HONVÉDELMI MINISZTÉRIUM
ELEKTRONIKAI, LOGISZTIKAI ÉS VAGYONKEZELŐ
ZÁRTKÖRŰEN MŰKÖDŐ RÉSZVÉNYTÁRSASÁG (HM EI Zrt.)

Nyt. szám: 887/505 2.számú példány

Jóváhagyom!
2018. május 25 - n

Móró Lajos
vezérigazgató

HONVÉDELMI MINISZTÉRIUM Elektronikai, Logisztikai és Vagyonkezelő Zártkörűen Működő Részvénytársaság

Honvédelmi Minisztérium Elektronikai, Logisztikai és Vagyonkezelő Zártkörűen Működő Részvénytársaság

Adatvédelmi és Adatbiztonsági Szabályzata

TARTALOMJEGYZÉK

I. Általános rendelkezések

1. A szabályzat célja és hatálya

Jelen szabályzat (a továbbiakban: **Szabályzat**) célja, hogy biztosítsa a Honvédelmi Minisztérium Elektronikai, Logisztikai és Vagyonkezelő Zártkörűen Működő Részvénytársaságnál (a továbbiakban: **Társaság vagy adatkezelő**) a személyes adatok védelméhez fűződő jog érvényesülését, a személyes adatok jogszerű kezelését, a személyes adatokat tartalmazó papíralapú és elektronikus nyilvántartások kezelésének rendjét, az érintettek jogainak gyakorlását, megakadályozza az adatokhoz való jogosulatlan hozzáférést, az adatok illetéktelen megváltoztatását, jogosulatlan nyilvánosságra hozatalát, ezáltal biztosítsa az adatvédelem és az adatbiztonság követelményeinek érvényesülését.

A Szabályzat tárgyi hatálya a Társaság valamennyi – személyes adatokat érintő – papíralapú, vagy nyilvántartási rendszer részét képező, vagy elektronikus adatkezelésére, illetve adatfeldolgozására vonatkozik.
A Szabályzat személyi hatálya kiterjed a Társaság valamennyi adatkezelést, adatfeldolgozást végző szervezeti egységére, munkavállalójára, továbbá a Társasággal szerződéses jogviszonyban álló természetes és jogi személyre, jogi személyiséggel nem rendelkező szervezetre, a velük kötött szerződésben, illetve a titoktartási nyilatkozatban rögzített mértékben.

2. Kapcsolódó jogszabályok és belső szabályozási dokumentumok

Kapcsolódó főbb jogszabályok:
- Magyarország Alaptörvénye (2011. április 25.),
- 2013. évi V. törvény a Polgári Törvénykönyvről (a továbbiakban: Ptk.),
- 2012. évi I. törvény a munka törvénykönyvéről (a továbbiakban: Mt.),
- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (a továbbiakban: **Info tv.**),
- 1997. évi CLIX. törvény a fegyveres biztonsági őrségről, a természetvédelmi és a mezei őrszolgálatról,
- 2005. évi CXXXIII. törvény a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól
- az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) 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, a továbbiakban: **GDPR**).

Kapcsolódó belső szabályozási dokumentumok különösen:
- Szervezeti és Működési Szabályzat (a továbbiakban: **SZMSZ**),
- A Társaság Biztonsági Rendszabályairól szóló Szabályzat,
- Iratkezelési Szabályzat,
- Elektronikus Informatikai és Információvédelmi Biztonsági Szabályzat (a továbbiakban: **EIIBSZ**),
- 10/2017. számú vezérigazgatói intézkedés a HM EI Zrt. és az egyes szolgáltatási helyek területére érvényes belépővel történő ellátás rendjére.
- 2/2018. számú vezérigazgatói intézkedés a HM EI Zrt. gépjárművekbe szerelt GPS alapú online nyomkövető szolgáltatás használatáról.

3. Fogalom-értelmezések

A Szabályzat alkalmazása során:
Adatfeldolgozó: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely a Társasággal, mint adatkezelővel kötött szerződése alapján – beleértve a jogszabály rendelkezése alapján történő szerződéskötést is – vagy egyébként a Társaság nevében személyes adatot kezel.
Adatkezelés: a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy azok összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tagolása, tárolása, átalakítása vagy megváltoztatása, lekérdezése, betekintés, felhasználása, közlése továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, korlátozása, törlése, illetve megsemmisítése, így különösen fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése.
Adatkezelés korlátozása: a tárolt személyes adat megjelölése az adat további, jövőbeli kezelésének korlátozása céljából.
Adatkezelő: adatkezelőnek minősül a Társaság az olyan adat tekintetében, amely esetében önállóan vagy másokkal együtt meghatározza a személyes adatok kezelésének célját és eszközeit, az adatkezelést végrehajtja, vagy az általa megbízott adatfeldolgozóval végrehajtatja azokat. Adatkezelőnek minősül a Társaság azon adatkezelések tekintetében is, amelyek esetében az adatkezelés céljait és eszközeit, a Társaságot, mint adatkezelőt vagy a Társaság adatkezelőként történő kijelölésére vonatkozó különös szempontokat uniós vagy hazai jogszabály állapítja meg.
Adattovábbítás: az adat meghatározott harmadik fél részére történő hozzáférhetővé tétele.
Adattörlés: az adat megsemmisítése vagy felismerhetetlenné tétele oly módon, hogy helyreállítása többé nem lehetséges.
Adatvédelmi incidens: a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi.
Álnevesítés: a személyes adat olyan módon történő kezelése, amely – a személyes adattól elkülönítve tártolt – további információ felhasználása nélkül megállapíthatatlanná teszi, hogy a személyes adat mely konkrét természetes személyre vonatkozik, valamint technikai és szervezési intézkedések megtételével biztosítja, hogy azonosított vagy azonosítható természetes személyhez ezt a személyes adatot ne lehessen kapcsolni.
Azonosítható természetes személy: az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, azonosító szám, helymeghatározó adat, online azonosító vagy természetes személy fizikai, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható.
BEBD: Belső Ellenőrzési és Biztonsági Divízió.
Címzett: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, akivel vagy amellyel a személyes adatot közlik, függetlenül attól, hogy harmadik fél-e. Azon közhatalmi szervek, amelyek egy egyedi vizsgálat keretében az uniós vagy a tagállami joggal összhangban férhetnek hozzá személyes adatokhoz, nem minősülnek címzettnek.
Érintett: bármely információ alapján azonosított vagy – közvetlenül vagy közvetve – azonosítható természetes személy.
Harmadik fél: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, aki vagy 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.

Hozzájárulás: az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező más magatartás, cselekedet útján jelzi, hogy beleegyezését adja a rá vonatkozó személyes adatok – teljes körű vagy egyes műveletekre kiterjedő – kezeléséhez.

EII: Elektronikai és Informatikai Igazgatóság.

Információ: az információ ismeretté értelmezett adat, amely érzékelésre, észlelésre és felfogásra kerülhet.

Különleges adat: 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 természetes személyek egyedi azonosítását célzó genetikai és biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok.

Genetikai adat: egy természetes személy örökölt vagy szerzett genetikai jellemzőire vonatkozó minden olyan személyes adat, amely az adott személy fiziológiájára vagy egészségi állapotára vonatkozó egyedi információt hordoz, és amely elsősorban az említett természetes személyből vett biológiai minta elemzéséből ered.

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

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

Munkaügyi nyilvántartás: a Humánpolitikai Divízió által vezetett, a munkavállaló munkaviszonnyal összefüggésben keletkezett és azzal kapcsolatban álló adatait tartalmazó nyilvántartás.

NAIH: Nemzeti Adatvédelmi és Információszabadság Hatóság

Nyilvánosságra hozatal: az adat bárki számára történő hozzáférhetővé tétele.

Nyilvántartási rendszer: a személyes adatok bármely módon – centralizált, decentralizált vagy funkcionális, vagy földrajzi szempontok szerint – tagolt állománya, amely meghatározott ismérvek alapján hozzáférhető.

Profilalkotás: személyes adat bármely olyan - automatizált módon történő - kezelése, amely az érintett személyes jellemzőinek, különösen a munkahelyi teljesítményéhez, gazdasági helyzetéhez, egészségi állapotához, személyes preferenciáihoz vagy érdeklődéséhez, megbízhatóságához, viselkedéséhez, tartózkodási helyéhez vagy mozgásához kapcsolódó jellemzőinek értékelésére, elemzésére vagy előrejelzésére irányul.

Személyes adat: azonosított vagy azonosítható természetes személyre („érintett") vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható.

Személyi irat: minden – bármilyen anyagon, alakban és bármilyen eszköz felhasználásával keletkezett – adathordozó, amely a munkaviszony létesítésekor, fennállása alatt, megszűnésekor, illetve azt követően keletkezik és a munkavállaló személyével összefüggésben adatokat, megállapítást tartalmaz.

4. Az adatkezelés

4.1. Személyes adat kezelésének elvei

Törvényesség: Az adatkezelésnek minden szakaszában meg kell felelnie az adatkezelés céljának, az adatok felvételének és kezelésének tisztességesnek és törvényesnek, az érintettek számára átláthatónak kell lennie.
Célhoz kötöttség: Személyes adat kizárólag egyértelműen meghatározott és jogszerű célból, kezelhető.
Adattakarékosság és korlátozott tárolhatóság: Csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, szükséges, és a cél elérésére alkalmas. A személyes adat csak a cél megvalósulásához szükséges mértékben és ideig kezelhető. A személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható, azaz az adatkezelő rendelkezik azokkal a technikai feltételekkel, amelyek a helyreállításhoz szükségesek.
Pontosság: Az adatkezelés során biztosítani kell az adatok pontosságát, teljességét és – ha az adatkezelés céljára tekintettel szükséges – naprakészségét.
Integritás és bizalmasság: Az adatkezelést oly módon kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adat megfelelő biztonsága, az adat jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve.
Elszámoltathatóság: az adatkezelő felelős a fenti alapelveknek történő megfeleléséért, az e szabályzatban foglaltak betartásáért, valamint képesnek kell lennie e megfelelés igazolására.

4.2. A személyes adat kezelésére vonatkozó előzetes tájékoztatás

Az érintett részére a személyes adatok kezelésére vonatkozó, e szabályzat által előírt valamennyi információt és tájékoztatást tömör, átlátható, érthető és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva kell nyújtani. Az információkat írásban vagy más módon – ideértve adott esetben az elektronikus utat is – kell megadni. Az érintett kérésére szóbeli tájékoztatás is adható, feltéve, hogy más módon igazolták az érintett személyazonosságát.

4.2.1. Tájékoztatás, ha a személyes adatokat az érintettől gyűjtik:

Az érintettel az adatkezelés megkezdése előtt, a személyes adatok megszerzésének időpontjában közölni kell, vagy az érintett rendelkezésére kell bocsátani a következő információk mindegyikét:

a) az adatkezelőnek a kiléte és elérhetőségei;
b) az adatvédelmi tisztviselő elérhetőségei;
c) a személyes adatok tervezett kezelésének célja, valamint az adatkezelés jogalapja;
d) ha az adatkezelés az adatkezelő vagy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, akkor a tájékoztatásnak ki kell terjednie a jogos érdek megnevezésére (GDPR 6. cikk (1) bekezdésének f) pontján alapuló adatkezelés);
e) adott esetben a személyes adatok címzettjei, illetve a címzettek kategóriái, ha van ilyen;
f) adott esetben annak ténye, hogy a Társaság harmadik országba vagy nemzetközi szervezet részére kívánja továbbítani a személyes adatokat, továbbá a Bizottság megfelelőségi határozatának léte vagy annak hiánya, vagy a GDPR rendelet 46. cikkben, a 47. cikkben vagy a 49. cikk (1) bekezdésének második albekezdésében említett adattovábbítás esetén a megfelelő és alkalmas garanciák megjelölése, valamint

az azok másolatának megszerzésére szolgáló módokra vagy az azok elérhetőségére való hivatkozás.

g) a személyes adatok tárolásának időtartamáról, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjairól;
h) az érintett azon jogáról, hogy kérelmezheti az adatkezelőtől a rá vonatkozó személyes adatokhoz való hozzáférést, azok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen, valamint – ha ennek feltételei fennállnak – az érintett adathordozhatósághoz való jogáról;
i) az érintett hozzájárulásán alapuló adatkezelés esetén a hozzájárulás bármely időpontban történő visszavonásához való jog, amely nem érinti a visszavonás előtt a hozzájárulás alapján végrehajtott adatkezelés jogszerűségét;
j) a felügyeleti hatósághoz címzett panasz benyújtásának jogáról;
k) arról, hogy a személyes adat szolgáltatása jogszabályon vagy szerződéses kötelezettségen alapul vagy szerződés kötésének előfeltétele-e, valamint hogy az érintett köteles-e a személyes adatokat megadni, továbbá hogy milyen lehetséges következményekkel járhat az adatszolgáltatás elmaradása;
l) kizárólag automatizált adatkezelésen alapuló döntéshozatal esetén (ideértve a profilalkotást is) ennek ténye, valamint legalább ezekben az esetekben az alkalmazott logikára és arra vonatkozóan érthető információk, hogy az ilyen adatkezelés milyen jelentőséggel, és az érintettre nézve milyen várható következményekkel bír.

Ha a Társaság a gyűjtés eredeti céljától eltérve további adatkezelést kíván végezni a személyes adatokon, ezt megelőzően is tájékoztatni kell az érintettet az eltérő célról és a fenti felsorolásban szereplő minden releváns, a változással kapcsolatos kiegészítő információról.

4.2.2. Tájékoztatás, ha a személyes adatokat nem az érintettől gyűjtik:

Ha az adatot nem az érintettől szerezték meg, a Társaság az érintett rendelkezésére bocsátja a 4.2.1. pont a)-j), l) pontjaiban szereplő információkat, valamint az érintett személyes adatok kategóriáira, a személyes adatok forrására vonatkozó információkat, ha nyilvánosan hozzáférhető forrásból származnak, ennek megjelölésével.

Ha a Társaság a gyűjtés eredeti céljától eltérve további adatkezelést kíván végezni a személyes adatokon, ezt megelőzően is tájékoztatni kell az érintettet az eltérő célról és a fenti felsorolásban szereplő minden releváns, a változással kapcsolatos kiegészítő információról.

A Társaság a tájékoztatást az alábbiak szerint adja meg:
a) a személyes adatok kezelésének konkrét körülményeit tekintetbe véve, a személyes adatok megszerzésétől számított észszerű határidőn, de legkésőbb egy hónapon belül;
b) ha a személyes adatokat az érintettel való kapcsolattartás céljára használják, legalább az érintettel való első kapcsolatfelvétel alkalmával; vagy
c) ha várhatóan más címzettel is közlik az adatokat, legkésőbb a személyes adatok első alkalommal való közlésekor.

Nem kell tájékoztatni az érintettet, amennyiben:
- a szóban forgó információk rendelkezésre bocsátása lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényelne, illetőleg ha a tájékoztatási kötelezettség teljesítése valószínűsíthetően lehetetlenné tenné vagy komolyan veszélyeztetné ezen adatkezelés céljainak elérését. Ilyen esetekben az adatkezelőnek megfelelő

intézkedéseket kell hoznia – az információk nyilvánosan elérhetővé tételét is ideértve – az érintett jogainak, szabadságainak és jogos érdekeinek védelme érdekében;
- az adat megszerzését vagy közlését kifejezetten előírja az adatkezelőre alkalmazandó uniós vagy hazai jogszabály, amely az érintett jogos érdekeinek védelmét szolgáló megfelelő intézkedésekről rendelkezik.

4.3. Új adatkezelés kezdeményezése:

Az új, személyes adatokra vonatkozó adatkezelés megkezdése előtt 40 nappal az új adatkezelést végezni kívánó szervezeti egység osztályvezetője vagy magasabb szintű vezetője köteles a vezérigazgatót és az adatvédelmi tisztviselőt egyidejűleg írásban tájékoztatni, annak érdekében, hogy a tervezett adatkezelés jogalapja, célja, hatóköre jogszerűsége és az adatbiztonsági intézkedések ellenőrzésre kerüljenek. Az adatvédelmi tisztviselő a tervezett adatkezelésre vonatkozó információkat továbbítja a Jogi Divízió és a BEBD számára egyeztetés és véleményezés céljából. Adatkezelési tevékenység folytatását az adatvédelmi tisztviselő javaslatára a vezérigazgató engedélyezheti.
A meglévő adatkezelésből történő legyűjtés új adatkezelésnek számít, amennyiben az adatkezelés célja eltérően kerül meghatározásra, vagy az adatkezelő személye megváltozik.
A meglévő személyes adatokat érintő adatkezelés céljának, jogalapjának, adatkörének, adatkezelésre, adatfeldolgozásra jogosult személyének, az adatkezelés időtartamának változtatásáról, illetve, arról, hogy kik ismerhetik meg az adatokat az érintett szervezeti egység osztályvezetője vagy magasabb szintű vezetője az adatvédelmi tisztviselőt 40 nappal a tervezett változások végrehajtása előtt előzetesen tájékoztatja.

4.4. Az adatkezelést végző szervezeti egység vezetőjének feladatai
- szervezeti egységénél gondoskodik az adatvédelmi szabályok végrehajtásáról,
- szervezeti egységénél irányítja és ellenőrzi a személyes adatok kezelésével, azok készítésével, továbbításával összefüggő adatvédelmi tevékenységet,
- szervezeti egységénél irányítja és ellenőrzi a személyes adatkezelések esetében a GDPR 30. cikkének megfelelő adatkezelési nyilvántartási kötelezettség teljesítését, illetve az adatkezelési tevékenységekről vezetendő nyilvántartás adott szervezeti egység által kezelt információnak továbbítását az adatvédelmi tisztviselő részére,
- szervezeti egységénél felmerült esetleges adatvédelmi incidens esetén gondoskodik az adatvédelmi tisztviselő haladéktalan tájékoztatásáról a 11. pont szerinti adatokat illetően,
- abban az esetben, ha az érintett a személyes adatok kezelésére, továbbítására vonatkozó tájékoztatási vagy egyéb kérelmével közvetlenül a szervezeti egységhez fordul, a kérelmet az adatvédelmi tisztviselő részére haladéktalanul továbbítja,
- intézkedik az irányítása alá tartozó szervezet által kezelt személyes adatok megfelelő technikai vagy szervezési intézkedések alkalmazásával történő védelméről,
- intézkedik a nem szabályszerű adatkezelési gyakorlat megszüntetéséről, az eset kivizsgálása érdekében értesíti az adatvédelmi tisztviselőt.

4.5. Személyes adatokat tartalmazó új nyilvántartási rendszer (adatbázis) kialakítása

Az adatvédelmi és adatbiztonsági intézkedések betartásának, valamint jelen Szabályzat rendelkezéseinek érvényesülése érdekében egy személyes adatokat tartalmazó, nyilvántartási rendszer (adatbázis) vagy bármilyen más (akár papíralapú) adatkezelés kialakítása során az azt tervező szervezeti egység osztályvezetőjének a következő lépéseket kell végrehajtani:
- adatkezelés koncepciójának megfogalmazása, adatkezelés megnevezése,
- az adatkezelés céljának meghatározása,

- az adatkezelés jogalapjának meghatározása, jogszabályhely kiválasztása,
- feldolgozandó adatkör meghatározása,
- annak vizsgálata, hogy különleges személyes adatok feldolgozására kerül-e sor,
- az adatkezeléssel érintettek csoportjának leírása, az adatok várható mennyiségének behatárolása,
- adatok forrásának meghatározása,
- adatok átvétele esetén a jogalap tisztázása, módja,
- adatkezelést végző szervezeti egység kijelölése,
- adatkezelést végző munkavállaló kijelölése,
- adatvédelmi tisztviselő előzetes tájékoztatása, igény esetén bevonása,
- az adatkezelés technológiájának, illetve automatizáltságának kiválasztása,
- informatikai feldolgozó rendszer alkalmazása esetén az EIIBSZ előírásainak érvényesítése,
- adatfeldolgozó bevonása esetén megállapodás készítése,
- a tényleges adatkezelés helyének meghatározása,
- adattovábbítás esetén a továbbítandó adatok körének meghatározása, jogalapjának kiválasztása, a címzett meghatározása,
- az adattörlés, archiválás megtervezése,
- az érintett hozzájárulásán alapuló adatkezelés esetén a hozzájáruló nyilatkozat kialakítása,
- adatkezelési tájékoztató elkészítése,
- az adatkezeléshez történő hozzájárulások beszerzése,
- adatbiztonsági intézkedések kialakítása a 21. pontban rögzítettek szerint,
- adatvédelmi hatásvizsgálat lefolytatása a 22. pontban szabályozott esetekben,
- a tervezett adatkezelés megkezdése előtt legalább 40 nappal a vezérigazgató és az adatvédelmi tisztviselő tájékoztatása, és az adatvédelmi tisztviselő előzetes javaslata alapján a vezérigazgatótól jóváhagyás kérése az adatkezelési tevékenység megkezdéséhez,
- a jóváhagyást követően történhet az adatkezelés megkezdése.

5. Az adatkezelés alapvető feltételei:

- a célhoz kötöttség elvének alkalmazása,
- az adatkezelés jogalapjának megléte,
- az érintett számára egyértelmű, részletes tájékoztatás rendelkezésre bocsátása,
- adatkezelési nyilvántartás vezetése.

6. Az adatkezelés jogalapja

Személyes adat a Társaságnál akkor kezelhető, ha az alábbiak valamelyike teljesül:

a) az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez;

b) az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél, vagy az a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges;

c) az adatkezelés az adatkezelőre vonatkozó (uniós vagy tagállami jogszabályból eredő) jogi kötelezettség teljesítéséhez szükséges;

d) az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges;

e) az adatkezelés (uniós vagy tagállami jogszabályban meghatározott) közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges;

f) az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan

érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé, különösen, ha az érintett gyermek.

A c) és e) pont szerinti adatkezelés (kötelező adatkezelés) akkor folytatható, ha az adatkezelés jogalapját uniós vagy hazai jogszabály állapítja meg. A c) és e) pontban meghatározott kötelező adatkezelés esetén a kezelendő adatok fajtáit, az adatkezelés célját és feltételeit, az adatok megismerhetőségét, az adatkezelő személyét, valamint az adatkezelés időtartamát vagy szükségessége időszakos felülvizsgálatát az adatkezelést elrendelő törvény, illetve önkormányzati rendelet határozza meg. Ha az adatkezelés időtartamát vagy szükségessége időszakos felülvizsgálatát törvény vagy az Európai Unió kötelező jogi aktusa nem határozza meg, a Társaság az adatkezelés megkezdésétől legalább háromévente felülvizsgálja, hogy az általa, illetve a megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által kezelt személyes adat kezelése az adatkezelés céljának megvalósulásához szükséges-e. Ezen felülvizsgálat körülményeit és eredményét a Társaság dokumentálja, e dokumentációt a kezelt adat törlését követő 10 évig megőrzi és azt a NAIH kérésére rendelkezésére bocsátja.

A Társaságnál nem kezelhető különleges adat, kivéve

a) ha az érintett kifejezett hozzájárulását adta az érintett személyes adatok egy vagy több konkrét célból történő kezeléséhez, és uniós vagy tagállami jog megengedi a hozzájáruláson alapuló adatkezelést, pl. arckép, ujjlenyomat vagy egyéb biometrikus adat kezelése esetén;
b) ha az adatkezelés az érintett vagy más természetes személy létfontosságú érdekeinek védelméhez szükséges, ha az érintett fizikai vagy jogi cselekvőképtelensége folytán nem képes a hozzájárulását megadni;
c) ha az adatkezelés jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez szükséges;
d) ha az adatkezelés jelentős közérdek miatt szükséges, uniós jog vagy hazai jogszabály (pl. vagyonvédelemre vonatkozó jogszabályi előírások) alapján, amely arányos az elérni kívánt céllal, tiszteletben tartja a személyes adatok védelméhez való jog lényeges tartalmát, és az érintett alapvető jogainak és érdekeinek biztosítására megfelelő és konkrét intézkedéseket ír elő;
e) ha az adatkezelés olyan személyes adatokra vonatkozik, amelyeket az érintett kifejezetten nyilvánosságra hozott;
f) a Humánpolitikai Divíziónál a munkavállalók egészségi állapotára vonatkozó adatok, abban az esetben, ha

- az adatkezelés a Társaságnak vagy az érintettnek a foglalkoztatást, valamint a szociális biztonságot és szociális védelmet szabályozó jogi előírásokból fakadó kötelezettségei teljesítése és konkrét jogai gyakorlása érdekében szükséges, ha az érintett alapvető jogait és érdekeit védő megfelelő garanciákról is rendelkező uniós vagy hazai jogszabály, illetve a hazai jogszabály szerinti kollektív szerződés ezt lehetővé teszi;
- az adatkezelés megelőző egészségügyi vagy munkahelyi egészségügyi célokból, a munkavállaló munkavégzési képességének felmérése, orvosi diagnózis felállítása, egészségügyi vagy szociális ellátás vagy kezelés nyújtása, illetve egészségügyi vagy szociális rendszerek és szolgáltatások irányítása érdekében szükséges, uniós vagy tagállami jog alapján vagy egészségügyi szakemberrel kötött szerződés értelmében, szakmai titoktartási kötelezettség hatálya alatt.

Hozzájárulás: Az érintettnek – amennyiben az adatkezelés hozzájáruláson alapul - a személyes adatainak kezeléséhez történő hozzájárulását bizonyítható módon kell megtennie (írásban, vagy rögzített kép-, hangfelvételen vagy egyéb elektronikus formában rögzített módon). Ha az

érintett hozzájárulását olyan írásbeli nyilatkozat keretében adja meg, amely más ügyekre is vonatkozik, a hozzájárulás iránti kérelmet ezektől a más ügyektől egyértelműen megkülönböztethető módon kell előadni, érthető és könnyen hozzáférhető formában, világos és egyszerű nyelvezettel. Az érintett jogosult arra, hogy hozzájárulását bármikor visszavonja. A hozzájárulás visszavonása nem érinti a hozzájáruláson alapuló, a visszavonás előtti adatkezelés jogszerűségét. A hozzájárulás megadása előtt az érintettet erről tájékoztatni kell. A hozzájárulás visszavonását ugyanolyan egyszerű módon kell lehetővé tenni, mint annak megadását.
A 16. életévét betöltött kiskorú érintett hozzájárulását tartalmazó jognyilatkozatának érvényességéhez törvényes képviselőjének beleegyezése vagy utólagos jóváhagyása nem szükséges. A 16. életévét még nem, azonban 14. életévét már betöltött kiskorú hozzájáruló nyilatkozatához törvényes képviselője hozzájárulása szükséges. A 14. életétévét még nem betöltött kiskorú nevében törvényes képviselője tehet hozzájáruló nyilatkozatot.
Kétség esetén azt kell vélelmezni, hogy az érintett a hozzájárulását nem adta meg.

7. Adatfeldolgozás

Amennyiben a Társaság adatfeldolgozót vesz igénybe, az adatfeldolgozónak a személyes adatok feldolgozásával kapcsolatos jogait és kötelezettségeit - az adatkezelésre vonatkozó uniós és hazai jogszabályok keretei között - a Társaság, mint adatkezelő határozza meg. A Társaság által adott utasítások jogszerűségéért a Társaság felel. Az adatfeldolgozó a személyes adatokat kizárólag az adatkezelő írásbeli utasításai alapján kezeli, kivéve, ha az adatkezelési műveletet az adatfeldolgozóra alkalmazandó uniós vagy tagállami jogszabály írja elő.
Az adatfeldolgozó tevékenységének ellátása során – az adatkezelő előzetes írásban tett eseti vagy általános felhatalmazása nélkül – más adatfeldolgozót nem vehet igénybe.
Az adatfeldolgozó adatkezelést érintő érdemi döntést nem hozhat, a tudomására jutott személyes adatokat kizárólag a Társaság, mint adatkezelő rendelkezései szerint dolgozhatja fel, továbbá a személyes adatokat a Társaság, mint adatkezelő rendelkezései szerint köteles tárolni és megőrizni. Az adatkezelési szolgáltatás nyújtásának befejezését követően az adatkezelő döntése alapján minden személyes adatot töröl vagy visszajuttat az adatkezelőnek, és törli a meglévő másolatokat, kivéve, ha az uniós vagy a tagállami jogszabály a személyes adatok további tárolását írja elő.
Az adatfeldolgozásra vonatkozó szerződést írásba kell foglalni, melyben az adatfeldolgozót kötelezni kell arra, hogy a Társaságot, mint adatkezelőt az adatvédelmi tisztviselő útján megfelelő időn belül, de legfeljebb 24 órán belül tájékoztassa, amennyiben adatvédelmi incidens merül fel az adatfeldolgozónál. Az adatfeldolgozással nem bízható meg olyan szervezet, személy, amely a feldolgozandó személyes adatokat felhasználó üzleti tevékenységben érdekelt. Adatfeldolgozással kizárólag olyan adatfeldolgozó bízható meg, amely az érintettek jogainak és a személyes adatok védelmét biztosító, a Társaság vonatkozó szabályzatainak és a GDPR előírásainak megfelelő technikai és szervezési intézkedéseket alkalmaz. Az adatfeldolgozásra vonatkozó szerződésnek tartalmaznia kell a GDPR 28. cikkében előírt követelményeket. Amennyiben az Európai Unió Bizottsága, vagy a NAIH az uniós felügyeleti hatóságokkal együttműködve általános szerződési feltételeket állapítanak meg az adott adatfeldolgozási tevékenységre nézve, a szerződésben figyelemmel kell lenni ezek tartalmára is.

8. Adatvédelmi tisztviselő

A Társaságnál adatvédelmi tisztviselő kerül kijelölésre, a GDPR 37. cikk (1) bekezdés a) pontja alapján. A Társaság közzéteszi honlapján az adatvédelmi tisztviselő nevét és elérhetőségét,

valamint közli a NAIH-al is. Az adatvédelmi tisztviselő feladatait az SZMSZ-ben és a munkaköri leírásban meghatározottak alapján végzi.
Az adatvédelmi tisztviselő jogviszonyának fennállása alatt és annak megszűnését követően is megőrzi a tevékenységével, annak ellátásával kapcsolatban tudomására jutott személyes adatot, minősített adatot, illetve törvény által védett titoknak és hivatás gyakorlásához kötött titoknak minősülő adatot, valamint minden olyan adatot, tényt vagy körülményt, amelyet a Társaság nem köteles törvény előírásai szerint a nyilvánosság számára hozzáférhetővé tenni.

Feladatai:
- Az adatvédelmi jogszabályok és azok gyakorlati alkalmazása terén naprakész információkkal segíti a Társaság vezérigazgatóját és a menedzsmentet az üzleti döntésekben és végrehajtási folyamatokban, továbbá figyelemmel kíséri, hogy a Társaság adatkezelései megfeleljenek a hatályos jogszabályoknak.
- Közreműködik, illetve segítséget nyújt az adatkezeléssel összefüggő döntések meghozatalában, valamint az érintettek jogainak biztosításában.
- Tájékoztat és szakmai tanácsot ad a Társaság vagy az adatfeldolgozó, továbbá az adatkezelést végző alkalmazottak részére az e Szabályzat valamint az egyéb uniós vagy hazai jogszabályi adatvédelmi rendelkezések szerinti kötelezettségeikkel kapcsolatban.
- A Jogi Divízióval együttműködésben elkészíti a belső adatvédelmi és adatbiztonsági szabályzatot, és aktualizálja azt a jogszabályi vagy a belső szervezeti változásoknak megfelelően.
- Ellenőrzi a GDPR, Info tv. és az adatkezelésre vonatkozó más jogszabályok, valamint a belső adatvédelmi és adatbiztonsági szabályzat rendelkezéseinek és az adatbiztonsági követelményeknek a megtartását.
- Az érintettek a személyes adataik kezeléséhez és jogaik gyakorlásához kapcsolódó valamennyi kérdésben az adatvédelmi tisztviselőhöz fordulhatnak. Ennek biztosítása érdekében az érintettek panaszai fogadására a Társaság külön elektronikus elérhetőséget biztosít (adatvedelem@hmei.hu).
- Kivizsgálja a hozzá érkezett bejelentéseket, jogosulatlan adatkezelés észlelése esetén annak megszüntetésére javaslatot tesz a vezérigazgatónak.
- Beérkező kérelem esetén előkészíti a vezérigazgató részére az érintettel kapcsolatos adatkezelésről, adattovábbításról a tájékoztató levelet, valamint a GDPR 34. cikkében meghatározott esetekben az érintett adatait érintő adatvédelmi incidens körülményeiről, hatásairól és az elhárítására megtett intézkedésekről is megadja a tájékoztatást.
- Szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomon követi a hatásvizsgálat elvégzését.
- Részt vesz az adatvédelmi tisztviselők konferenciáján, mely a NAIH és az adatvédelmi tisztviselők rendszeres szakmai kapcsolattartását, az egységes joggyakorlat kialakítását szolgálja.
- Együttműködik a NAIH-hal, adatkezeléssel összefüggő ügyekben kapcsolattartó pontként szolgál a hatóság felé.
- Gondoskodik az adatvédelmi ismeretek továbbadásáról a Társaságon belül.
- A szervezeti egységek által részére nyújtott adatszolgáltatások és információk alapján az adatvédelmi incidensekről, az adatkezelési tevékenységekről, az érintett személyes adatokra vonatkozó tájékoztatási kérelméről nyilvántartást vezet. Ennek teljesítéséhez és a törvényben előírt határidők betartásához a szervezeti egységek a hozzájuk közvetlenül beérkező kéréseket, illetve adattovábbítási kérelmeket az adatvédelmi tisztviselő részére haladéktalanul továbbítani, valamint a náluk történt adatvédelmi incidensekről az adatvédelmi tisztviselőt annak bekövetkezésekor a 11. pont szerint tájékoztatni kötelesek.

- Gondoskodik a Társaságnál vagy az általa megbízott adatfeldolgozónál történt adatvédelmi incidensek 72 órán belüli bejelentéséről a NAIH felé a GDPR 33. cikkében rögzített tartalmi követelmények szerint. Késedelmes bejelentés esetén a hozzá beérkezett incidens bejelentésben leírtak alapján gondoskodik a késedelem igazolásáról szóló indokok összeállításáról, valamint haladéktalan bejelentéséről.
- Gondoskodik a GDPR 49. cikk (1) bekezdésében meghatározott adattovábbítások bejelentéséről a NAIH felé a II. 10. pontban leírtak alapján.

9. Ellenőrzés

Az adatkezeléssel kapcsolatos jogszabályi előírások és belső szabályozók betartását az adatkezelést végző szervezeti egységek vezetői kötelesek folyamatosan ellenőrizni, hiányosságok, illetve a szabályzóknak nem megfelelő működés észlelésekor erről az adatvédelmi tisztviselőt tájékoztatni.
Az adatvédelmi tisztviselő jogosult az irat- és adatkezeléssel kapcsolatos belső szabályozók, dokumentumok, nyilvántartások stb. áttekintésével ellenőrizni az adatkezelés jogszerű rendjének megtartását. Jogsértés észlelése esetén annak megszüntetésére javaslatot tesz a vezérigazgatónak.
Az adatvédelmi tisztviselő jogosult a Társaságnál végzett adatkezeléseket, valamint az adatbiztonsági követelmények betartását – szükség esetén a BEBD bevonásával - ellenőrizni.

II. Részletes szabályok

10. Az adattovábbítás harmadik ország vagy nemzetközi szervezet részére

A személyes adatok továbbítására – mint adatkezelési műveletre – a Szabályzat 6. pontjában foglalt rendelkezések (Az adatkezelés jogalapja) megfelelően alkalmazandók.
A személyes adatok továbbítására érkező – nem jogszabályon alapuló - megkeresés teljesítését megelőzően a tárgyban az adatvédelmi tisztviselővel haladéktalanul egyeztetni szükséges, annak érdekében, hogy amennyiben bejelentés szükséges a NAIH felé, azt teljesíteni tudja.
A Társaság megbízásából és érdekében adatkezelést vagy adatfeldolgozást végző személlyel, szervezettel kötendő szerződés kapcsán a szerződést előkészítő szervezeti egység - az adatvédelmi tisztviselő segítségével - köteles gondoskodni arról, hogy a szerződés szövegébe beépítésre kerüljenek az e Szabályzat szerinti adatvédelmi követelmények, garanciák.

Harmadik országba vagy nemzetközi szervezet részére történő adattovábbításra csak a GDPR 44-50. cikkben rögzített feltételek mellett kerülhet sor.

11. Az adatkezelési tevékenységek nyilvántartása

A szervezeti egységek adatkezeléseikről a 3. számú melléklet alapján nyilvántartást vezetnek, melyet új adatkezelések tervezése előtt 40 nappal, illetve a meglévő adatkezeléseket érintő változások nyilvántartásban történő átvezetése után az adatvédelmi tisztviselő részére tájékoztatásul haladéktalanul kötelesek elektronikus úton megküldeni. Az adatvédelmi tisztviselő a szervezeti egységek adatszolgáltatása alapján, az általuk megküldött dokumentumok és információk alapján elektronikus formában vezeti a Társaság egészére vonatkozóan a személyes adatkezelésekről az összesített adatkezelési nyilvántartást a GDPR 30. cikkében meghatározott adattartalommal.

Ezen összesített nyilvántartás az alábbi információkat tartalmazza:

- az adatkezelő, adatvédelmi tisztviselő neve, elérhetősége;
- az adatkezelés célja,
- az érintettek kategóriái, a személyes adatok kategóriái;
- az adatok közlésének címzettjei,
- harmadik országba vagy nemzetközi szervezet részére történő adattovábbítás esetén a továbbításra vonatkozó információk, beleértve a harmadik ország vagy a nemzetközi szervezet azonosítását, valamint a GDPR 49. cikk (1) bekezdésének második albekezdése szerinti továbbítás esetében a megfelelő garanciák leírása;
- a különböző adatkategóriák törlésére előirányzott határidők;
- az adatkezelés biztonsága érdekében alkalmazott technikai és szervezési intézkedések általános leírása.

Ez a nyilvántartás a Társaság személyes adatkezeléseket tartalmazó adatvagyon leltára, amely tartalmazza az adatkezelésekre vonatkozó, a GDPR-ban előírt részletes információkat.

Amennyiben a Társaság adatfeldolgozó tevékenységet végez, a szervezeti egységek által megküldött dokumentumok és információk alapján az adatvédelmi tisztviselő a Társaság egészére vonatkozóan a más adatkezelő nevében végzett adatkezelési tevékenységekről szintén nyilvántartást vezet (adatfeldolgozói nyilvántartás), a következő tartalommal:

- adatfeldolgozó neve, elérhetőségei; az adatkezelők és adatvédelmi tisztviselőik, képviselőik neve és elérhetőségei;
- az egyes adatkezelők nevében végzett adatkezelési tevékenységek kategóriái;
- harmadik országba vagy nemzetközi szervezet részére történő adattovábbítás esetén a továbbításra vonatkozó információk, beleértve a harmadik ország vagy a nemzetközi szervezet azonosítását, valamint a GDPR 49. cikk (1) bekezdésének második albekezdése szerinti továbbítás esetében a megfelelő garanciák leírása;
- az adatfeldolgozás biztonsága érdekében alkalmazott technikai és szervezési intézkedések általános leírása.

A nyilvántartást írásban kell vezetni, ideértve az elektronikus formátumot is. Erre irányuló megkeresés esetén az adatvédelmi tisztviselő a NAIH rendelkezésére bocsátja az e pont szerinti nyilvántartásokat.

12. Az adatvédelmi incidensek nyilvántartása, bejelentése

A Társaság, mint adatkezelő a nála vagy megbízott adatfeldolgozójánál felmerülő esetleges adatvédelmi incidenseket dokumentálni köteles, ezekről a szervezeti egységek által megküldött információk alapján a Társaság adatvédelmi tisztviselője vezet nyilvántartást.
A nyilvántartás tartalmazza az incidens időpontját, az adatvédelmi incidenssel érintettek körét és számát, az érintett személyes adatok körét, az incidens körülményeit és annak hatásait, az elhárítására tett intézkedések leírását, valamint az adatkezelést előíró jogszabályban meghatározott adatokat (GDPR 33., 34. cikkben foglaltak alapján). Ebben nem az incidenssel összefüggő konkrét személyes adatokat kell feltüntetni, hanem az érintettek és adatok behatárolására, az érintettek körére vonatkozó információkat.
Ennek érdekében a szervezeti egységek az esetlegesen felmerült adatvédelmi incidensekről a BEBD igazgatóját – a fentiekben felsorolt, dokumentált adatok feltüntetésével – haladéktalanul, de legkésőbb 24 órán belül kötelesek tájékoztatni az 5. számú mellékletben lévő adatlap kitöltésével, illetve annak az incidensbejelentés@hmei.hu címre történő elektronikus megküldésével.

A BEBD igazgató, amennyiben megállapítja, hogy adatvédelmi incidens történt, erről a bejelentés továbbításával az adatvédelmi tisztviselőt haladéktalanul tájékoztatja.
Az adatvédelmi tisztviselő az adatvédelmi incidenst indokolatlan késedelem nélkül, az incidens megállapításától számított legkésőbb 72 órán belül bejelenti a NAIH-nak a hatóság által erre a célra biztosított elektronikus felületen, vagy annak hiánya, illetve nem működése esetén a GDPR 33. cikkben foglaltak alapján a 6. számú mellékletben szereplő kitöltött adatlap NAIH részére történő elektronikus úton történő megküldésével. Ha a bejelentés nem történik meg 72 órán belül, mellékelni kell hozzá a késedelem igazolására szolgáló indokokat is. Az adatvédelmi incidens megtörténtéről, illetve bejelentéséről az adatvédelmi tisztviselő a vezérigazgatót tájékoztatja. Nem kell az adatvédelmi incidenst bejelentenie, ha az valószínűsíthetően nem jár kockázattal az érintett természetes személyek jogaira nézve.

A bejelentésben közölni kell legalább:

a) az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát;
b) az adatvédelmi felelős vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;
c) az adatvédelmi incidensből eredő, valószínűsíthető következményeket;
d) a Társaság által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

Ha az adatvédelmi incidens az adatvédelmi tisztviselő megítélése szerint valószínűsíthetően magas kockázattal jár a természetes személyek jogaira nézve, a Társaság indokolatlan késedelem nélkül tájékoztatja az érintetteket az adatvédelmi incidensről. Az érintettek részére adott tájékoztatásban világosan és közérthetően ismertetni kell az adatvédelmi incidens jellegét, és közölni kell a felügyeleti hatóságnak küldött bejelentés b)-d) pontjaiban szereplő információkat és intézkedéseket.

Az érintettek tájékoztatása mellőzhető, ha a következő feltételek bármelyike teljesül:

a) a Társaság, mint adatkezelő megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre, és ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében alkalmazták, különösen azokat az intézkedéseket – mint például a titkosítás alkalmazása –, amelyek a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik az adatokat;
b) az adatkezelő az adatvédelmi incidenst követően olyan további intézkedéseket tett, amelyek biztosítják, hogy az érintett jogaira jelentett magas kockázat a továbbiakban valószínűsíthetően nem valósul meg;
c) a tájékoztatás (például az érintettek magas száma miatt) aránytalan erőfeszítést tenne szükségessé. Ilyen esetekben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, vagy olyan hasonló intézkedést kell hozni, amely biztosítja az érintettek hasonlóan hatékony tájékoztatását.

A NAIH elrendelheti az érintettek tájékoztatását, vagy megállapíthatja az érintettek tájékoztatásának szükségtelenségét.
A Társaság incidenskezelési eljárásrendjének részleteit a 4. számú melléklet tartalmazza.

Az adatkezelési tevékenységek nyilvántartásában és az adatvédelmi incidens nyilvántartásban az adatokat 5 évig, különleges adatok esetében 20 évig kell megőrizni.

13. Az érintett jogai és érvényesítésük

13.1. Kérelmek megválaszolása

A tájékoztatásra/helyesbítésre/törlésre/korlátozásra/tiltakozásra irányuló, vagy a 13. pont szerinti egyéb kérelem (ide nem értve az érintett adataiban bekövetkező változás átvezetése céljából történő megkeresést) beérkezéséről az arról tudomást szerző szervezeti egység haladéktalanul tájékoztatja az adatvédelmi tisztviselőt. A szervezeti egység a beérkezett kérelem alapján azonosítja vagy megkísérli azonosítani az érintettet. Ha a szervezeti egységnek megalapozott kétségei vannak a kérelmet benyújtó természetes személy kilétével kapcsolatban, további, az érintett személyazonosságának megerősítéséhez szükséges információk nyújtását kérheti.
A szervezeti egység tájékoztatása alapján az adatvédelmi tisztviselő a válaszlevelet elkészíti, és a vezérigazgatóhoz felterjeszti. A vezérigazgató jóváhagyása esetén az adatvédelmi tisztviselő gondoskodik a válasz érintettel történő közléséről. A tájékoztatást a kérelem beérkezését követően legfeljebb egy hónapon belül a kérelmező részére meg kell adni, írásban, vagy elektronikus úton, tömör átlátható, érthető és könnyen hozzáférhető formában, kitérve a kérelem nyomán megtett intézkedésekre is vagy az intézkedés elmaradásának okaira, valamint ez utóbbi esetben arra, hogy az érintett panaszt nyújthat be valamely felügyeleti hatóságnál, és élhet bírósági jogorvoslati jogával. Az érintett kérésére szóbeli tájékoztatás is adható, feltéve, hogy az érintett igazolta személyazonosságát. ***Az érintett kérelmének a teljesítése nem tagadható meg, kivéve, ha a szervezeti egység bizonyítja, hogy az érintettet nem áll módjában azonosítani.***
Szükség esetén – figyelembe véve a kérelem összetettségét és a kérelmek számát – a válaszadási határidő további két hónappal meghosszabbítható. A határidő meghosszabbításáról az adatvédelmi tisztviselő a késedelem okainak megjelölésével a kérelem kézhezvételétől számított egy hónapon belül tájékoztatja az érintettet. Ha az érintett elektronikus úton nyújtotta be a kérelmet, a tájékoztatást lehetőség szerint elektronikus úton kell megadni, kivéve, ha az érintett azt másként kéri.
A tájékoztatást és intézkedést díjmentesen kell biztosítani. Ha az érintett kérelme egyértelműen megalapozatlan vagy – különösen ismétlődő jellege miatt – túlzó, a Társaság, figyelemmel a kért információ vagy tájékoztatás nyújtásával vagy a kért intézkedés meghozatalával járó adminisztratív költségekre:

a) észszerű összegű díjat számíthat fel, vagy
b) megtagadhatja a kérelem alapján történő intézkedést.

A kérelem egyértelműen megalapozatlan vagy túlzó jellegének bizonyítása a Társaságot, mint adatkezelőt terheli. A szervezeti egység köteles az adatvédelmi tisztviselő rendelkezésére bocsátani a kérelem megalapozatlan vagy túlzó jellegét alátámasztó bizonyítékokat.

13.2. Az érintett hozzáférési joga (tájékoztatáshoz való jog)

Az érintett a Társaságtól tájékoztatást kérhet személyes adatainak kezelésével kapcsolatban és jogosult arra, hogy a személyes adatokhoz és az adatkezeléssel kapcsolatos alábbi információkhoz hozzáférést kapjon:

a) az adatkezelés céljai;
b) az érintett személyes adatok kategóriái;
c) azon címzettek vagy címzettek kategóriái, akikkel, illetve amelyekkel a személyes adatokat közölték vagy közölni fogják, ideértve különösen a harmadik országbeli címzetteket, illetve a nemzetközi szervezeteket;
d) a személyes adatok tárolásának tervezett időtartama, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjai;

e) az érintett azon joga, hogy kérelmezheti az adatkezelőtől a rá vonatkozó személyes adatok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen;
f) a NAIH-hoz címzett panasz benyújtásának joga;
g) ha az adatokat nem az érintettől gyűjtötték, a forrásukra vonatkozó minden elérhető információ;
h) amennyiben a Társaság az adatkezelés során automatizált döntéshozatalt (ideértve a profilalkotást is) alkalmaz, ennek ténye, valamint ezekben az esetekben legalább az alkalmazott logikára és arra vonatkozó érthető információk, hogy az ilyen adatkezelés milyen jelentőséggel bír, és az érintettre nézve milyen várható következményekkel jár.;
i) ha a személyes adat harmadik országba vagy nemzetközi szervezet részére kerül továbbításra, az érintettet kérésére tájékoztatni kell a GDPR 46. cikke szerinti megfelelő garanciákról.

Kérésre a Társaság az általa kezelt személyes adatok másolatát az érintett rendelkezésére bocsátja. Ha az érintett elektronikus úton nyújtotta be a kérelmet, az adatokat elektronikus formátumban kell rendelkezésre bocsátani, kivéve, ha az érintett másként kéri. A másolat igénylésére vonatkozó jog nem érintheti hátrányosan mások jogait és szabadságait, ezért, ha a másolaton más személyek személyes adatai is vannak, azt el kell távolítani, vagy egyéb módon gondoskodni kell az azonosíthatatlanná tételről.

A tájékoztatás megtagadása esetén írásban közölni kell az érintettel, hogy a felvilágosítás megtagadására milyen uniós vagy hazai jogszabály rendelkezése alapján került sor, továbbá tájékoztatni kell a bírósági jogorvoslat, továbbá a NAIH-hoz fordulás lehetőségéről.

13.3. Helyesbítéshez és törléshez való jog

Az érintett téves adatrögzítés észlelése esetén kérheti a kezelt személyes adatainak helyesbítését, hiányos adatainak kiegészítését. Az érintett – a kötelező adatkezelés kivételével – kérheti a kezelt személyes adatainak törlését.
A valóságnak nem megfelelő adatot 30 napon belül helyesbíteni kell.
Az érintett kérésére a személyes adatot indokolatlan késedelem nélkül, de lehetőség szerint 30 napon belül törölni kell, ha

a) a személyes adatokra már nincs szükség abból a célból, amelyből azokat gyűjtötték vagy más módon kezelték;
b) az érintett visszavonja az adatkezelés alapját képező hozzájárulását, és az adatkezelésnek nincs más jogalapja;
c) az érintett a GDPR 21. cikk (1) bekezdése alapján tiltakozik az adatkezelése ellen, és nincs elsőbbséget élvező jogszerű ok az adatkezelésre, vagy az érintett a GDPR 21. cikk (2) bekezdése alapján tiltakozik az adatkezelés ellen;
d) a személyes adatokat jogellenesen kezelték;
e) a személyes adatokat a Társaságra, mint adatkezelőre alkalmazandó uniós vagy tagállami jogban előírt jogi kötelezettség teljesítéséhez törölni kell;
f) a személyes adatok gyűjtésére közvetlenül gyermekeknek kínált, információs társadalommal összefüggő szolgáltatások kínálásával kapcsolatosan került sor.

Nem törölhető a személyes adat az érintett kérésére, amennyiben az adatkezelés szükséges

a) a véleménynyilvánítás szabadságához és a tájékozódáshoz való jog gyakorlása céljából (pl. közérdekből nyilvános adatok esetén),

b) a személyes adatok kezelését előíró, a Társaságra alkalmazandó uniós vagy hazai jogszabály szerinti kötelezettség teljesítése, illetve közérdekből vagy a Társaságra ruházott közhatalmi jogosítvány gyakorlása keretében végzett feladat végrehajtása céljából,
c) a GDPR 9. cikk (2) bekezdése h) és i) pontjának, valamint a 9. cikk (3) bekezdésének megfelelően a népegészségügy területét érintő közérdek alapján,
d) a GDPR 89. cikk (1) bekezdésével összhangban a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból, amennyiben az (1) bekezdésben említett jog valószínűsíthetően lehetetlenné tenné vagy komolyan veszélyeztetné ezt az adatkezelést vagy
e) jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez.

Ha a Társaság már nyilvánosságra hozta a személyes adatot, és azt törölni köteles, az elérhető technológia és a megvalósítás költségeinek figyelembevételével megteszi az észszerűen elvárható lépéseket – ideértve technikai intézkedéseket – annak érdekében, hogy tájékoztassa az adatokat kezelő adatkezelőket, hogy az érintett kérelmezte tőlük a szóban forgó személyes adatokra mutató linkek vagy e személyes adatok másolatának, illetve másodpéldányának törlését.

A Társaság minden olyan címzettet tájékoztat a helyesbítésről vagy törlésről, akivel, illetve amellyel a személyes adatot közölték, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel. Az érintettet kérésére a Társaság tájékoztatja e címzettekről.

13.4. Az adatkezelés korlátozásához való jog

Az érintett a Társaságtól kérheti személyes adata kezelésének korlátozását, az alábbi esetekben:
- az érintett vitatja a személyes adat pontosságát, ez esetben a korlátozás arra az időtartamra vonatkozik, amely lehetővé teszi, hogy az adatkezelő ellenőrizze a személyes adat pontosságát;
- az adatkezelés jogellenes, és az érintett ellenzi az adat törlését, és ehelyett kéri a felhasználásának korlátozását;
- az adatkezelőnek már nincs szüksége a személyes adatra adatkezelés céljából, de az érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez vagy
- az érintett a GDPR 21. cikk (1) bekezdése szerint tiltakozott az adatkezelés ellen; ez esetben a korlátozás arra az időtartamra vonatkozik, amíg megállapításra nem kerül, hogy az adatkezelő jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben.

A Társaság az érintettet, akinek a kérésére korlátozták az adatkezelést, az adatkezelés korlátozásának feloldásáról előzetesen tájékoztatja.

Ha az adatkezelés az érintett kérelme alapján korlátozás alá esik, az ilyen személyes adatot a tárolás kivételével csak az érintett hozzájárulásával, vagy jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez, vagy más természetes vagy jogi személy jogainak védelme érdekében, vagy az Európai Unió, illetve valamely tagállam fontos közérdekéből lehet kezelni.

A Társaság minden olyan címzettet tájékoztat az adatkezelés-korlátozásról, akivel, illetve amellyel a személyes adatot közölték, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel. Az érintettet kérésére a Társaság tájékoztatja e címzettekről.

13.5. Adathordozhatósághoz való jog

Az érintett jogosult arra, hogy a rá vonatkozó, általa a Társaság rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja, továbbá jogosult arra, hogy ezeket az adatokat egy másik adatkezelőnek továbbítsa, ha:

a) az adatkezelés az érintett hozzájárulásán alapul vagy az érintettel kötött szerződés teljesítéséhez szükséges; és
b) az adatkezelés automatizált módon történik.

Az adatok hordozhatóságához való jog gyakorlása során az érintett jogosult arra, hogy – ha ez technikailag megvalósítható – kérje a személyes adatok adatkezelők közötti közvetlen továbbítását.

Az adatok hordozhatóságához való jog nem alkalmazandó abban az esetben, ha az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítványai gyakorlásának keretében végzett feladat végrehajtásához szükséges. Az adathordozhatósághoz való jog gyakorlása

- nem érintheti hátrányosan mások jogait;
- nem járhat automatikusan az adat törlésével (mindaddig meg kell őrizni az adatot, amíg az adatkezelés célja fennáll);
- nem érinti az átvitt adatokra vonatkozó eredeti megőrzési időszakot.

Meg kell teremteni a biztonságos adatátadás feltételeit. Az adathordozhatósághoz való jog a származtatott adatokra nem terjed ki.

13.6. Tiltakozás személyes adat kezelése ellen

Az érintett a saját helyzetével kapcsolatos okokból bármikor tiltakozhat személyes adatának kezelése és az azon alapuló profilalkotás ellen,

a) ha a személyes adatok kezelése közérdekű vagy a Társaságra ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges;
b) ha a személyes adatok kezelése a Társaság vagy harmadik fél jogos érdekének érvényesítéséhez szükséges;
c) ha a személyes adat kezelése közvetlen üzletszerzés érdekében történik; valamint
d) ha a személyes adatok kezelésére tudományos és történelmi kutatási célból vagy statisztikai célból kerül sor, kivéve, ha az adatkezelésre közérdekű okból végzett feladat végrehajtása érdekében van szükség.

Az a) és b) pontokban szabályozott esetekben a Társaság a tiltakozást követően is kezelheti az érintett adatokat, ha bizonyítja, hogy az adatkezelést olyan kényszerítő erejű jogos okok indokolják, amelyek elsőbbséget élveznek az érintett érdekeivel, jogaival szemben, vagy amelyek jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódnak.

Az a)-c) pont szerinti jogra legkésőbb az érintettel való első kapcsolatfelvétel során kifejezetten fel kell hívni annak figyelmét, és az erre vonatkozó tájékoztatást egyértelműen és minden más információtól elkülönítve kell megjeleníteni.

Ha a fentiek alapján az kerül megállapításra, hogy az érintett tiltakozása megalapozott, az adatkezelést végző szervezeti egység az adatkezelést – beleértve a további adatfelvételt és adattovábbítást is – megszünteti, és az adatokat törli, valamint a tiltakozásról, továbbá az annak alapján tett intézkedésekről értesíti mindazokat, akik részére a tiltakozással érintett személyes

adatot korábban továbbította, és akik kötelesek intézkedni a tiltakozási jog érvényesítése érdekében. A szervezeti egység ezen intézkedéseiről az adatvédelmi tisztviselőt tájékoztatja, aki elkészíti a válaszlevelet és a vezérigazgatóhoz felterjeszti. A vezérigazgató jóváhagyása esetén az adatvédelmi tisztviselő gondoskodik a válasz érintettel történő közléséről.

13.7. Automatizált döntéshozatal elleni tiltakozás

Az érintett jogosult arra, hogy ne terjedjen ki rá az olyan, kizárólag automatizált adatkezelésen – ideértve a profilalkotást is – alapuló döntés hatálya, amely rá nézve joghatással járna vagy őt hasonlóképpen jelentős mértékben érintené (pl. elesne valamilyen előnytől).

A tiltakozás lehetősége nem alkalmazandó abban az esetben, ha a döntés:
a) az érintett és a Társaság, mint adatkezelő közötti szerződés megkötése vagy teljesítése érdekében szükséges;
b) meghozatalát a Társaságra, mint adatkezelőre alkalmazandó olyan uniós vagy hazai jogszabály teszi lehetővé, amely az érintett jogainak, valamint jogos érdekeinek védelmét szolgáló megfelelő intézkedéseket is megállapít vagy
c) az érintett kifejezett hozzájárulásán alapul.

Az érintett jogosult arra, hogy az a) és c) pontban meghatározott, kizárólag automatizált adatkezelésen – ideértve a profilalkotást is – alapuló döntés esetén a Társaságtól emberi beavatkozást kérjen, álláspontját kifejezze és a döntéssel szemben a Társaságnál kifogást nyújtson be.

Az a)-c) pontban említett döntések nem alapulhatnak különleges személyes adatokon, kivéve, ha a GDPR 9. cikk (2) bekezdésének a) vagy g) pontja alkalmazandó, és az érintett jogainak, szabadságainak és jogos érdekeinek védelme érdekében megfelelő intézkedések megtételére került sor.

Az érintett kérelmében előadottak alapján az adatkezelést végző szervezeti egység felülvizsgálja a döntést, illetve emberi beavatkozás révén új döntést hoz. Amennyiben az új döntés eredménye megegyezik a korábbi, automatizált döntéshozatal eredményével, az adatvédelmi tisztviselő útján erről is tájékoztatni kell az érintettet.

III. Kiemelendő egyéb adatkezelések

14. Kiemelendő egyéb adatkezelések csoportosítása

Az érintettek köre alapján a Társaság az alábbi adatkezeléseket végzi:

a) a munkavállalók munkaviszonyával, munkavégzésével kapcsolatos adatkezelések;
b) a Társaság által kötött polgári jogi szerződések teljesítése érdekében a szerződő partnerek, illetve bármely szerződő partnerrel munkajogi, polgári jogi vagy egyéb jogviszonyban álló természetes személyek, és/vagy munkavállalók tekintetében végzett adatkezelések;
c) a Társaság székhelyére és egyes telephelyeire történő be- és kiléptetéssel, megfigyeléssel kapcsolatban a munkavállalónak nem minősülő természetes személyek személyes adatainak kezelése.

15. A munkavállalók munkaviszonyával, munkavégzésével kapcsolatos adatkezelések

A Társaság munkavállalói (leendő munkavállalói) személyes adatait a munkaviszony létesítése előtt, a munkaviszony létesítésekor, a munkaviszony fennállása alatt, annak megszűnésekor és a megszűnést követően, valamint a munkavégzéssel összefüggésben kezeli.

A munkavállalót munkaszerződése megkötésekor tájékoztatni kell személyes adatainak kezeléséről. A munkavállalót a szerződés megkötése előtt az adatkezelés főbb feltételeiről szóban is tájékoztatni kell, majd át kell adni részére a részletes írásos adatkezelési tájékoztatót. A munkavállaló a tájékoztató megismerését és az abban foglaltak tudomásulvételét a tájékoztató egy példányának átvételével írásban igazolja. Az adatkezelési tájékoztatót a Társaság belső elektronikus hálózatán is folyamatosan elérhetővé kell tenni a Társaság munkavállalói számára.

15.1. A Társasággal munkaviszonyban álló munkavállalókra vonatkozó munkaügyi adatkezelés főbb szabályai

A munkavállalótól csak olyan nyilatkozat megtétele vagy adat közlése kérhető, amely személyiségi jogát nem sérti, és a munkaviszony létesítése, teljesítése vagy megszűnése szempontjából lényeges. A munkavállalóval szemben csak olyan alkalmassági vizsgálat alkalmazható, amelyet munkaviszonyra vonatkozó szabály ír elő, vagy amely munkaviszonyra vonatkozó szabályban meghatározott jog gyakorlása, kötelezettség teljesítése érdekében szükséges.

A Társaság a munkavállalóra vonatkozó tényt, adatot, véleményt harmadik személlyel csak törvényben meghatározott esetben vagy a munkavállaló hozzájárulásával közölhet.

A munkaviszonyból származó kötelezettségek teljesítése céljából a Társaság a munkavállaló személyes adatait – az adatszolgáltatás céljának megjelölésével, törvényben meghatározottak szerint – adatfeldolgozó számára átadhatja. Erről a munkavállalót előzetesen tájékoztatni kell.

A munkavállalóra vonatkozó adatok statisztikai célra felhasználhatók és statisztikai célú felhasználásra – hozzájárulása nélkül, személyazonosításra alkalmatlan módon – átadhatók.

A Társaság a munkavállaló írásbeli kérelmére/hozzájárulása alapján olyan adatokat is kezelhet, amelyek átadására törvény a munkavállalót nem kötelezi, a munkaszerződés teljesítéséhez nem szükséges, azonban ezen adatok csak a munkavállaló által megjelölt célra használhatók fel. Ezeket az adatokat elkülönítetten kell kezelni és az ezekben szereplő személyazonosító adatokat a munkavállaló kérésére haladéktalanul törölni kell. A munkavállaló írásbeli kérelmére kezelt adatok személyazonosításra alkalmatlan módon statisztikai célra felhasználhatók, illetve ezekből adatszolgáltatás végezhető.

A Társaságnál a Szabályzatban foglaltak figyelembevételével kell ellátni a munkaügyi nyilvántartás, valamint a bér- és társadalombiztosítási-, valamint adó nyilvántartás (a továbbiakban együtt: **munkaügyi nyilvántartás**) vezetését, továbbá a munkavállaló személyi iratainak és adatainak kezelését (a továbbiakban együtt: **munkaügyi adatkezelés**).

A munkavállaló a munkaügyi nyilvántartáshoz szükséges adatokat a munkaviszony létesítésekor a szerződés létrehozása és teljesítése érdekében a Humánpolitikai Divízió részére köteles megadni, és az adatváltozásokat haladéktalanul bejelenteni a Humánpolitikai Divízión.

A Humánpolitikai Divízió haladéktalanul köteles a munkaügyi nyilvántartásban átvezetni a munkavállaló által bejelentett adatváltozásokat.
A munkaügyi nyilvántartásban szereplő adatok körét a Szabályzat 1. számú melléklete tartalmazza.

A személyi iratok körébe az alábbiak tartozhatnak különösen:

- „Személyi anyag": nyilvántartó lap, személyi adatlap, önéletrajz, erkölcsi bizonyítvány, a munkavállaló legmagasabb iskolai végzettségére (több végzettség esetén valamennyire), szakképzettsége(i)re, idegennyelv-ismerete(i)re vonatkozó okiratok adatai, a munkaszerződés és annak módosítása(i), a módosításra irányuló engedély, a vezetői megbízás és annak visszavonása, a munkaviszonyt megszüntető irat, az írásbeli figyelmeztetésre, kártérítési felelősség megállapítására, hátrányos jogkövetkezmény alkalmazására vonatkozó irat;
- a munkavállaló munkaviszonyával összefüggő egyéb iratok (pl. a tanulmányi szerződés);
- a munkavállalónak a munkaviszonyával összefüggő más jogviszonyaival kapcsolatos iratok.

A munkaviszony létrehozásának elmaradása esetén a munkaviszony létrehozását kezdeményező iratokat – az ezzel kapcsolatos döntést követő 8 munkanapon belül – vissza kell adni az érintettnek.

A Társasággal munkavégzésre irányuló egyéb jogviszonyban álló személyekkel, illetve máshol ilyen jogviszonnyal rendelkező munkavállalók bejelentéseivel kapcsolatos nyilvántartást a Humánpolitikai Divízió vezeti.
A Társasággal munkavégzésre irányuló egyéb jogviszonyban álló személyekre vonatkozó nyilvántartásban szereplő adatok körét a Szabályzat 2. számú melléklete tartalmazza.

A munkaügyi nyilvántartás jogszerűségéért, a személyes adatok védelméért, valamint a személyes adatokból történő adatszolgáltatásért a Humánpolitikai Divízió vezetője a felelős.

15.2. A Társasággal munkaviszonyban álló munkavállalókra vonatkozó egyéb adatkezelések

A Társaság a munkaügyi adatkezelésen túl az adatkezelési tájékoztató mellékletében rögzített célból és jogalappal jogosult a munkavállaló személyes adatát kezelni.
Ennek keretében a Társaság különösen

- a munkavállaló elektronikus levelezésének és internet használatának ellenőrzésével kapcsolatban,
- a Társaság székhelyén, egyes telephelyein elektronikus megfigyelő rendszer, elektronikus be- és kiléptető rendszer alkalmazásával kapcsolatban,
- GPS alapú online nyomkövető szolgáltatás használatával,
- telekommunikációs eszközök biztosításával kapcsolatban

végez adatkezelést.

Amennyiben a szerződések szerződésszerű és maradéktalan teljesítéséhez fűződő jogos érdek alapján munkavállaló személyes adatainak kezelésére kerül sor (pl. kapcsolattartó), erről az érintettet belső szabályzatban előírt szerződéskísérő adatlapon kell tájékoztatni, melynek tudomásulvételételét az érintett aláírásával igazolja.

A munkavállaló hozzátartozójának személyes adatát a Társaság kivételesen, kizárólag a munkavállaló hozzátartozójának hozzájárulása alapján jogosult kezelni.

A munkavállalót a munkaügyi adatkezelések körébe nem tartozó adatkezelésekről a 15. pont szerint kell tájékoztatni.

Az adatkezelésekre vonatkozó részletes szabályok a Társaság külön belső szabályzóiban, illetve az adatkezelési tájékoztatóban találhatóak.

16. A Társasággal szerződő partnerek, illetve a partnerekkel munkajogi, polgári jogi vagy egyéb jogviszonyban álló természetes személyek tekintetében végzett adatkezelések

A Társaság tevékenysége során a Társaság és a szerződő fél között létrejövő jogviszonyra vonatkozó tények dokumentálására nyilvántartást vezet ezen szerződésekről (szerződés-nyilvántartás), továbbá törvényben előírt adó és számviteli kötelezettségek teljesítése (könyvelés, adózás) céljából kezeli a vevőként, szállítóként vele üzleti kapcsolatba lépő természetes személyek törvényben meghatározott adatait.

A Társasággal jelen Szabályzat és külön adatkezelési tájékoztató honlapon történő kihelyezésével tájékoztatja szerződéses kapcsolatban állt, álló vagy szerződni kívánó partnereit az általa végzett adatkezelésekről.

Az érintett felet a szerződés megkötése előtt vagy a szerződés megkötésekor külön is tájékoztatni kell a 4.2.1. pontban meghatározott információk közlésével.

17. A Társaság székhelyére és egyes telephelyeire történő ki- és beléptetéssel, illetve az érintettek megfigyelésével kapcsolatos adatkezelések

17.1. A Társaság székhelyére és egyes telephelyeire történő ki- és beléptetéssel kapcsolatos adatkezelések

A Társaság a székhelyén és egyes telephelyein az ingatlanokból történő ki-, illetve az azokba történő belépők vonatkozásában **elektronikus be- és kiléptető rendszert** alkalmaz.

Az elektronikus beléptető rendszer vonatkozásában a beléptető rendszer előtt adatkezelési tájékoztatót kell elhelyezni.

Az adatkezelésre vonatkozó részletes információkat a recepcióknál kihelyezett, illetve közzétett részletes adatkezelési tájékoztatók tartalmazzák.

A be- és kiléptetés vonatkozásában adatkezelési tájékoztatót kell elhelyezni, továbbá az adatkezelésre vonatkozó részletes információkat a kihelyezett, illetve közzétett részletes adatkezelési tájékoztatóból ismerheti meg az érintett.

17.2. Az érintettek megfigyelésével kapcsolatos adatkezelések

A Társaság az emberi élet, testi épség, személyi szabadság védelme és a vagyonvédelem céljából a székhelyén és egyes telephelyein **elektronikus megfigyelő rendszert, kamerát**

üzemeltet, amely során személyes adatokat kezel. Erről az ingatlanok területére belépők figyelmét a bejáratnál jól látható piktogrammal és feliratokkal hívja fel.

Az érintettek a recepciókon elhelyezett adatkezelési tájékoztatóból informálódhatnak a Társaság adatkezeléssel kapcsolatos tevékenységéről.

IV. Adatbiztonsági alapelvek, rendszabályok

18. Védelmi alapelvek

Az adatokat a természetes személyek jogaira jelentett esetleges kockázatokhoz igazodóan megfelelő technikai és szervezési eljárási szabályokkal, intézkedésekkel védeni kell, különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen. A „kockázat" olyan eshetőség, amely a súlyosság és valószínűség szempontjából jellemez valamilyen eseményt és annak következményeit.

Az adatkezelő köteles az egyes adatkezelési műveleteket, műveletcsoportokat úgy megtervezni és végrehajtani, hogy az biztosítsa az érintettek magánszférájának védelmét.

Az adatkezelő, illetőleg tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról.

A Társaságnak az adatok biztonságát szolgáló intézkedések meghatározásakor és alkalmazásakor tekintettel kell lennie a technika mindenkori fejlettségére. Több lehetséges adatkezelési megoldás közül azt kell választani, amely a személyes adatok magasabb szintű védelmét biztosítja, kivéve, ha az aránytalan nehézséget jelentene a Társaságnak.

Az adatbiztonsági rendszabályok érvényesítése érdekében a szükséges intézkedéseket meg kell tenni mind a papír alapon, mind az elektronikusan kezelt és feldolgozott személyes adatok biztonsága érdekében.

A konkrét védelmi intézkedések kidolgozása során az alábbi alapelveket kell figyelembe venni:

- **Tudatosság**: az informatikai rendszerekbe vetett bizalom növelése érdekében minden azt használó személynek legalább alapszinten ismernie kell a biztonsági módszereket és eljárásokat.
- **Felelősség:** az informatikai rendszerek és felhasználóinak biztonságot érintő felelősségének egyértelműnek és világosnak kell lennie.
- **Arányosság:** a biztonsági fokozatoknak és intézkedéseknek megfelelőnek és arányosnak kell lenniük a védett rendszerek értékével és megbízhatósági követelményeivel, a biztonság fokozásának költségeivel, illetve a biztonság megsértéséből eredő potenciális károk súlyosságával és valószínűségével.
- **Aktualitás:** a biztonságot gyakori időközönként újra kell gondolni, és fel kell frissíteni a biztonság megsértéséből eredő potenciális kockázatok és következmények változásainak megfelelően. (Kockázatelemzés-kockázatkezelés).
- **Integráció:** koherens és integrált biztonsági megközelítés szükséges egy információrendszer összes elemének tekintetében.

- **Reakciókészség:** az összes résztvevőnek együtt kell működnie a biztonság sérülésének, megsértésének megelőzése és a megsértésre adandó gyors válasz érdekében.

A Társaságon, illetve a szervezeti egységen belül az egyes adatkezelési műveletek vonatkozásban ki kell alakítani a hozzáférési/jogosultsági szinteket. A jogosulatlan hozzáférés elkerülése érdekében fel kell készíteni a fizikai védelmi rendszert az illetéktelen behatolások elhárítására, az „infokommunikációs" infrastruktúra üzemeltetőit pedig ezek észlelésére, elhárítására, továbbá az eszközök jogosulatlan használatának megakadályozására.

19. Az elektronikusan tárolt adatok védelme

Megfelelő technikai védelemmel kell biztosítani, hogy eltérő célú elektronikus nyilvántartások ne legyenek közvetlenül összekapcsolhatók és az érintetthez rendelhetők.

Automatizált adatfeldolgozás során biztosítani kell a jogosulatlan személyek általi adatbevitel és felhasználás megakadályozását, üzemzavar esetén a rendszer helyreállíthatóságát. Naplózni kell azt, hogy kik, mikor, milyen adatokat vittek be a nyilvántartásba, kiknek továbbították az adatokat, vagy milyen hibák fordultak elő.

Az elektronikus eszközön, számítógépen, illetve hálózati meghajtókon tárolt személyes adatok biztonsága vonatkozásában az EIIBSZ előírásait kell alkalmazni.

20. A papír alapon kezelt adatok védelme

A papír alapon kezelt személyes adatok biztonsága érdekében az alábbi intézkedéseket kell foganatosítani.

- **Tűz- és vagyonvédelem:** az irattári kezelésbe vett iratokat jól zárható, száraz, tűz- és vagyonvédelmi riasztó berendezéssel ellátott helyiségben kell elhelyezni.
- **Hozzáférés-védelem:** a folyamatos aktív kezelésben lévő iratokhoz csak az illetékes ügyintézők férhetnek hozzá. A bér- és munkaügyi iratokat lemez szekrényben, a munkavállalók jogviszonnyal kapcsolatos személyi iratait pedig különálló, zárható helyiségben, zárható iratszekrényekben kell őrizni.

21. Adatbiztonsági intézkedések

Személyes adatok kezelése esetén az adatkezelést végző szervezeti egység a BEBD-val, az EII illetékes munkavállalójával, valamint az adatvédelmi tisztviselővel együttműködve köteles kidolgozni az egy nyilvántartási rendszerben tárolt és/vagy a természetes személyek jogaira azonos súlyú kockázatot jelentő személyes adatkezeléshez kapcsolódó adatbiztonsági és adatvédelmi technikai és szervezési intézkedéseket (**adatbiztonsági intézkedéseket**), a kockázat mértékének megfelelő adatbiztonság kialakítása érdekében. Ennek kialakítása során a szervezeti egység különösen az alábbi intézkedések bevezetését fontolhatja meg, a jelen Szabályzatban foglalt elvek megvalósítása érdekében:

- a személyes adatok álnevesítését és titkosítását, vagy speciális hozzáférési jogosultságok biztosítását egyes munkavállalók számára;
- a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítását, integritását, rendelkezésre állását és ellenálló képességét;

- fizikai vagy műszaki incidens esetén az arra való képességet, hogy a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását kellő időben vissza lehet állítani;
- az adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedések hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárást;
- a személyes adatokhoz hozzáféréssel rendelkező természetes személyek kizárólag a szervezeti egység vezetője utasításainak, belső szabályzóknak és a jogszabályi előírásoknak megfelelően kezelhetik a személyes adatokat, ennek érdekében belső oktatások tartása, valamint az adatkezelési tevékenység rendszeres vezetői ellenőrzése javasolt.

22. Előzetes adatvédelmi hatásvizsgálat

Az adatkezelő szervezeti egység a tervezett adatkezelés bevezetése előtt, vagy az adatkezelés megváltoztatásának bevezetése előtt a 4.3. pontban foglaltak szerint tájékoztatja az adatvédelmi tisztviselőt. **Amennyiben az adatkezelés – figyelemmel annak jellegére, hatókörére, körülményére és céljaira, különösen új technológiák alkalmazása esetén – valószínűsíthetően magas kockázattal jár a természetes személyek jogaira nézve**, az adatvédelmi tisztviselő kezdeményezésére a szervezeti egység előzetes hatásvizsgálatot végez arra vonatkozóan, hogy a tervezett adatkezelési műveletek a személyes adatok védelmét hogyan érintik, melynek elvégzését az adatvédelmi tisztviselő figyelemmel kíséri. Az egymáshoz hasonló típusú adatkezelési műveletek, amelyek egymáshoz hasonló magas kockázatokat jelentenek, egyetlen hatásvizsgálat keretei között is értékelhetőek.

Az adatvédelmi hatásvizsgálatot különösen az alábbi esetekben kell elvégezni:

a) természetes személyekre vonatkozó egyes személyes jellemzők olyan módszeres és kiterjedt értékelése, amely automatizált adatkezelésen – ideértve a profilalkotást is – alapul, és amelyre a természetes személy tekintetében joghatással bíró vagy a természetes személyt hasonlóképpen jelentős mértékben érintő döntések épülnek;
b) a különleges személyes adatok kategóriái, vagy a büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó személyes adatok nagy számban történő kezelése vagy
c) nyilvános helyek nagymértékű, módszeres megfigyelése esetén, valamint
d) az olyan adatkezelések esetében, amelyek esetén NAIH által kiadott jegyzékben meghatározottak szerint adatvédelmi hatásvizsgálat elvégzése indokolt. [1]

Ha a NAIH valamely meghatározott adatkezelés-típust magas kockázatú adatkezelésnek minősít, és e megállapítását közzéteszi, valamint a tervezett adatkezelés e megállapítással érintett adatkezelés-típus során alkalmazottal azonos vagy ahhoz hasonló típusú művelet vagy műveletsorozat alkalmazásával jár, a tervezett adatkezelés tekintetében annak magas kockázatát vélelmezni kell. A NAIH minősítéséről az adatvédelmi tisztviselő az adatkezelő szervezeti egységet soron kívül tájékoztatja.

---

[1] További szempontokat ad az uniós adatvédelmi munkacsoport vonatkozó (WP248) iránymutatása: http://naih.hu/files/Iranymutatas-az-adatvedelmi-hatasvizsgalat-elvegzesehez.pdf.
Az ebben foglaltak alapján valószínűsíthetően magas kockázattal járó adatkezelés, ha teljesül egy vagy több elem az alábbiak közül: az értékelésen vagy pontozáson alapuló, vagy profilalkotással járó adatkezelés, a joghatással vagy más jelentős hatással járó automatizált döntéshozatal, a módszeres, vagy folyamatos megfigyelés, a különleges vagy nagyszámú adat kezelése, különböző adatbázisok összevonása, a kiszolgáltatott helyzetben lévőkkel vagy munkavállalókkal kapcsolatos adatok kezelése, új technológia vagy szervezési megoldások innovatív használatával kezelt adatok, vagy amikor az adatkezelés kizár egyes egyéneket valamilyen előnyből, szolgáltatásból.

Az adatvédelmi hatásvizsgálat elvégzésére vonatkozó követelmény azokra a folyamatban lévő adatkezelési műveletekre is vonatkozik, amelyeknél valószínűsíthető, hogy magas kockázattal járnának a természetes személyek jogaira és szabadságaira nézve, és amelyek esetében megváltoztak a kockázatok, figyelemmel az adatkezelés jellegére, hatókörére, körülményére és céljára.

A hatásvizsgálat kiterjed legalább:

a) a tervezett adatkezelési műveletek módszeres leírására és az adatkezelés céljainak ismertetésére, beleértve adott esetben az adatkezelő által érvényesíteni kívánt jogos érdeket;
b) az adatkezelés céljaira figyelemmel az adatkezelési műveletek szükségességi és arányossági vizsgálatára;
c) az érintettek jogait érintő kockázatok vizsgálatára;
d) a kockázatok kezelését célzó intézkedések bemutatására, ideértve a személyes adatok védelmét és az érintettek és más személyek jogait és jogos érdekeit figyelembe vevő garanciákat, biztonsági intézkedéseket és mechanizmusokat;
e) az adatkezelés során esetlegesen alkalmazott ágazati adatkezelési magatartási kódexre és annak érvényesülésére.

A szervezeti egység kezdeményezésére, a vezérigazgató jóváhagyásával a Társaság adott esetben – a kereskedelmi érdekek vagy a közérdek védelmének vagy az adatkezelési műveletek biztonságának sérelme nélkül – kikérheti az érintettek vagy képviselőik véleményét a tervezett adatkezelésről.

Az adatvédelmi hatásvizsgálat elvégzésébe be kell vonni a BEBD igazgatóját, a Fizikai és Informatikai Biztonsági Osztály vezetőjét, a Jogi Divízió kijelölt jogtanácsosát, az EII által kijelölt személyt, továbbá azt megelőzően a szervezeti egység köteles az adatvédelmi tisztviselő tanácsát is kikérni, aki igény esetén segíti a hatásvizsgálat módszertanának meghatározását, illetve a hatásvizsgálat elvégzését követően a hatásvizsgálati jelentés elkészítését.

Az adatvédelmi hatásvizsgálat eredményét a szervezeti egységnek a 7. számú melléklet szerinti tartalommal írásos dokumentumban (hatásvizsgálati jelentésben) kell rögzítenie, és a kockázatokhoz igazodó gyakorisággal rendszeresen felül kell vizsgálnia/újra el kell végeznie. A szervezeti egység a hatásvizsgálat alapján elfogadja az adatbiztonsági intézkedéseket, amelyekkel a kockázatok elfogadhatók, illetve a GDPR előírásainak megfelelő szintre csökkenthetők.[2]

A szervezeti egység vezetője az adatkezelés megkezdését követően a rögzített adatbiztonsági intézkedések betartásának ellenőrzése céljából, továbbá az adatkezelési műveletek által jelentett kockázat változása esetén ellenőrzést folytat le annak értékelése miatt, hogy a személyes adatok kezelése az adatvédelmi hatásvizsgálati jelentésben foglaltak alapján történik-e. Ha eltérést tapasztal, erről az adatvédelmi tisztviselőt tájékoztatja.

Ha az adatvédelmi hatásvizsgálat, illetve annak utólagos követése megállapítja, hogy az adatkezelés az adatkezelő által a kockázat mérséklése céljából tett intézkedések hiányában (vagy azok ellenére) valószínűsíthetően magas kockázattal jár, a személyes adatok kezelését

[2] A hatásvizsgálat módszerére nézve a WP248 iránymutatás ágazatspecifikus hatásvizsgálatok kialakítását szorgalmazza, de megemlít pár már működő modellt is, pl. a francia CNIL által kiadott PIA Tools nevű alkalmazást. https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment

megelőzően az adatvédelmi tisztviselő konzultál a felügyeleti hatósági feladatokat ellátó NAIH-hal.
Ha a NAIH véleménye szerint a tervezett adatkezelés megsértené a GDPR rendelet vagy az Info tv. előírásait – különösen, ha az adatkezelő a kockázatot nem elégséges módon azonosította vagy csökkentette –, a NAIH legkésőbb a konzultáció iránti megkeresés kézhezvételétől számított nyolc héten belül írásban tanácsot ad, továbbá gyakorolhatja jogszabályban rögzített hatásköreit. Ez a határidő – a tervezett adatkezelés összetettségétől függően – hat héttel meghosszabbítható. Az eljárásra vonatkozó időtartamba nem számít bele a felügyeleti hatóság által kért tájékoztatás kérésig és annak teljesítéséig eltelt időtartam.

Az adatvédelmi tisztviselő a konzultáció során a felügyeleti hatóságot tájékoztatja:

a) az adatkezelésben részt vevő adatkezelő, közös adatkezelők és adatfeldolgozók feladatköreiről, különösen vállalkozáscsoporton belüli adatkezelés esetén;
b) a tervezett adatkezelés céljairól és módjairól;
c) az érintettek jogainak védelmében hozott intézkedésekről és garanciákról;
d) az adatvédelmi tisztviselő elérhetőségeiről;
e) az adatvédelmi hatásvizsgálatról; és
f) a felügyeleti hatóság által kért minden egyéb információról.

V. Jogkövetkezmények

23. Jogellenes adatkezelés és az adatbiztonság követelményei megszegésének jogkövetkezményei

A hatóság vizsgálata: a NAIH-nál bejelentéssel bárki vizsgálatot kezdeményezhet arra hivatkozással, hogy személyes adatok kezelésével, illetve a közérdekű adatok vagy a közérdekből nyilvános adatok megismeréséhez fűződő jogok gyakorlásával kapcsolatban jogsérelem következett be, vagy annak közvetlen veszélye fennáll.

Adatvédelmi hatósági eljárás (panasztételhez való jog): a személyes adatok védelméhez való jog érvényesülése érdekében a NAIH erre irányuló kérelemre adatvédelmi hatósági eljárást indít és hivatalból adatvédelmi hatósági eljárást indíthat. Az érintett hatósági eljárás lefolytatását kezdeményezheti, ha megítélése szerint személyes adatainak kezelése során az adatkezelő, illetve az általa megbízott vagy rendelkezése alapján eljáró adatfeldolgozó megsérti a személyes adatok kezelésére vonatkozó, jogszabályban vagy az Európai Unió kötelező jogi aktusában meghatározott előírásokat. A NAIH határozatával vagy mulasztásával szemben bírósági jogorvoslat kezdeményezhető. A NAIH határozat megtámadására nyitva álló keresetindítási határidő lejártáig, illetve közigazgatási per indítása esetén a bíróság jogerős határozatáig a vitatott adatkezeléssel érintett adatok nem törölhetők, illetve nem semmisíthetők meg.

Az adatkezelővel szembeni hatékony bírósági jogorvoslathoz való jog: Az érintett – a bírósági jogorvoslathoz való jogának érvényesítése érdekében – bírósághoz fordulhat, ha megítélése szerint az adatkezelő, illetve az általa megbízott vagy rendelkezése alapján eljáró adatfeldolgozó a személyes adatait a személyes adatok kezelésére vonatkozó, jogszabályban vagy az Európai Unió kötelező jogi aktusában meghatározott előírások megsértésével kezeli. Azt, hogy az adatkezelés a személyes adatok kezelésére vonatkozó, jogszabályban vagy az

Európai Unió kötelező jogi aktusában meghatározott előírásoknak megfelel, az adatkezelő, illetve az adatfeldolgozó köteles bizonyítani.
Ha a bíróság a kérelemnek helyt ad, és a jogsértés tényét megállapítja, úgy az adatkezelőt, illetve az adatfeldolgozót
a) a jogellenes adatkezelési művelet megszüntetésére,
b) az adatkezelés jogszerűségének helyreállítására, illetve
c) az érintett jogai érvényesülésének biztosítására
kötelezi.

Az érintettek képviselete: az érintett jogosult arra, hogy panaszának a nevében történő benyújtásával, a fenti jogoknak a nevében való gyakorlásával olyan nonprofit jellegű szervet, szervezetet vagy egyesületet bízzon meg, amelyet valamely tagállam jogának megfelelően hoztak létre, és amelynek az alapszabályában rögzített céljai a közérdeket szolgálják, és amely az érintettek jogainak és szabadságainak a személyes adataik vonatkozásában biztosított védelme területén tevékenykedik.

A kártérítéshez (sérelemdíjhoz) való jog: minden olyan személy, aki a GDPR szabályok megsértésének eredményeként vagyoni kárt szenvedett, vagy személyiségi jogsérelem érte, az elszenvedett kárért, illetve személyiségi jogának sérelméért az adatkezelőtől vagy az adatfeldolgozótól kártérítésre, illetve sérelemdíjra jogosult. Az adatkezelésben érintett valamennyi adatkezelő felelősséggel tartozik minden olyan kárért (személyiségi jogsérelemért), amelyet a GDPR szabályait sértő adatkezelés okozott. Az adatfeldolgozó csak abban az esetben tartozik felelősséggel az adatkezelés által okozott károkért (személyiségi jogsérelemért), ha nem tartotta be a GDPR rendeletben meghatározott, kifejezetten az adatfeldolgozókat terhelő kötelezettségeket, vagy ha az adatkezelő jogszerű utasításait figyelmen kívül hagyta vagy azokkal ellentétesen járt el. (GDPR 82. cikk) A kártérítés vagy sérelemdíj iránti igényeiket az érintettek a Ptk. vonatkozó rendelkezései szerint érvényesíthetik.

A Társaság munkavállalói az adatkezelési és/vagy adatbiztonsági feladatokkal kapcsolatos munkaviszonyból származó kötelezettségeik megsértéséért felelősséggel tartoznak.

VI. Záró, átmeneti és hatálybaléptető rendelkezések

24. Adatok megőrzése, selejtezése

A Szabályzat szerint kezelt, illetve feldolgozott adatok megőrzésére és selejtezésére vonatkozó szabályokat az EIIBSZ, a Társaság Biztonsági Rendszabályairól szóló Szabályzat, az Iratkezelési Szabályzat, valamint a vonatkozó egyéb belső szabályozási dokumentumok tartalmazzák.

25. Hatálybaléptető és átmeneti rendelkezések

Jelen Szabályzat 2018. május 25. napján lép hatályba, és ezzel egyidejűleg a Társaság 887/209. számú Adatvédelmi és Adatbiztonsági Szabályzata hatályon kívül helyezésre kerül.

Jelen Szabályzatot, valamint a munkavállalói adatkezeléssel kapcsolatos tájékoztatót és annak mellékletét valamennyi munkavállalóval meg kell ismertetni, melyben foglaltak tudomásulvételét a munkavállaló írásbeli nyilatkozattal köteles igazolni. Ennek végrehajtása a Szabályzat hatálybalépését követően munkajogi jogviszonyt létesítő munkavállalók tekintetében a Szabályzat 15. pontjában foglaltak szerint a Humánpolitikai Divízió feladata, a Szabályzat hatálybalépésekor már munkaviszonyban álló munkavállalók tekintetében a hatálybalépést követő 15 napon belül a közvetlen munkahelyi vezető felelőssége. A nyilatkozatokat szervezeti egységenként a Humánpolitikai Divízió részére kell átadni, ahol azok külön nyilvántartásba vételére kerül sor.

Mellékletek:
1. sz. melléklet: Munkaügyi nyilvántartás adatai (3 lap)
2. sz. melléklet: Munkavégzésre irányuló egyéb jogviszonyra vonatkozó nyilvántartás adatai (1 lap)
3. sz. melléklet: Szervezeti egységek adatkezeléseinek nyilvántartására szolgáló adatlap (1 lap)
4. sz. melléklet: Incidenskezelési eljárásrend (5 lap)
5. sz. melléklet: Adatvédelmi incidens nyilvántartásba vételére szolgáló adatlap (3 lap)
6. sz. melléklet: Adatvédelmi incidens bejelentő lap (3 lap)
7. sz. melléklet: Az adatvédelmi hatásvizsgálati jelentés tartalma (5 lap)

Budapest, 2018. május 25. -n

dr. Homonnai Ildikó
adatvédelmi tisztviselő

Készült: 2 példányban
Egy példány: 31 lap
Ügyintéző (tel.): dr. Homonnai Ildikó (45-910)
Kapják: 1. sz. pld.: Levéltár
2. sz. pld.: HM EI Zrt. Irattár

887/509

1. sz. melléklet a HM EI Zrt. …….nyt. számú Adatvédelmi és Adatbiztonsági Szabályzatához

2. számú példány

Munkaügyi nyilvántartás adatai

A nyilvántartás a munkavállaló alábbi személyügyi adatait tartalmazza:

- neve (születési neve);
- születési helye, ideje;
- anyja neve;
- állampolgársága;
- személyi azonosító igazolvány száma, érvényessége;
- útlevél száma, érvényessége (ha nincs érvényes személyi igazolványa);
- jogosítvány száma, érvényessége (csak akkor, ha a munkakör betöltéséhez szükséges);
- vagyonőri igazolvány száma, kelte, érvényessége, kiállító hatóság (csak akkor, ha a munkakör betöltéséhez szükséges);
- kamarai igazolvány száma, érvényessége (csak akkor, ha a munkakör betöltéséhez szükséges);
- adóazonosító jele;
- társadalombiztosítási azonosító jele (TAJ száma);
- munkaképesség csökkenéssel kapcsolatos információ (rehabilitációs hozzájáruláshoz kapcsolódó határozatok az Adóügyi és Szolgáltatási Osztályon, adózási vonatkozású adatok a Munkaügyi, illetve a Bér és Társadalombiztosítás Elszámolási Osztályon);
- foglalkozás egészségügyi vizsgálat eredménye, az alkalmasság lejárati dátuma (érvényessége);
- munka alkalmassági vizsgálatok érvényességének nyilvántartása.
- lakóhelye (irányítószámmal), lakcíme, tartózkodási helye, telefonszáma;
- nyugdíjas státuszával kapcsolatos információk (nyugdíjas törzsszám, nyugdíj típusa, kezdetének ideje);
- legmagasabb iskolai végzettsége (több végzettség esetén valamennyi), az oktatási intézmény neve, oklevél kelte, oklevél száma;
- szakképzettsége(i) megnevezése, intézmény neve, oklevél kelte, oklevél száma;
- iskolarendszeren kívüli oktatás keretében szerzett szakképesítése(i), valamint meghatározott munkakör betöltésére jogosító okiratok adatai;
- tudományos fokozata;
- idegennyelv-ismerete, típusa, okirat kelte, okirat száma, (az idegennyelv-tudást az államilag elismert nyelvvizsga eredményét igazoló bizonyítvánnyal, vagy azzal egyenértékű okirattal kell igazolni);
- képzésre, továbbképzésre, vezetőképzésre, átképzésre vonatkozó adatai;
- önéletrajz (korábbi szakmai pályafutás);
- alkalmazás jellege;
- statisztikai adatai;
- munkakör;
- munkakör(ök) megnevezése, betöltésének időtartama;
- szervezetben betöltött helye; a Társaságnál a munkaviszony kezdete;

- próbaidő kikötése esetén annak időtartama;
- a munkavállaló besorolása, besorolásának időpontja;
- hátrányos jogkövetkezményre vonatkozó iratok, figyelmeztetők, hatályos fegyelmi büntetés;
- jutalmazás, címadományozás, elismerés, kitüntetéseinek megnevezése, fokozata, adományozás éve;
- erkölcsi bizonyítvány száma, kelte (az Őrzés-védelmi Igazgatóságon dolgozó munkavállalók, valamint a pénztáros, vagy pénzkezelő munkakörben lévők esetében);
- vezetői megbízása, a megbízás megszűnésének adatai;
- alapjárandóságok;
- meghatározott egyéb juttatások nyilvántartása;
- a munkavállaló munkaviszonya megszűnésének/megszüntetésének időpontja, módja, felmondási idő, felmentési idő, a kapott végkielégítés adatai;
- összeférhetetlenséggel kapcsolatos adatok (pl. a munkavállaló bejelentése gazdasági társaságnál vezető tisztségviselői, illetve felügyelő bizottsági tagságával kapcsolatos megbízásáról);
- munkaszerződéstől eltérő foglalkoztatás adatai;
- munkaszerződés módosítások.

A nyilvántartás a munkavállaló alábbi bér-, társadalombiztosítási és munkaügyi adatait tartalmazza:

- neve (születési neve);
- születési helye, ideje;
- anyja neve;
- állampolgársága;
- családi állapota;
- lakóhelye (irányítószámmal), lakcíme, tartózkodási helye, telefonszáma;
- adóazonosító jele;
- társadalombiztosítási azonosító jele (TAJ száma);
- számlavezető bank neve, bankszámlaszáma;
- Tb kiskönyv (adatai) a jogviszonyok igazolására (korábbi munkahelyek kapcsán);
- a belépést megelőző munkahely megnevezése,
- a Társaságnál a munkaviszony kezdete;
- próbaidő kikötése esetén annak időtartama;
- a munkavállaló jelenlegi besorolása, besorolásának időpontja;
- rendes és rendkívüli munkaidővel, ügyelettel, készenléttel kapcsolatos dokumentumok;
- pótszabadság megállapításához kapcsolódó dokumentumok;
- szabadság kiadásával kapcsolatos dokumentumok;
- egyéb munkaidő-kedvezménnyel kapcsolatos nyilvántartások;
- kafetéria juttatással kapcsolatos adatok nyilvántartása;
- a munkavállaló munkaviszonya megszűnésének/megszüntetésének időpontja, módja, a megállapított végkielégítés adatai (felmondási idő, felmentés a munkavégzés alól);
- személyi jellegű kifizetések bérelemei;

- adózással kapcsolatos nyilatkozatok, családi kedvezmény (és járulékkedvezmény) érvényesítésének dokumentálása;
- pénzbeli ellátásokkal kapcsolatos nyilvántartás, dokumentumok;
- egyéb béren felüli juttatások (étkezési és önkéntes nyugdíjpénztári hozzájárulás) adatai;
- törvényileg meghatározott járulékok levonása, azok nyilvántartása adónemenként;
- munkabért terhelő levonások, letiltások egyedi adatai;
- a munkaviszony megszűnésekor/megszüntetésekor kiadásra kerülő – személyi és jövedelem adatokat tartalmazó – adó- és járulék igazolások és egyéb igazolások;
- magán-nyugdíjpénztári tagság megnevezése, tagi jogviszony kezdete (megszűnése);
- eltartottak adatai (név/születési név, lakcímkártya vagy nyilatkozat a lakcímről, születési hely és idő, anyja neve, adóazonosító, TAJ szám, esetleges fogyatékosság, emelt összegű családi pótlék igazolásával, rokonsági fok: saját gyermek, örökbe fogadott feltüntetése);
- önkéntes pénztári tagsággal kapcsolatos dokumentumok;
- évközi belépő esetén az előző munkahelyi szja. adatlapok, igazolás a munkaviszony megszűnésekor (a letiltások végett), ezek hiányában büntetőjogi nyilatkozat.

Készült: 2 példányban
Egy példány: 3 lap
Ügyintéző (tel.): dr. Homonnai Ildikó (45-910)
Kapják: 1. sz. pld.: Levéltár
2. sz. pld.: HM EI Zrt. Irattár

2. sz. melléklet a HM EI Zrt. ….nyt. számú Adatvédelmi és Adatbiztonsági Szabályzatához

2. számú példány

Munkavégzésre irányuló egyéb jogviszonyra vonatkozó nyilvántartás adatai

A munkavégzésre irányuló egyéb jogviszonyra vonatkozó nyilvántartás a megbízott természetes személy alábbi adatait tartalmazza:

- neve (születési neve);
- születési helye és ideje,
- anyja neve;
- állampolgársága;
- lakóhelye (irányítószámmal), lakcíme, tartózkodási helye, telefonszáma;
- társadalombiztosítási azonosító jele (TAJ száma);
- adóazonosító jele, adószáma (ha van);
- adózással kapcsolatos kötelező nyilatkozatok (pl. költség nyilatkozat, családi adókedvezmény);
- nyugdíjas státuszával kapcsolatos információk (nyugdíjas törzsszám, nyugdíj típusa, kezdetének ideje);
- számlavezető bank neve, számlaszáma.

A nyilvántartás tartalmazza továbbá

- a megbízás időtartama;
- a megbízás tárgya;
- díjazásra, számlázásra vonatkozó adatok;
- a szerződésben foglaltak teljesítésének igazolására jogosult vezető munkavállaló neve, beosztása;
- tájékoztatás a felmondás lehetőségéről;
- tájékoztatást arról, hogy a szerződésben nem szabályozott kérdésekben a Ptk. rendelkezései az irányadók;
- a megbízott nyilatkozata (igazolás) a megbízás melletti egyéb jogviszony(ok)ról.

Készült: 2 példányban
Egy példány: 1 lap
Ügyintéző (tel.): dr. Homonnai Ildikó (45-910)
Kapják: 1. sz. pld.: Levéltár
2. sz. pld.: HM EI Zrt. Irattár

887/509

3. sz. melléklet a HM EI Zrt. ……. nyt. számú Adatvédelmi és Adatbiztonsági Szabályzatához

2 sz. példány

SZERVEZETI EGYSEGEK ADATKEZELESEINEK NYILVANTARTASARA SZOLGALO ADATLAP

Adatokat kezelő szervezeti egység	
Szervezeti egység neve:	
Adatkezelési feladatokat végző személy:	
Telefonszám:	
Adatkezelés megnevezése	
Adatkezelés célja	
Jogalap	
Érintettek kategóriái	
Személyes adatok kategóriái	
Címzettek kategóriái	
Törlésre előirányzott határidő	
Adatbiztonsági intézkedések	
Adatok kezelésének időtartama	
Adatok forrása	
Tényleges adatkezelés helye	
Megjegyzés, egyéb információ	
Adatkezelés megnevezése	
Adatkezelés célja	
Jogalap	
Érintettek kategóriái	
Személyes adatok kategóriái	
Címzettek kategóriái	
Törlésre előirányzott határidő	
Adatbiztonsági intézkedések	
Adatok kezelésének időtartama	
Adatok forrása	
Tényleges adatkezelés helye	
Megjegyzés, egyéb információ	

Készült: 2 példányban
Egy példány: 1 lap
Ügyintéző (tel.): dr. Homonnai Ildikó (45-910)
Kapják: 1. sz. pld: Levéltár
2. sz. pld: HM EI Zrt. Irattár

4. sz. melléklet a HM EI Zrt. 887/505.....nyt. számú Adatvédelmi és Adatbiztonsági Szabályzatához
2. számú példány

Incidenskezelési eljárásrend

1. Kormányzati eseménykezelő központ / egyéb sérülékenység felügyelő központokból érkező incidensekre vonatkozó információk kezelése

A Belső Ellenőrzési és Biztonsági Divízió (a továbbiakban: BEBD) Fizikai és Informatikai Biztonsági Osztály kijelölt munkatársa folyamatosan figyeli a Kormányzati Eseménykezelő Központ által a kritikus hálózatbiztonsági eseményekről és sérülékenységekről közzétett figyelmeztetéseket (http://www.cert-hungary.hu/aggregator/sources/2), és az egyéb forrásból érkező riasztásokat.
Az esemény kezelésének folyamatát az *1. számú ábra* tartalmazza.

2. A számítástechnikai hálózat naplóállományának folyamatos figyelése/elemzése, automatikus incidens figyelés

Az informatikai rendszerek üzemeltetőinek naponta ellenőriznie kell a naplóállományok bejegyzéseit.
Adatvédelmi, adatbiztonságot veszélyeztető incidens esemény bekövetkeztekor, vagy ennek alapos gyanúja esetén a belső számítástechnikai biztonsági rendszernek (amennyiben alkalmas rá) automatikusan jelentést kell generálnia és elküldenie az információ biztonsággal megbízott szervezeti egység (BEBD) és a számítástechnikai üzemeltetéssel megbízott szervezeti egység, a Belső Informatikai Infrastruktura Csoport (BIICS) részére.
Az esemény kezelésének folyamatát a *2. számú ábra* tartalmazza.

3. Felhasználói bejelentésre történő incidens kezelés

A felhasználóknak munkavégzésük során tapasztalt minden olyan számítástechnikai rendellenességet be kell jelenteniük, amely a megszokott munkamenetükben fennakadást okoz, számítógépük működése a megszokottól eltér.
Az esemény kezelésének folyamatát *a 3. számú ábra* tartalmazza.

4. Általános szabályok

Az információbiztonsági szabályok megsértéséről az informatikusoknak jelentést kell tenniük a BEBD vezetőjének.

A BEBD igazgatója minősíti az incidenst a körülmények ismeretében, vagy eseti szakértői csoportot hoz létre az incidens körülményeinek kivizsgálására.

A BEBD vezetője az incidens súlyának ismeretében dönt a következményekről, az incidens kezeléséről és a hibák javításáról. Az informatikai biztonságban résztvevőknek - az informatikai vagy szakmai rendszergazdák szükség szerinti bevonásával - a riasztásokban szereplő sérülékenység elhárításakor a következők szerint kell eljárniuk:

- figyelembe kell venni a különböző informatikai biztonsági szabályozásokban a sérülékenységek elhárítására vonatkozó részeket,
- amennyiben az informatikai rendszer rendelkezik automatizált módszerrel az adott sérülékenység elhárítására, akkor azt azzal az eszközzel azonnal el kell kezdeni,
- amennyiben az informatikai rendszer nem rendelkezik automatizált módszerrel az adott sérülékenység elhárítására, akkor azt manuális módon kell azonnal elkezdeni,
- amennyiben a sérülékenység elhárítása belső erőforrásból nem kivitelezhető, akkor külsős szakértőket kell bevonni az elhárítás folyamatába.

Amennyiben a sérülékenység jellege olyan, hogy annak elterjedése megelőzhető, akkor belső figyelmeztetést kell kiadni belső e-mail rendszeren keresztül.
Ha a BEBD igazgatója megállapítja, hogy az incidens személyes adatokat (is) érint, erről haladéktalanul értesíti az adatvédelmi tisztviselőt.

A biztonsági esemény kivizsgálásának eredményéről a BEBD vezetője értesíti az érintett szervezeti egység vezetőjét, aki intézkedik a további esetleges fegyelmi, jogi eljárásról.

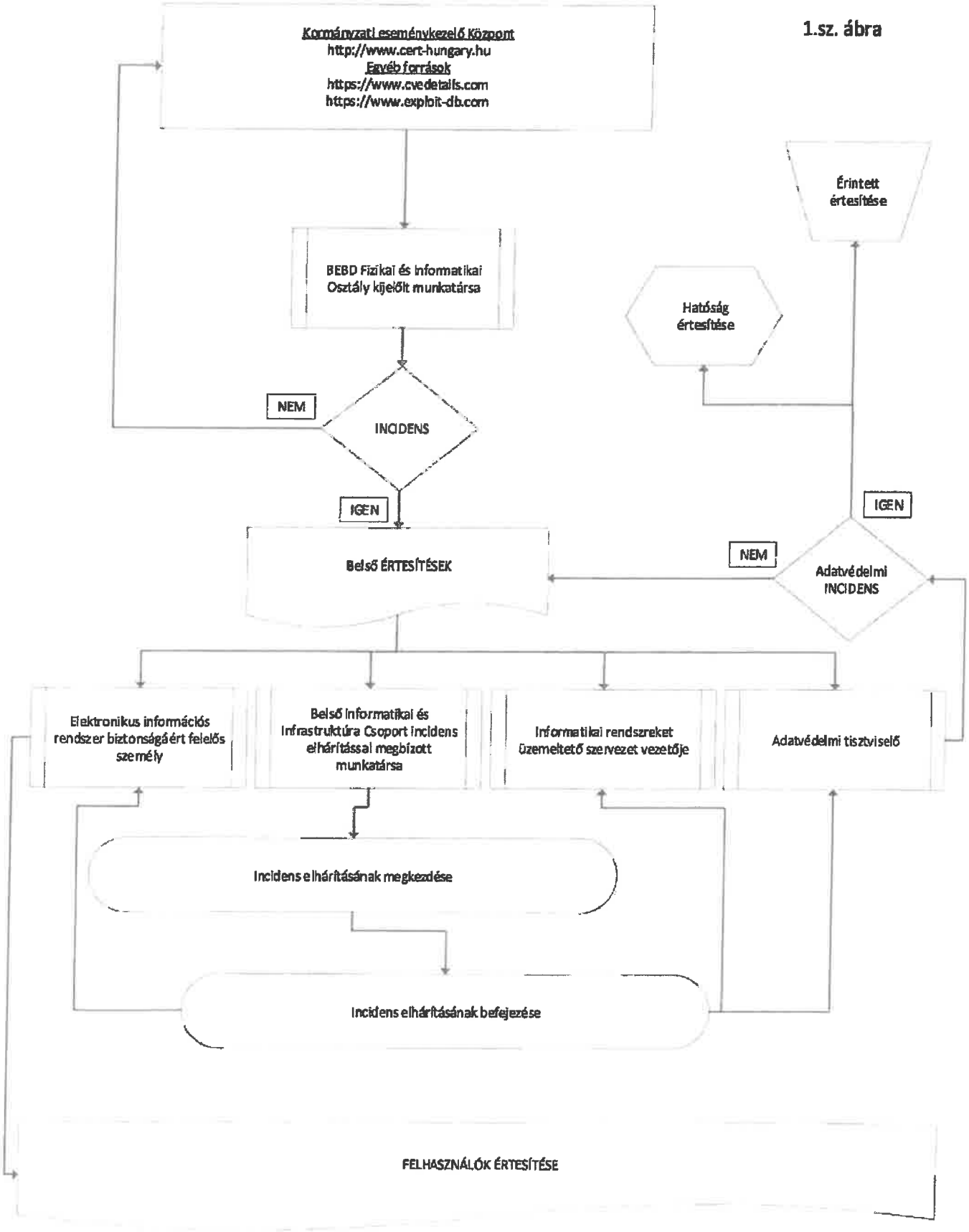
5. Bejelentési kötelezettség

Abban az esetben, ha felmerül a gyanú, hogy számítógépes adatvédelmi incidens áldozatává vált a Társaság számítástechnikai rendszere, vagy éppen ennek folyamata alatt van, akkor a jogszabályokban meghatározott esemény bejelentési kötelezettség mellett be kell jelenteni ezen incidens tényét a szakhatóságnak, a Nemzeti Adatvédelmi és Információszabadság Hatóságnak (a továbbiakban: NAIH).
Az adatvédelmi incidensről szóló bejelentést a NAIH mindenkori kapcsolati pontjára (http://naih.hu/uegyfelszolgalat,--kapcsolat.html) kell eljuttatni.

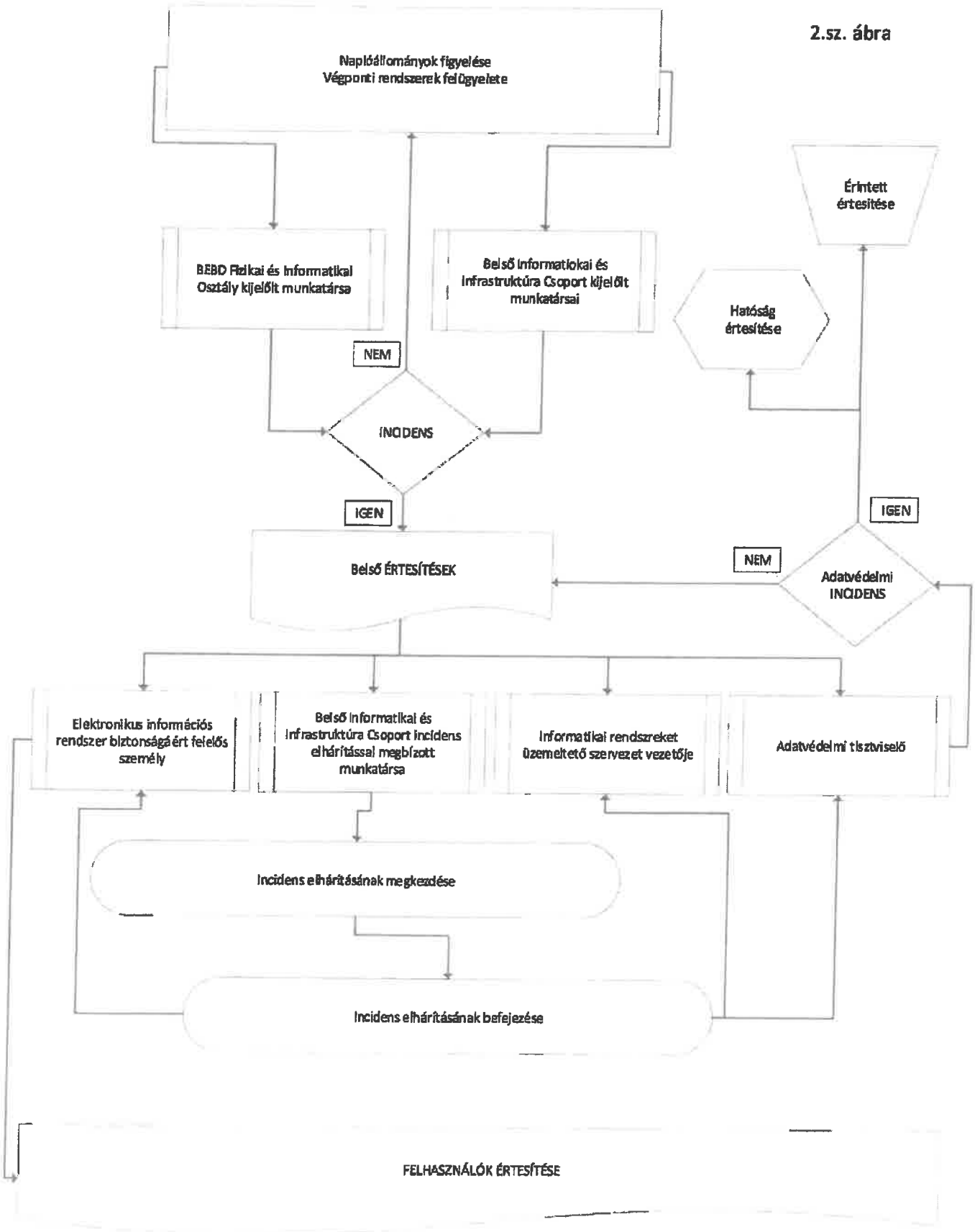
Amint a BEBD vezetőjének tudomására jut egy esetleges adatvédelmi incidens, azt indokolatlan késedelem nélkül, legkésőbb 72 órával azután, hogy az adatvédelmi incidens ténye kiderült, be kell jelenteni a felügyeleti hatóságnál (NAIH), amelyet a részére biztosított tájékoztatás alapján az adatvédelmi tisztviselő teljesít. Ha a bejelentés 72 órán belül nem tehető meg teljeskörűen, akkor a bejelentésben meg kell jelölni a késedelem okát, az előírt információk pedig – további indokolatlan késedelem nélkül – részletekben is bejelenthetők.

Nem kell bejelenteni az adatvédelmi incidenst, ha – az elszámoltathatóság elvével összhangban – bizonyítható, hogy az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve.

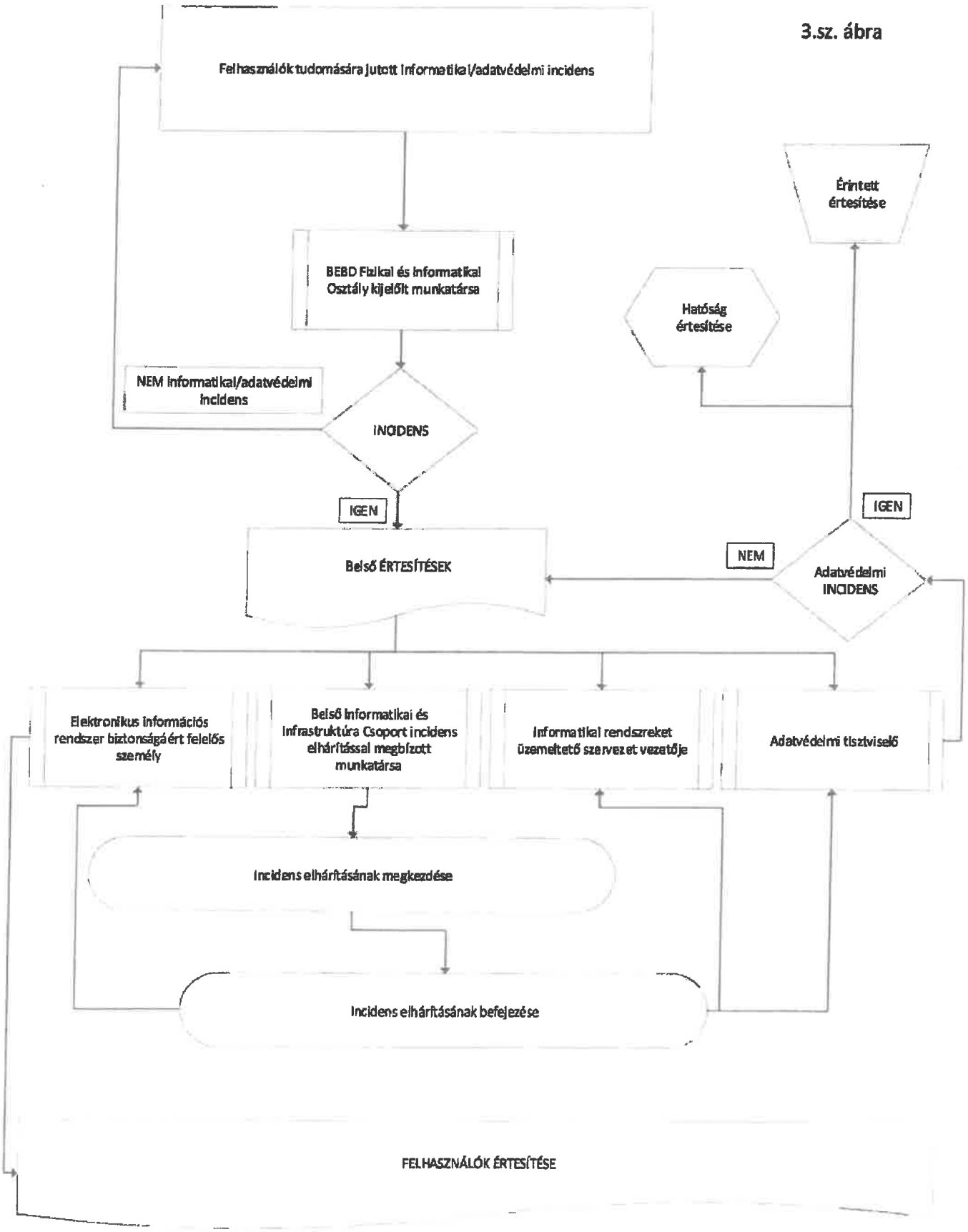
1.sz. ábra


Kormányzati Eseménykezelő Központ
http://www.cert-hungary.hu
Egyéb források
https://www.cvedetails.com
https://www.exploit-db.com
Érintett értesítése
BEBD Fizikai és Informatikai Osztály kijelölt munkatársa
Hatóság értesítése
NEM
INCIDENS
IGEN
IGEN
Belső ÉRTESÍTÉSEK
NEM
Adatvédelmi INCIDENS
Elektronikus információs rendszer biztonságáért felelős személy
Belső Informatikai és Infrastruktúra Csoport incidens elhárítással megbízott munkatársa
Informatikai rendszereket üzemeltető szervezet vezetője
Adatvédelmi tisztviselő
Incidens elhárításának megkezdése
Incidens elhárításának befejezése
FELHASZNÁLÓK ÉRTESÍTÉSE

2.sz. ábra


Naplóállományok figyelése
Végponti rendszerek felügyelete
BEBD Fizikai és Informatikai Osztály kijelölt munkatársa
Belső informatikai és Infrastruktúra Csoport kijelölt munkatársai
NEM
INCIDENS
IGEN
Belső ÉRTESÍTÉSEK
Érintett értesítése
Hatóság értesítése
IGEN
NEM
Adatvédelmi INCIDENS
Elektronikus információs rendszer biztonságáért felelős személy
Belső informatikai és Infrastruktúra Csoport incidens elhárítással megbízott munkatársa
Informatikai rendszereket üzemeltető szervezet vezetője
Adatvédelmi tisztviselő
Incidens elhárításának megkezdése
Incidens elhárításának befejezése
FELHASZNÁLÓK ÉRTESÍTÉSE

3.sz. ábra


Felhasználók tudomására jutott informatikai/adatvédelmi incidens
Érintett értesítése
BEBD Fizikai és Informatikai Osztály kijelölt munkatársa
Hatóság értesítése
NEM informatikai/adatvédelmi incidens
INCIDENS
IGEN
IGEN
Belső ÉRTESÍTÉSEK
NEM
Adatvédelmi INCIDENS
Elektronikus információs rendszer biztonságáért felelős személy
Belső informatikai és infrastruktúra Csoport incidens elhárítással megbízott munkatársa
Informatikai rendszereket üzemeltető szervezet vezetője
Adatvédelmi tisztviselő
Incidens elhárításának megkezdése
Incidens elhárításának befejezése
FELHASZNÁLÓK ÉRTESÍTÉSE

Készült: 2 példányban
Egy példány: 5 lap
Ügyintéző (tel.): dr. Homonnai Ildikó (45-910)
Kapják: 1. sz. pld.: Levéltár
2. sz. pld.: HM EI Zrt. Irattár

HONVÉDELMI MINISZTÉRIUM
ELEKTRONIKAI, LOGISZTIKAI ÉS VAGYONKEZELŐ
ZÁRTKÖRŰEN MŰKÖDŐ RÉSZVÉNYTÁRSASÁG (HM EI Zrt.)

5. sz. melléklet a HM EI Zrt. 884/505 nyt. számú Adatvédelmi és Adatbiztonsági Szabályzatához

2. számú példány

Nyt. szám:

ADATVÉDELMI INCIDENS
nyilvántartásba vételére szolgáló adatlap

Az adatvédelmi incidens (a továbbiakban: Incidens) bejelentése a GDPR 33. cikkben foglaltak alapján történik, ennek teljesítéséhez az adatvédelmi incidens észleléséről az adatvédelmi tisztviselőt (adatvedelem@hmei.hu) haladéktalanul, de legkésőbb 24 órán belül ezen adatlap kitöltésével, majd részére elektronikus úton történő megküldésével tájékoztatni kell. Amennyiben a tájékoztatás 24 órán túli (késedelmes), az adatlap „Egyéb" pontjában részletes indoklás szükséges.

Bejelentő adatai

Szervezeti egység megnevezése:	
Bejelentő neve/munkaköre:	
Kijelölt kapcsolattartó személy neve:	

Incidens időpontjára vonatkozó adatok

Kezdete:	
Tudomásra jutásának (észlelés) időpontja:	
Észlelésének módja:	

Incidens jellege, kategóriája
(például :eszköz elvesztése vagy ellopása, informatikai rendszer feltörése, rosszindulatú számítógépes programok, zsarolóprogram, személyes adatok téves címzett részére történő elküldése):

.....
.....
.....

Incidens ismertetése, leírása

.....
.....
.....

Érintettek kategóriái
(például: munkavállalók, szerződéses partnerek, kiskorúak stb.):

.....
.....
.....

Érintettek hozzávetőleges száma

.....
.....
.....

Incidenssel érintett személyes adatok kategóriái
(személyes adatok, különleges adatok):

.....
.....
.....

Incidenssel érintett személyes adatok mennyisége, hozzávetőleges száma

.....
.....
.....

Incidensből eredő, valószínűsíthető következmények ismertetése

- *Bizalmas jelleg sérülése* (például: szélesebb körű hozzáférés, mint ami szükséges, vagy amihez az érintett hozzájárult; az adat összekapcsolhatóvá vált az érintett egyéb adatával; az adat más célokból, vagy tisztességtelen módon történő kezelése lehetséges; egyéb):

  .....
  .....
  .....

- *Integritás sérülése* (az adat módosíthatóvá vált annak ellenére, hogy archivált elavult adat volt; az adatot valószínűsíthetően módosították egyébként pontos adatokra, és azokat eltérő célokra használhatták; egyéb):

  .....
  .....
  .....

- *Rendelkezésre állás sérülése* (az érintettek számára történő kritikus szolgáltatásnyújtás képességének elvesztése vagy módosulása; az egyéb rendelkezésre állást érintő következmény leírása):

  .....
  .....
  .....

- *Az érintetteket ért* fizikai, anyagi vagy nem vagyoni *károk*, vagy egyéb jelentős következmények – ami az incidens valószínűsíthető hatásainak feleltethető meg az érintettekre vonatkozóan –, valamint azok *valószínűsíthető súlyossága*:

  .....
  .....
  .....

Incidens megítélése (megfelelő rész kiválasztása és indokolása szükséges)

Nem jár kockázattal, mert

.....

Mérsékelt kockázattal jár, mert

.....

Magas kockázattal jár, mert

.....

Megtett, illetve tervezett intézkedések

(ideértve az érintettek tájékoztatását – annak időpontját, formáját, tartalmát, a tájékoztatott érintettek számát, amennyiben a tájékoztatás nem történt meg, annak indokait – a GDPR 34. cikke alapján; az adatvédelmi incidens orvoslására tett intézkedések felsorolását; következmények enyhítésére tett intézkedéseket; egyéb):

.....
.....
.....
.....
.....
.....
.....
.....
.....

Egyéb (pl. késedelmes bejelentés indoka)

.....
.....
.....

Budapest, 20… év ……..hó……..nap

……
szervezeti egység vezetője
név, beosztás

Készült: 2 példányban
Egy példány: 3 lap
Ügyintéző (tel.): dr. Homonnai Ildikó (45-910)
Kapják: 1. sz. pld.: Levéltár
2. sz. pld.: HM EI Zrt. Irattár

HONVÉDELMI MINISZTÉRIUM
ELEKTRONIKAI, LOGISZTIKAI ÉS VAGYONKEZELŐ
ZÁRTKÖRŰEN MŰKÖDŐ RÉSZVÉNYTÁRSASÁG (HM EI Zrt.)

6. sz. melléklet a HM EI Zrt. 8875/05 nyt. számú Adatvédelmi és Adatbiztonsági Szabályzatához

2. számú példány

Nyt. szám:

ADATVÉDELMI INCIDENS
bejelentő lap
(Adatvédelmi tisztviselő tölti ki!)

Bejelentő/adatkezelő adatai

Cégnév:	Honvédelmi Minisztérium Elektronikai, Logisztikai és Vagyonkezelő Zártkörűen Működő Részvénytársaság (rövidített név: HM EI Zrt.)
Székhely:	1101 Budapest, Salgótarjáni út 20.
Telefon:	+36 1 431 2900
Elektronikus levélcím:	hmei@hmei.hu

Adatvédelmi tisztviselő neve és elérhetősége

Név:	
Telefon:	
Elektronikus levélcím:	

Incidens időpontjára vonatkozó adatok

Kezdete:	
Tudomásra jutásának (észlelés) időpontja:	
Észlelésének módja:	
Késedelmes bejelentés indoka(i):	

Incidens jellege

.....
.....
.....

Incidens ismertetése, leírása

.....
.....
.....
.....
.....
.....
.....

Érintettek kategóriái

.....
.....
.....

Érintettek hozzávetőleges száma

.....
.....
.....

Incidenssel érintett személyes adatok kategóriái

.....
.....
.....

Incidenssel érintett személyes adatok mennyisége, hozzávetőleges száma

.....
.....
.....

Incidensből eredő, valószínűsíthető következmények ismertetése

- *Bizalmas jelleg sérülése* (például: szélesebb körű hozzáférés, mint ami szükséges, vagy amihez az érintett hozzájárult; az adat összekapcsolhatóvá vált az érintett egyéb adatával; az adat más célokból, vagy tisztességtelen módon történő kezelése lehetséges; egyéb):

  .....
  .....
  .....

- *Integritás sérülése* (az adat módosíthatóvá vált annak ellenére, hogy archivált elavult adat volt; az adatot valószínűsíthetően módosították egyébként pontos adatokra, és azokat eltérő célokra használhatták; egyéb):

  .....
  .....
  .....

- *Rendelkezésre állás sérülése* (az érintettek számára történő kritikus szolgáltatásnyújtás képességének elvesztése vagy módosulása; az egyéb rendelkezésre állást érintő következmény leírása):

  .....
  .....
  .....

- *Az érintetteket ért* fizikai, anyagi vagy nem vagyoni *károk*, vagy egyéb jelentős következmények – ami az incidens valószínűsíthető hatásainak feleltethető meg az érintettekre vonatkozóan –, valamint azok *valószínűsíthető súlyossága*:

  .....
  .....
  .....

Érintettek tájékoztatása szükséges

☐ **Igen**

☐ **Nem**

Megtett, illetve tervezett intézkedések

.....
.....
.....
.....
.....
.....
.....
.....
.....

Egyéb

.....
.....
.....

Budapest, 20... év .....hó.....nap

.....
HM EI Zrt.

Készült: 2 példányban
Egy példány: 3 lap
Ügyintéző (tel.): dr. Homonnai Ildikó (45-910)
Kapják: 1. sz. pld.: Levéltár
2. sz. pld.: HM EI Zrt. Irattár

7. sz. melléklet a HM EI Zrt. 887/505 .....nyt. számú Adatvédelmi és Adatbiztonsági Szabályzatához

2. számú példány

AZ ADATVÉDELMI HATÁSVIZSGÁLATI JELENTÉS TARTALMA

1 Az adatkezelés folyamata

1.1 Az Adatkezelés jellemzői

- az adatkezelés célja;
- az üzleti folyamat leírása;
- az adatkezelés funkcionális követelményei, törvényi kötelezettségek;
- információbiztonsági célkitűzések;
- jogosultságok leírása;
- adatok továbbítása.

1.2 Az Adatkezelés szerkezete

- funkcionális (logikai) architektúra;
- fizikai architektúra;
- a személyes adatokat tartalmazó adatbázisok, táblázatok és mezők szerkezete és listája;
- adatáramlás diagrammja entitások és interfészek szerint;
- adatáramlás életciklusának diagramja;
- az érintettek tájékoztatásának, hozzájárulás beszerzésének diagrammja;
- kapcsolódási pontok, a továbbított adatok meghatározására szolgáló interfészek listája (a portok, protokollok, API-k és titkosítás részletei).

1.3 Üzemeltetés eljárásainak leírása

- az adatkezelő rendszer azonosításának és használatának koncepciója;
- a működési koncepció, beleértve, ha az adatkezelő rendszer egészének vagy részeinek működtetését a helyszínen, külső helyen, vagy felhőalapon stb.;
- az üzemeltetés támogatásának koncepciója, különös tekintettel az adatkezelő rendszer támogatását biztosító harmadik felek nevére, arra, hogy milyen mértékben férnek hozzá a személyes adatokhoz és azon helyekhez, ahonnan a személyes adatok hozzáférhetők;
- a naplózási koncepció és a naplózott információk megfelelő megőrzési tervei;
- a mentések rendje és helyreállítási tervek; a metaadatok védelme és kezelése; az adatmegőrzési és törlési tervek és az adathordozók ártalmatlanítása.

1.4 A kockázati kritériumok

- a hatás mértékének becslésére vonatkozó kritériumok;
- a valószínűség becslésének kritériumai;
- a kockázat mértékének megállapítása;
- a kockázat elfogadásának kritériumai.

1.5 Erőforrások biztosítása (szervezeti, anyagi humán)

- a hatásvizsgálati csoport összetétele és vezetése;
- a hatásvizsgálat végrehajtásának terve és a szükséges források.

1.6 Az érdekelt felekkel folytatott konzultáció

- az érdekeltek típusa, mely érdekcsoportokkal folytattak konzultációt és hogyan (például felmérésekkel, interjúkkal, fókuszcsoportokkal, műhelyekkel);
- a konzultációk eredményének, illetve következményének rögzítése (ha a konzultációnak van valamilyen következménye).

2 Adatvédelmi követelmények

- Az alkalmazandó jogszabályok, szabályozás és szerződések leírása.
- A releváns információbiztonsági ellenőrző megoldások leírása (például információbiztonsági szabványok).
- A kapcsolódó adatvédelmi követelmények azonosítása.
- A tervezett vagy meglévő intézkedések leírása, amelyek várhatóan teljesítik az adatvédelmi követelményeket (a korábbi projektektől elérhető releváns információk felhasználása).

3 Kockázatértékelés

3.1 Kockázati források (kockázatok azonosítása)

Az adatvédelmi kockázatok többek között, de nem kizárólag:

- a személyes adatokhoz való jogosulatlan hozzáférés (bizalmasság elvesztése);
- a személyes adatok (az integritás elvesztése) jogosulatlan módosítása;
- a személyes adatok elvesztése, lopása vagy jogosulatlan eltávolítása (rendelkezésre állás hiánya);
- a személyes adatok túlzott gyűjtése (működési ellenőrzés elvesztése);
- a személyes adatok engedély nélküli vagy nem megfelelő összekapcsolása;
- nem elégséges információ a személyes adatok kezelésének céljáról (az átláthatóság hiánya);
- az érintett jogainak korlátozása (pl. a hozzáférési jog elvesztése);
- jogosulatlan adatkezelés az érintett tudomása vagy beleegyezése nélkül (kivéve, jogszabályon alapuló adatkezelést);
- a személyes adatok harmadik felekkel való megosztása vagy újra hasznosítása az érintett beleegyezése nélkül;
- a személyes adatok túltárolása.

3.2 Fenyegetések és valószínűségeik

- A fenyegetések valószínűségének becslésére (lásd: ISO / IEC 27000: 2016, 2.83) a szervezetnek figyelembe kell vennie a kockázati források kapacitásait, a támogató eszközök sérülékenységeit és a meglévő vagy tervezett ellenőrzéseket. Ennek alapján a fenyegetés és bekövetkezésének valószínűsége lehet
- ***1) Elhanyagolható:*** A támogató eszközök tulajdonságainak kihasználásával történő fenyegetés nem tűnik lehetségesnek a kiválasztott kockázati források miatt (pl. egy borítékolvasó és hozzáférési kód által védett helyiségben tárolt papírdokumentumok eltulajdonítása).
- ***2) Korlátozott***: A támogató eszközök tulajdonságainak kihasználásával történő fenyegetés a kiválasztott kockázati források miatt nehézségekbe ütközik (például a borítékolvasóval védett helyiségben tárolt papírdokumentumok eltulajdonítása).
- ***3) Jelentős:*** A támogatott eszközök tulajdonságainak kihasználásával történő fenyegetés valóban lehetségesnek tűnik a kiválasztott kockázati források számára (pl.irodai tárolt papírdokumentumok eltulajdonítása, amelyek nem érhetők el a recepción történő bejelentkezés nélkül).
- ***4) Maximális:*** A támogató eszközök tulajdonságainak kihasználásával történő fenyegetés rendkívül könnyűnek tűnik a kiválasztott kockázati forrásokhoz (pl. az előtérben tárolt papírdokumentumok eltulajdonítása).

3.3 Következmények és hatásuk szintje

- ***1) Elhanyagolható:*** Az érintettekre nem lesznek hatással, vagy esetleg néhány kellemetlenséggel találkozhatnak, amelyek minden probléma nélkül leküzdhetők (az információk újbóli bevitelének ideje, bosszúságok, irritációk stb.).
- ***2) Korlátozott:*** Az érintettek jelentős nehézségeket tapasztalhatnak, amelyek néhány nehézség ellenére képesek lesznek leküzdeni (többletköltségek, üzleti szolgáltatásokhoz való hozzáférés megtagadása, félelem, megértés hiánya, stressz, kisebb fizikai betegségek stb.).
- ***3) Jelentősebb:*** Az érintettekre jelentős következményekkel járhatnak, amelyeket komoly nehézségekkel kell megoldaniuk (pénzhamisítás, bankok feketelistázása, vagyoni kár, foglalkoztatás elvesztése, felszólítás, állapotromlás stb.).
- ***4) Maximális:*** Az érintettek jelentős vagy akár visszafordíthatatlan következményekkel is szembesülhetnek, amelyeket nem lehet leküzdeni (pénzügyi nehézségek, mint például a kiszolgáltathatatlan adósság vagy munkaképtelenség, hosszú távú pszichés vagy fizikai betegségek, halál stb.).

3.4 Megfelelőségi elemzés

- az adatvédelmi követelmények résznél definiált elvárásoknak megfelelés, illetve azoktól való elmaradás és annak mértéke.

4 Kockázatkezelési terv

- mit fognak tenni;
- milyen forrásokra lesz szükség;
- ki lesz felelős;
- határidő;
- az eredmények értékelése.

5 Következtetések és döntések

- A maradvány adatvédelmi kockázatok elfogadása.
- Hatásvizsgálati ajánlások, a kezelési terv nem nyilvános részeinek meghatározása.

5.1 Nyilvános összefoglaló

- az adatkezelési folyamat előnyei;
- a kezelt, összegyűjtött személyes adatok kategóriái;
- az adatkezelés jogalapja;
- a megfelelés elemzésének összefoglalása;
- összefoglaló minden olyan intézkedésről, amely eleget tesz az adatvédelmi követelményeknek;
- az adatkezelő elérhetősége;
- az érintettek által elérhető adatvédelmi „segélyvonalak", illetve a felhasználó támogatási lehetőségeinek részletei.

Készült: 2 példányban
Egy példány: 5 lap
Ügyintéző (tel.): dr. Homonnai Ildikó (45-910)
Kapják: 1. sz. pld: Levéltár
2. sz. pld: HM EI Zrt. Irattár