvizsgálásával kell meggyőződnie az adatmentés eredményéről.

Sikertelen adatmentés esetén a mentésért felelős üzemeltető feladata a hiba kivizsgálása, lehetőleg annak elhárítása vagy az elhárításra irányuló lépések megtétele, valamint az Informatikai vezető tájékoztatása az adatmentés sikertelenségéről, és a hibaelhárítás megtett és tervezendő lépéseiről.

A mentőegység médiáinak tárolásáért az Informatikai vezető felelős.

Az adat-visszaállítást – amennyiben lehetséges – a mentésért felelős üzemeltető minden esetben egy másik, ideiglenes vagy teszt rendszer erre a célra kijelölt területére végezze, ahonnét az Informatikai vezető megfelelő ellenőrzése és jóváhagyása után állíthatók vissza eredeti helyükre a mentett adatok.

Minden informatikai rendszer esetén évente legalább egyszeri alkalommal adat-visszatöltési tesztet kell végrehajtani, melyről jegyzőkönyvet kell készíteni.

5. Tranzakciós és személyes adatok kezelése

5.1. Tranzakciós és személyes adatok besorolása

Az általános adatkezelési elveknek megfelelően a Társaságnál kezelt, továbbított vagy tárolt adatok, illetve személyes adatok „**Titkos**” besorolású adatnak számítanak.

5.2. Tranzakciós és személyes adatokhoz való hozzáférés

Az éles adatkörnyezet felhasználói jogosultságait úgy kell kialakítani, hogy minden felhasználó - élő személyek és technikai felhasználók egyaránt – csak a munkakörükhöz, feladataik ellátásához feltétlenül szükséges mértékben férjenek hozzá az adatokhoz.

5.3. Tranzakciós és személyes adatok tárolása

Üzleti szempontból a felhasználó által megadott adatok esetében az adatok kezelésének célja a felhasználó jogosultságának azonosítása, valamint a megrendelt szolgáltatás teljesítésének lehetősége.

Az adott üzleti és jogi szabályozásoknak megfelelően, az adatok tárolása lehetséges a Társaság rendszereiben, lehetőleg titkosított formában. A minimális tárolási idő meghatározásának alapja a magyar törvényi szabályozás a tranzakciós adatok megőrzéséről, az MNB irányadó rendeletei és ajánlásai, illetve a nemzetközi szabványok erre vonatkozó rendelkezései.

Gondoskodni kell arról, hogy tranzakciós és személyes adatok csak olyan rendszerekben kerüljenek tárolásra, ahol ez elengedhetetlenül szükséges.

5.4. Tranzakciós és személyes adatok továbbítása nyílt hálózaton

A tranzakciós adatok és személyes adatokat nyilvános hálózaton keresztül (Internet, GSM, GPRS, Wifi) vagy eltávolítható adathordozón titkosított formában és módon lehet továbbítani.

A titkosítás megvalósítására több különféle módszer alkalmas, így pl.:

a) Titkosított csatorna pl. virtuális magánhálózat (VPN) kialakításával.
b) A küldött adatok titkosítása iparágilag elfogadott speciális titkosítási metódusok vagy protokollok segítségével (pl. SSL, TLS stb.).
c) A tranzakciós és személyes adatok titkosítása esetén a titkosító kulcsoknak az elfogadott iparági szabványnak megfelelő erősségűnek kell lennie. Kulcsok erősségének beállításakor figyelembe kell venni a gyártói ajánlásokat, és olyan beállításokat kell használni, amivel biztosítható a megfelelően erős titkosítás az adattovábbításhoz.

d) Gondoskodni kell arról, hogy az adattovábbítás során használt kulcsok és certificate-ek kizárólag hiteles és megbízható forrásból származzanak.
e) Titkosítatlan tranzakciós és személyes adatok küldése másoknak üzenetküldő rendszerben szigorúan tilos (e-mail, instant messaging, chat).
f) A titkosítás megvalósításakor biztosítani kell, hogy az implementált megoldás csak biztonságos konfigurációt támogasson és kizárja a nem biztonságos konfigurációk használatát (pl. ne lehessen MS-CHAPv2-s protokollt downgrade-elni CHAP-re).
g) SSL, TLS megoldások böngészőn keresztüli használata esetén biztosítani kell, hogy:
   ga) A HTTPS megjelenjen a böngésző URL-sávjában.
   gb) Tranzakciós és személyes adatok ne kerüljenek bekérésre és továbbításra, ha a HTTPS nem jelenik meg az URL-ben.
h) Vezeték nélküli hálózatban a titkosító kulcsoknak az elfogadott iparági szabvány által elfogadott megfelelő erősségűnek kell lennie.

5.5. Tranzakciós és személyes adatok megsemmisítése

Az éles környezetek esetében a tranzakciós adatok üzleti megőrzési ideje – amennyiben törvényi és/vagy rendeleti szabályozások másképp nem rendelkeznek – 8 év.

A tranzakciós adatokat – amennyiben lehetséges, automatikus eljárások keretében – negyedévente ellenőrizni kell.

6. Adatvédelmi incidensek kezelése

6.1. Adatvédelmi rendellenesség és adatvédelmi incidens elhatárolása

Adatvédelmi incidens csak akkor következik be, ha az adatbiztonsági intézkedések – akár vétlen, akár szándékos – megsértésének következtében megtörténik a személyes adatok véletlen vagy jogellenes megsemmisítése, elvesztése, megváltoztatása, jogosulatlan közlése vagy az azokhoz való jogosulatlan hozzáférés.

Adatvédelmi rendellenességnek minősül különösen:

a) a személyes adatok kezelésére vonatkozó adatbiztonsági intézkedések minden olyan – akár vétlen, akár szándékos – sérülése, megszegése, amely nem eredményezi a személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést, de ennek lehetősége fennáll,
b) a személyes adatok kezelésére vonatkozó adatbiztonsági intézkedéseken kívüli adatvédelmi szabályok megsértése, pl. személyes adatok megfelelő jogalap nélküli kezelése (felvétele, tárolása, továbbítása stb.), a szükségesnél több adat kezelése, a személyes adatoknak az adatmegőrzési határidőn túli kezelése. E pont alá tehát jogvitás esetek tartoznak, elbírálásukra a vizsgálandó eset, rendellenesség tárgyához igazodó hatályos jogszabályok rendelkezései vonatkoznak.

Az adatok véletlen vagy jogellenes megsemmisítésének az adatok – szabályszerű selejtezési, törlési eljáráson kívüli – helyreállíthatatlan megváltoztatása vagy az adatokat tartalmazó adathordozó – nem szabályos selejtezési eljárás során történt – fizikai megsemmisítése, használhatatlanná tétele

minősül. Az adat véletlen vagy jogellenes törlése akkor is adatvédelmi incidens, ha a törölt adatot, illetve a megsérült adathordozón lévő adatot úgy sikerül maradéktalanul helyreállítani, hogy az az érintett számára semmilyen következménnyel nem jár, azt nem is észleli.

Az adatok elvesztésének az adatoknak, illetve az adatot tartalmazó adathordozónak a Társaság birtokából való időleges vagy végleges kikerülése minősül, akkor is, ha a Társaság birtokába visszakerült adaton később semmilyen módosítás nem állapítható meg. A Társaság tulajdonát képező, személyes adatokat tartalmazó eszközök, adathordozók, illetve személyes adatokat tartalmazó információs rendszerek elérésére alkalmas eszközök eltulajdonítása is e körbe tartozik.

A fent leírtakat kell alkalmazni a Társaság tulajdonát képező adathordozókra, mobiltelefonra, laptopra, egyéb számítástechnikai eszközre, továbbá a Társaság alkalmazottainak olyan saját tulajdonú eszközeire (adathordozókra, mobiltelefonra, laptopra, egyéb számítástechnikai eszközre), amelyeket a munkavégzéshez, munkaköri feladatok ellátásához, hivatalos célból használhat.

Jogosulatlan közlésnek az adatoknak olyan harmadik személy tudomására hozása minősül (akár szóban, akár írásban, elektronikus vagy bármely más úton), aki az adatokat nem ismerhette volna meg (pl. egy ügyfél adatainak egy másik ügyféllel való közlése a nem kellő azonosítás miatt). E bekezdés alkalmazása szempontjából harmadik személy a Társaság azon alkalmazottja is, aki a munkaköre és az ellátott feladatokat szabályozó belső szabályozók alapján nem jogosult a kérdéses adatot megismerni, vagy feladata ellátásához az ilyen adat nem szükséges.

Jogosulatlan hozzáférésnek minősül minden olyan eset, amikor arra nem jogosult személyek – nekik címzett közlés nélkül is – megismerik a személyes adatot (pl. személyes adatot tartalmazó dokumentum felügyelet nélkül hagyása, vagy más által is látható módon történő elhelyezése ügyféltérben, más személy személyes adatainak megjelenítése nyilvános internetes felületen stb.)

Az információbiztonsági incidens – az Incidenskezelési Szabályzatnak megfelelően - adatvédelmi incidensnek vagy adatvédelmi rendellenességnek is minősül, amennyiben személyes adatokra nézve következik be.

6.2. Adatvédelmi esemény bejelentése

Személyes adat véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést vagy ezek közvetlen veszélyének fennállását a tudomásra jutást követően az Adatvédelmi Tisztviselő részére haladéktalanul köteles bejelenteni:

a) az IBF, információbiztonsági bejelentés esetén,
b) az Informatikai vezető, incidens bejelentése esetén,
c) a Társaság adatvédelmi eseményt észlelő alkalmazottja, az első két pont alá nem eső adatvédelmi esemény esetén. a.

Adatvédelmi eseményre utaló bejelentés érkezhet:

a) a Társaság ügyfeleitől vagy más személytől,
b) a Társasággal szerződéses kapcsolatban álló adatkezelőtől,

c) a Társasággal közös adatkezelőnek minősülő másik adatkezelő kapcsolattartójától, valamint a Társaság adatfeldolgozójának képviselőjétől.

A közös adatkezelésről szóló szerződésben, illetve az adatfeldolgozóval kötendő szerződésben egyértelműen rendelkezni kell a másik adatkezelő, illetve az adatfeldolgozó azon kötelezettségéről, hogy az adatvédelmi incidensről a Társaság adatvédelmi tisztviselőjét köteles haladéktalanul, de legkésőbb az észlelést követő 24 órán belül értesíteni a szerződésben meghatározott csatornákon.

A bejelentésben meg kell adni:

a) bejelentő neve, beosztása, szervezeti egysége, szervezet neve, elérhetősége,
b) az észlelt adatvédelmi rendellenesség/incidens rövid leírása, jellege (eszköz elvesztése/ellopása, rosszindulatú program, rendszer feltörése stb.),
c) az adatvédelmi rendellenesség/incidens bekövetkezésének és/vagy észlelésének első időpontja,
d) az adatvédelmi eseménnyel/incidenssel érintett személyek körének típusa (pl. ügyfél, alkalmazott, kiskorú) és nagysága (hány személyt érinthet),
e) az adatvédelmi eseménnyel/incidenssel érintett személyes adatok köre, érzékenysége (pl. személyazonosító adatok, tranzakciós adatok, különleges adatok), hozzávetőleges száma,
f) az adatvédelmi rendellenesség/incidens már bekövetkezett és lehetséges következményei, hatásai (milyen sérelmet okozhat a személyes adatok bizalmasságának, integritásának vagy rendelkezésre állásának sérülését illetően) és annak súlyossága (az érintetteket ért fizikai, anyagi vagy nem vagyoni kár nagysága),
g) az adatvédelmi rendellenességhez/incidenshez kapcsolódó egyéb tényadatok és körülmények (beleértve az azonosíthatóság mértékének a meghatározását is). Az adatvédelmi incidens előtt alkalmazott védelmi intézkedésekre, illetve az incidens orvoslására tett és/vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket (pl. az érintettek tájékoztatása, kárenyhítési lépések, jelszó-visszaállítás vagy -változtatás, biztonsági javítóprogram feltelepítése stb).

6.3. Adatvédelmi esemény kivizsgálása

Az adatvédelmi esemény bejelentését követően az Adatvédelmi tisztviselő:

a) az adatvédelmi esemény jellegétől függően értesíti az Informatikai vezetőt, a Társaság Jogi Képviselőjét,
b) értesíti azon szervezeti egységek vezetőit és adatgazdáit, amely szervezeti egységek részéről közreműködés szükséges az adatvédelmi esemény kivizsgálásában,
c) a Társaság illetékes szervezeti egysége, illetve a bejelentő közreműködésével kivizsgálja és feltárja az adatvédelmi rendellenesség vagy incidens körülményeit.

Amennyiben az információbiztonsági incidens a pénzforgalmi szolgáltatással kapcsolatos esemény következményeinek elhárítására, illetve a védett adatok megsértésére utaló bejelentések kivizsgálására az adatvédelmi eseménynek is minősülő pénzforgalmi szolgáltatással kapcsolatos rendellenesség, akkor a titoksértés következményeinek elhárítását saját hatáskörükben a vonatkozó szabályzatok szerint az információbiztonsági incidens, pénzforgalmi szolgáltatással kapcsolatos esemény, illetve titoksértés tudomásukra jutását követően azonnal megkezdik és megállapításaikról, intézkedéseikről az adatvédelmi tisztviselőt folyamatosan tájékoztatják

A bejelentő az adatvédelmi esemény kivizsgálása során köteles bármikor az Adatvédelmi tisztviselő, az Adatvédelmi Csoport és az adatvédelmi esemény kivizsgálásában részt vevő egyéb szervezeti egységek rendelkezésére állni, valamint szükség szerint a tőle elvárható mértékben azokkal együttműködni.

Az adatvédelmi esemény körülményeinek feltárásában az Adatvédelmi tisztviselő rendelkezésének megfelelően a Társaság valamennyi szervezeti egysége köteles közreműködni (amennyiben az adott szervezeti egységnél adatgazda működik, az adatgazda útján). Ennek keretében köteles az Adatvédelmi tisztviselő által kért adatokat, információkat, bizonyítékokat a kért határidőre rendelkezésre bocsátani, különösen:

a) az adatvédelmi eseménnyel érintett természetes személyek köre és száma,
b) az adatvédelmi eseménnyel érintett személyes adatok fajtája (beleértve az azonosíthatóság mértékének a meghatározását is) és köre, valamint hozzávetőleges száma,
c) az adatvédelmi esemény észlelésének időpontja és fennállásának időtartama,
d) az adatvédelmi esemény részletes leírása, körülményei [mely adatbiztonsági előírás sérült, milyen cselekmény(ek) vagy mulasztás(ok) vezetett/vezettek az adatvédelmi rendellenességhez/incidenshez],
e) az adatvédelmi esemény lehetséges vagy már bekövetkezett következményei (pl. vagyoni vagy nem vagyoni kár, személyazonosság-lopás vagy a személyazonossággal való visszaélés, pénzügyi veszteség) és hatásai,
f) az adatvédelmi esemény következményeinek elhárítása érdekében tervezett vagy más megtett intézkedések.

Az adatvédelmi tisztviselő az adatvédelmi esemény körülményeinek feltárása, az adatvédelmi incidensnek a Nemzeti Adatvédelmi és Információszabadság Hatóság felé történő bejelentése, az érintettek tájékoztatásának előkészítése, valamint az adatvédelmi esemény tapasztalatai nyomán megteendő intézkedések előkészítése során bármikor, ismétlődően is kérhet adatokat, információkat, továbbá rendszeres (pl. 24 óránkénti) adatszolgáltatást írhat elő.

Az Adatvédelmi tisztviselő vizsgálata során, illetve eredményeként:

a) dönt arról, hogy a bejelentésben leírt eset adatvédelmi rendellenességnek vagy adatvédelmi incidensnek minősül-e,
b) az adatvédelmi incidens e jellegének megállapítása esetén – szükség esetén – tájékoztatja az Informatikai vezetőt, a Társaság Jogi Képviselőjét az adatvédelmi incidensről, annak súlyosságáról, a lehetséges következményekről, a következmények mérséklésére tett, illetve teendő intézkedésekről,
c) dönt arról, hogy az adatvédelmi incidens bejelentendő-e a Nemzeti Adatvédelmi és Információszabadság Hatóságnak, és szükség esetén az adatvédelmi incidenst bejelenti a Hatóságnak,
d) javaslatot tesz az érintettek tájékoztatásának elrendelésére. A tájékoztatás szükségességéről és jogi tartalmáról megkéri a Jogi képviselő véleményét. Az érintettek tájékoztatására vonatkozó döntés esetén pedig – a Jogi Képviselő, illetve a Vezérigazgató közreműködésével – előkészíti a tájékoztató formaszövegét,
e) nyilvántartást vezet az adatvédelmi incidensekről, feltüntetve az adatvédelmi incidenshez kapcsolódó tényeket, annak hatásait és az orvoslására tett intézkedéseket;
f) oktatóanyagot készít a Társaság munkatársai, alkalmazottai számára az adatvédelmi esemény felismerése és az ilyen esetben követendő eljárás elsajátítása érdekében,
g) amennyiben sajtóközlemény kiadása szükséges, közreműködik a Vezérigazgató a sajtóközlemény előkészítésében.

Az adatvédelmi incidens vagy rendellenesség elhárítása vagy orvoslása érdekében tett egyes intézkedésekről az adatok kezelését vagy feldolgozását végző szakterület vezetője, vagy a kijelölt adatgazda az adott intézkedések végrehajtását követő 2 munkanapon belül köteles az Adatvédelmi tisztviselőt tájékoztatni. Az adatvédelmi incidensek elhárítása vagy orvoslása érdekében tett egyes intézkedéseket alátámasztó tény adatokat, bizonyítékokat az illetékes szakterület visszakereshető módon dokumentálja és tárolja.

6.4. Adatvédelmi incidensek hatóság felé történő bejelentése

Az adatvédelmi incidenst az Adatvédelmi tisztviselő – ha lehetséges – a tudomásszerzést követő 72 órán belül bejelenti az adatvédelmi felügyeleti hatóság felé.

Amennyiben a bejelentés megtétele 72 órán belül nem lehetséges, az Adatvédelmi tisztviselő összegyűjti a késedelem alapjául szolgáló indokokat, bizonyítékokat az adatvédelmi incidensek kivizsgálásában résztvevő szervezeti egységektől.

A bejelentést az Adatvédelmi tisztviselő az adatvédelmi felügyeleti hatóság online felületén teszi meg.

A bejelentésnek tartalmaznia kell:

a) az adatvédelmi tisztviselő nevét és elérhetőségét,
b) az adatvédelmi incidens bekövetkezésének időpontját,
c) az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek körét és nagyságát,
d) az adatvédelmi incidenssel érintett adatok kategóriáit és hozzávetőleges számát,
e) az adatvédelmi incidensből eredő, valószínűsíthető következményeket,
f) az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

Amennyiben a fenti információk egyidejű közlése nem lehetséges, úgy azokat az Adatvédelmi tisztviselő indokolatlan késedelem nélkül később részletekben közli a hatósággal.

6.5. Érintettek tájékoztatása az adatvédelmi incidensekről

A Társaság az érintettet a Vezérigazgató döntése alapján és annak megfelelően – az érintett által korábban megadott elérhetőségeken – írásban, elektronikus üzenetben, vagy telefonon közvetlenül tájékoztatja az adatvédelmi incidensről.

A Vezérigazgató döntése alapján a Társaság az érintetteket a Társaság honlapján vagy országos lefedettségű sajtótermékben közzétett hirdetmény útján is értesítheti.

6.6. Külső kommunikáció

Amennyiben az adatvédelmi incidenssel kapcsolatosan bármilyen információ a nyilvánosság elé kerül, úgy az adatvédelmi incidenssel kapcsolatos bármilyen és valamennyi sajtóközlemény tételére, a sajtóval való kapcsolattartásra kizárólag a Társaság Vezérigazgatója jogosult az Adatvédelmi tisztviselő közreműködésével.

6.7. Adatvédelmi felügyeleti hatóságokkal való kapcsolattartás

Az Adatvédelmi tisztviselő feladata:

a) előzetes konzultáció kezdeményezése a felügyeleti hatósággal, amennyiben az adatvédelmi hatásvizsgálat elvégzését követően megállapítható, hogy az adatkezelés a kockázat mérséklése céljából tett intézkedések hiányában valószínűsíthetően magas kockázattal jár;
b) tanúsítási eljárás kezdeményezése és a tanúsítást végző szervezettel való kapcsolattartás, illetve az együttműködés koordinálása a tanúsítási eljárás lefolytatása érdekében;
c) az adatvédelmi felügyeleti hatóságtól érkező, a GDPR, illetve az Infotv. hatálya alá tartozó ügyre vonatkozó megkeresésekre (vagyis az adatvédelmi felügyeleti hatóság vizsgálati, illetve korrekciós hatáskörében hozott intézkedésekre – a továbbiakban együtt: adatvédelmi hatósági megkeresés) adandó válasz koordinált előkészítése, továbbá a felügyeleti hatóság által folytatott helyszíni vizsgálat esetén a felügyeleti hatósággal való együttműködés koordinálása;
d) az adatvédelmi felügyeleti hatóság eljárásának kezdeményezése magatartási kódex jóváhagyása céljából;
e) az adatvédelmi felügyeleti hatóság eljárásának kezdeményezése adattovábbítási szerződéses feltételek jóváhagyása céljából;
f) az adatvédelmi felügyeleti hatóság eljárásának kezdeményezése kötelező erejű vállalati szabályok jóváhagyása céljából;
g) döntés az adatvédelmi felügyeleti hatóság döntéseivel szembeni jogorvoslati eljárás megindításáról;
h) a felügyeleti hatóság értesítése az adatvédelmi incidensről.

Az adatvédelmi felügyeleti hatóságtól érkező bármilyen küldeményt – amennyiben azt nem az Adatvédelmi tisztviselőnek címezték és/vagy nem közvetlenül hozzá juttatta el az adatvédelmi felügyeleti hatóság – a küldeményt átvevő szervezeti egység haladéktalanul, de legkésőbb az átvételt követő munkanapon – belső kézbesítés útján– át kell, hogy adja az Adatvédelmi tisztviselőnek.

Az Adatvédelmi tisztviselő az adatvédelmi hatósági megkeresést megvizsgálja.
Ennek keretében:

a) az adatvédelmi hatósági megkereséssel érintett szakterület(ek)től – az adatgazda (adatgazdák) útján – adatok rendelkezésre bocsátását és álláspontja (álláspontjuk) kifejtését kéri, illetve felvilágosítást, magyarázatot, szakmai állásfoglalást, illetve az Adatvédelmi tisztviselő döntésének előkészítésében való egyéb közreműködést kér;
b) kérheti az informatikai rendszerekben tárolt adatokhoz és az adatkezelési műveletekhez való hozzáférés biztosítását;
c) szükség esetén a Társaság Jogi képviselőjétől jogszabály-értelmezési kérdésben támogatást kér;
d) az általa az adatvédelmi hatósági megkeresés megválaszolásához szükségesnek ítélt egyéb intézkedést kérhet.

Az Adatvédelmi tisztviselő által kért adatot, információt, felvilágosítást, magyarázatot, hozzáférést, illetve jogi és szakmai állásfoglalást az általa megjelölt határidőben rendelkezésére kell bocsátani.
Az adatvédelmi hatósági megkeresésekre adandó választ az Adatvédelmi tisztviselő küldi meg az adatvédelmi felügyeleti hatóságnak.

Az adatvédelmi felügyeleti hatósági eljárásban a Társaságot az Adatvédelmi tisztviselő képviseli. Az adatvédelmi felügyeleti hatósági eljárásban a Társaság Jogi képviselője szükség szerint közreműködik.

Az adatvédelmi felügyeleti hatóság határozata elleni jogorvoslati eljárás megindításáról az Adatvédelmi tisztviselő az érintett szakterület vezetőjének, illetve a Társaság Jogi képviselőjének véleményének kikérése után dönt. A jogorvoslati eljárásban a Társaság képviseletét a Társaság Jogi képviselője biztosítja. A jogorvoslati kérelem előkészítésében, megszövegezésében, a perstratégia kialakításában, továbbá a jogorvoslati eljárás során a Társaság képviselőjét az Adatvédelmi tisztviselő támogatja.

7. Mellékletek

1.számú melléklet - Adathordozó mozgatása/megsemmisítése – IB11M1