Egyedi azonosító:	67.	Verziószám:	4.0
Kiadmányozó:	vezérigazgató		
Hatályos:	2021.		
Mellékletek száma:	6	Nyomtatványok száma:	-

Adatvédelmi és adatbiztonsági szabályzat

Tartalomjegyzék

1 Általános rendelkezések

1.1 A Szabályzat célja

1. Az Adatvédelmi és adatbiztonsági szabályzat (továbbiakban: Szabályzat) célja annak biztosítása, hogy a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. (továbbiakban: adatkezelő vagy Társaság) megfeleljen *a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről szóló*, az Európai Parlament és a Tanács 2016/679 Rendeletében (a továbbiakban: GDPR), valamint *az információs önrendelkezési jogról és az információszabadságról szóló* 2011. évi CXII. törvényben (továbbiakban: Infotv.) foglaltaknak.

2. A Szabályzat célja a Társaság által adatkezelői, illetve adatfeldolgozói minőségben kezelt és feldolgozott személyes adatok védelmi rendszerének kiépítése és működtetése.

3. A Társaság által kezelt és feldolgozott személyes adatokat védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, véletlen megsemmisülés és sérülés, valamint az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen. Az elektronikusan kezelt adatállományok védelme érdekében megfelelő technikai megoldással biztosítani kell, hogy a nyilvántartásokban kezelt adatok – kivéve, ha azt törvény lehetővé teszi – közvetlenül ne legyenek összekapcsolhatók és az érintetthez rendelhetők.

1.2 A Szabályzat hatálya

4. A Szabályzat személyi hatálya kiterjed a Társaság valamennyi szervezeti egységére és munkatársára.

5. A velük kötendő szerződésekben biztosítani kell a Szabályzat rendelkezéseinek érvényesülését a Társasággal, mint megrendelővel szerződéses jogviszonyban álló magánszemélyek, jogi személyek és egyéb szervezetek, valamint ezek alkalmazottai (továbbiakban: külső támogatók) vonatkozásában, továbbá biztosítani kell, hogy az érintett személyek a Szabályzatot (eseti kivonatát) a szükséges mértékben megismerjék.

6. A Társasággal, mint szolgáltatóval kötött szerződések esetében a Szabályzatban foglaltakat a szerződés előkészítésekor irányadónak kell tekinteni.

7. A Szabályzat tárgyi hatálya kiterjed a Társaság bármely szervezeti egységénél folytatott valamennyi – személyes adatot érintő – számítógépes és manuális adatkezelésre, adatfeldolgozásra.

1.3 Hivatkozások

8. A Szabályzatot az alábbi jogszabályokkal összhangban kell alkalmazni:
   a) Magyarország Alaptörvénye,
   b) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről szóló, az Európai Parlament és a Tanács 2016/679 Rendelete (GDPR),
   c) 2016. évi CL. törvény az általános közigazgatási rendtartásról (Ákr.),
   d) 2016. évi CXXX. törvény a polgári perrendtartásról (Pp.),
   e) 2015. évi CCXXII. törvény az elektronikus ügyintézés és bizalmi szolgáltatások általános szabályairól (E-ügyintézési tv.),
   f) 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (Ibtv.),
   g) 2013. évi V. törvény a Polgári Törvénykönyvről (Ptk.),
   h) 2012. évi I. törvény a Munka Törvénykönyvéről (Mt.),
   i) 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (Infotv.),
   j) 2010. évi CLVII. törvény a nemzeti adatvagyon körébe tartozó állami nyilvántartások fokozottabb védelméről (Adatvagyon tv.),
   k) 2007. évi CLII. törvény az egyes vagyonnyilatkozat-tételi kötelezettségekről (Vnyt.),
   l) 2005. évi CXXXIII. törvény a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól (Vvtv.),
   m) 2003. évi C. törvény az elektronikus hírközlésről (Eht.),
   n) 2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről,
   o) 2017. évi XC. törvény a büntetőeljárásról (Be.),
   p) 1995. évi LXVI. törvény a köziratokról, a közlevéltárakról, és a magánlevéltári anyagok védelméről (Ltv.),
   q) 1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról (Nbtv.),
   r) 466/2017. (XII.28.) Korm. rendelet az elektronikus ügyintézéssel összefüggő adatok biztonságát szolgáló Kormányzati Adattrezorról,
   s) 451/2016. (XII. 19.) Korm. rendelet az elektronikus ügyintézés részletszabályairól,
   t) 186/2015. (VII.13.) Korm. rendelet a központosított informatikai és elektronikus hírközlési szolgáltató információbiztonsággal kapcsolatos feladatköréről,
   u) 309/2011. (XII.23.) Korm. rendelet a központosított informatikai és elektronikus hírközlési szolgáltatásokról,
   v) 346/2010. (XII.28.) Korm. rendelet a kormányzati célú hálózatokról,
   w) 335/2005. (XII. 29.) Korm. rendelet a közfeladatot ellátó szervek iratkezelésének általános követelményeiről,
   x) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről szóló 910/2014/EU Rendelet.

9. A Szabályzatot az alábbi belső szabályozó eszközökkel összhangban kell alkalmazni:
   a) 22. Vagyonnyilatkozat-tételi szabályzat
   b) 38. Gépjármű-használati szabályzat,
   c) 48. Adatközpont és gépteremüzemeltetés biztonsági szabályzat
   d) 49. Iratkezelési szabályzat,
   e) 51. Közadat szabályzat,
   f) 54. Alkalmazásfejlesztési és -tesztelési szabályzat,
   g) 55. Munkaerőgazdálkodási szabályzat,
   h) 64. Informatikai biztonsági szabályzat és az abban hivatkozott szabályzatok,
   i) 69. Személy-, objektum- és vagyonvédelmi szabályzat,
   j) 124. Munkáltatói visszaélés-bejelentési rendszer működtetési szabályzat,
   k) 128. Compliance szabályzat,
   l) 133. Tesztrendszerek adatkezelési szabályzata.

1.4 Fogalommeghatározások

10. A Szabályzat alkalmazása során az alábbiakban részletezett fogalmak irányadók.

Fogalom	Definíció
adatfeldolgozó	GDPR 4. cikk 8. pont alapján: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel.
adathordozó	Olyan anyagi eszköz, közeg, amely alkalmas adatok megőrzésére, tárolására. Megjelenési formája szerint lehet: papíralapú, mágneses, optikai, magnetooptikai elven működő vagy elektronikus.
adatkezelés	GDPR 4. cikk 2. pont alapján: a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés, továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés.
adatkezelő	GDPR 4. cikk 7. pont alapján: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza; ha az adatkezelés céljait és eszközeit az uniós vagy a tagállami jog határozza meg, az adatkezelőt vagy az adatkezelő kijelölésére vonatkozó különös szempontokat az uniós vagy a tagállami jog is meghatározhatja.
adatvédelmi incidens	GDPR 4. cikk 12. pont alapján: a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi.
biometrikus adat	GDPR 4. cikk 14. pont alapján: 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.
biztonsági esemény	IBSZ alapján: Ibtv. 1. § 9. pont alapján: biztonsági esemény: nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az

	elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül.
biztonságtechnikai rendszerek	Távfelügyeleti átjelzéssel vagy anélkül üzemeltetett behatolásjelző, beléptető, kamera- és tűzjelző rendszer.
Elektronikus információs rendszer	Ibtv. 1. § (1) bekezdés 14b. pontja alapján: a) az elektronikus hírközlésről szóló törvény szerinti elektronikus hírközlő hálózat; b) minden olyan eszköz vagy egymással összekapcsolt vagy kapcsolatban álló eszközök csoportja, amelyek közül egy vagy több valamely program alapján digitális adatok automatizált kezelését végzi; vagy c) az a) és b) pontban szereplő elemek által működésük, használatuk, védelmük és karbantartásuk céljából tárolt, kezelt, visszakeresett vagy továbbított digitális adatok.
érintett	GDPR 4. cikk 1. pont alapján: azonosított vagy azonosítható természetes személy.
harmadik fél	GDPR 4. cikk 10. pont alapján: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely nem azonos az érintettel, az adatkezelővel, az adatfeldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére felhatalmazást kaptak.
hozzájárulás	GDPR 4. cikk 11. pont alapján: az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez.
információs önrendelkezési jog	Alaptörvény VI. cikk alapján: a személyes adatok védelmét garantáló állampolgári alapjog, tárgya a személyes adat.
a személyes adatok különleges kategóriái	GDPR 9. cikk (1) bekezdés alapján: 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.
személy- és munkaügyi nyilvántartás	A HRI által vezetett, a munkavállaló – munkaviszonnyal összefüggésben keletkezett és azzal kapcsolatban álló – adatait tartalmazó nyilvántartás.
személyes adat	GDPR 4. cikk 1. pont alapján: 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.

1.5 Rövidítések

11. A Szabályzatban az alábbi rövidítések fordulnak elő.

Rövidítés	Definíció
BI	Biztonsági igazgatóság
EIBI	Elektonikus információbiztonsági igazgatóság
GLÜO	Géptermi létesítmény üzemeltetési osztály
HRI	Humánerőforrás igazgatóság
JSZI	Jogi és szabályozási igazgatóság
KMI	Kommunikációs és marketingmenedzsment igazgatóság
PSI	Pénzügyi és számviteli igazgatóság
ÜT	Üzemi Tanács

2 Adatvédelmi alapelvek

12. A Társaság által végzett adatkezelések, adatfeldolgozások során a 2.1.-2.7. fejezetekben meghatározott adatvédelmi alapelveknek kell érvényesülniük.

2.1 Jogszerűség, tisztességes eljárás és átláthatóság

13. A személyes adatok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni. Az adatkezelés akkor jogszerű, ha megfelelő jogalappal bír. Akkor átlátható és tisztességes, ha az adatkezelő és az adatkezelés célja világosan meghatározott, az érintett az adatkezelésről és jogai gyakorlásának módjáról megfelelő tájékoztatást kapott. A tájékoztatásnak könnyen hozzáférhetőnek és közérthetőnek kell lennie.

2.2 A célhoz kötöttség elve

14. A személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történjen, és azokat ne kezeljék ezekkel a célokkal össze nem egyeztethető módon. Nem minősül az eredeti céllal össze nem egyeztethetőnek a statisztikai célból történő további adatkezelés. Az információs önrendelkezési jog gyakorlásának feltétele és egyben legfontosabb garanciája, hogy az adatkezelés csak pontosan meghatározott és jogszerű célból történhet.

2.3 Az adattakarékosság elve

15. A személyes adatoknak az adatkezelés céljai szempontjából megfelelőnek és relevánsnak kell lenniük és a szükségesre kell korlátozódniuk. Az adattakarékosság elvének teljesülése adatkezelésenként mérlegelendő, és új adatkezelés esetén már az adatkezelés folyamatának megtervezésekor figyelembe kell venni („Privacy by Design”).

2.4 A pontosság elve

16. A személyes adatoknak pontosnak és szükség esetén naprakésznek kell lenniük; minden ésszerű intézkedést meg kell tenni annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul töröljék vagy helyesbítsék. Az adatok pontossága elsősorban az adatok felvételéhez kötődik (pl. személyazonosító és kapcsolatfelvételi adatokat tartalmazó nyilvántartások).

2.5 A korlátozott tárolhatóság elve

17. A személyes adatok tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé (a személyes adatok ennél hosszabb ideig történő tárolására csak pl. statisztikai célból kerülhet sor). Amennyiben tehát az adatkezelési cél teljesült, az adatokat törölni vagy anonimizálni kell. Az adatkezelőnek rendszeres időközönként vizsgálnia kell, hogy a megőrzési idő letelt-e.

2.6 Integritás és bizalmas jelleg

18. A személyes adatok kezelését oly módon kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve.

2.7 Elszámoltathatóság

19. Az adatkezelő felelős az adatkezelési elveknek való megfelelésért, továbbá képesnek kell lennie e megfelelés igazolására.

3 Az érintettek jogai és érvényesítésük

3.1 Átlátható tájékoztatás, kommunikáció és az érintett jogainak gyakorlására vonatkozó intézkedések

20. A Társaság, mint adatkezelő az érintettet a Társaság/adatkezelő által folytatott adatkezelésről átláthatóan és közérthetően tájékoztatja. A tájékoztatásról időben az alábbiak szerint kell gondoskodni:

    a. előzetesen (a személyes adatok megszerzésének időpontjában), vagy

    b. ha az adatokat az adatkezelő nem az érintettől szerezte meg, az érintettel való első kapcsolatfelvétel alkalmával, vagy

    c. a megszerzéstől számított észszerű határidőn belül, de legkésőbb egy hónapon belül, vagy

    d. ha várhatóan más címzettel is közli az adatokat, legkésőbb a személyes adatok első alkalommal való közlésekor.

    A tájékoztatás megtörténhet úgy is, hogy az adatkezelés részleteiről szóló tájékoztatót az adatkezelő közzéteszi és erre az érintett figyelmét felhívja.

21. Az adatkezelő az általa folytatott adatkezelések tekintetében tájékoztatást ad az adatkezelő és képviselője kilétéről és elérhetőségéről, az adatvédelmi tisztviselő elérhetőségéről, az érintett adatkezelő által kezelt személyes adatok kategóriáiról (adott esetben a személyes adatok különleges kategóriájába tartozó adatok kategóriáiról), azok forrásáról, az adatkezelés céljáról, jogalapjáról, időtartamáról (vagy ha ez nem lehetséges, az időtartam meghatározásának szempontjairól), amennyiben adatfeldolgozó igénybevétele megvalósul, az adatfeldolgozó nevéről, címéről, az adatkezeléssel összefüggő tevékenységéről, az érintett személyes adatainak továbbítása esetén az adattovábbítás címzettjéről, automatizált döntéshozatal alkalmazása esetén annak tényéről, az ahhoz alkalmazott logikáról, illetve az adatkezelés jelentőségére és a várható következményekre vonatkozó érthető információkról, továbbá az érintett által gyakorolható jogokról, illetve a Nemzeti Adatvédelmi és Információszabadság Hatósághoz (NAIH) címzett panasz benyújtásának jogáról. Ha az adatkezelés jogalapja a GDPR 6. cikk (1) bekezdésének f) pontján

alapul, a tájékoztatásnak ki kell térnie az adatkezelő vagy harmadik fél jogos érdekeire is. A Társaság adatfeldolgozóként nem adhat tájékoztatást a fentiekről, mert az az adatkezelő felelőssége.

22. Az adatkezelő elősegíti az érintett jogainak a gyakorlását. Az adatkezelő köteles legfeljebb a kérelem beérkezésétől számított egy hónapon belül a tájékoztatást megadni a joggyakorlásra vonatkozó kérelem nyomán hozott intézkedésekről. Az érintett joggyakorlására irányuló kérelmek teljesítése csak akkor tagadható meg, ha az adatkezelő bizonyítja, hogy az érintettet nem áll módjában azonosítani. Amennyiben az adatkezelő nem tesz intézkedéseket az érintett kérelme nyomán, késedelem nélkül, de legkésőbb a kérelem beérkezésétől számított egy hónapon belül tájékoztatja az érintettet az intézkedés elmaradásának okairól, valamint arról, hogy az érintett panaszt nyújthat be a NAIH-nál és élhet bírósági jogorvoslati jogával.

23. Az adatkezelésről, valamint az érintetti kérelmek nyomán hozott intézkedésekről szóló tájékoztatást és intézkedést díjmentesen biztosítja az adatkezelő. Az ezekről szóló tájékoztatást tömör, átlátható, érthető és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva kell megadni. Ha az érintett kérelme egyértelműen megalapozatlan vagy – különösen ismétlődő jellege miatt – túlzó, az adatkezelő, figyelemmel a kért információ vagy tájékoztatás nyújtásával vagy a kért intézkedés meghozatalával járó adminisztratív költségekre
    a) ésszerű összegű díjat számíthat fel vagy
    b) megtagadhatja a kérelem alapján történő intézkedést.

24. A kérelem egyértelműen megalapozatlan vagy túlzó jellegének bizonyítása az adatkezelőt terheli.

3.2 Hozzáféréshez való jog

25. Az érintett jogosult arra, hogy az adatkezelőtől visszajelzést kapjon arról, hogy adatainak kezelése folyamatban van-e, és ha igen, jogosult arra, hogy az alábbi információkhoz hozzáférést kapjon:
    a) adatkezelés célja,
    b) érintett személyes adatok kategóriái,
    c) adatok címzettjei vagy címzettek kategóriái,
    d) adattárolás tervezett időtartama, vagy ha ez nem lehetséges, a meghatározásának szempontjai,
    e) érintetti jogok,
    f) jogorvoslat, ideértve a NAIH-nak címzett panasz benyújtásának jogát,
    g) adatok forrása, ha nem az érintettől gyűjtötték.
    h) automatizált döntéshozatallal összefüggő információk.

26. Az adatkezelő az adatkezelés tárgyát képező személyes adatok másolatát az érintett kérelmére rendelkezésére bocsátja. Amennyiben az érintett elektronikus úton nyújtotta be a kérelmet, az információkat elektronikus formátumban kell rendelkezésére bocsátani, kivéve, ha az érintett másként kéri.

3.3 A helyesbítéshez való jog

27. Az érintett jogosult arra, hogy kérésére az adatkezelő indokolatlan késedelem nélkül helyesbítse a rá vonatkozó pontatlan személyes adatokat. Figyelembe véve az adatkezelés célját, az érintett jogosult arra, hogy kérje a hiányos személyes adatok – egyebek mellett kiegészítő nyilatkozat útján történő – kiegészítését.

3.4 A törléshez való jog

28. Az adatkezelő az érintett kérésére köteles törölni az érintettre vonatkozó személyes adatokat, ha az alábbi indokok valamelyike fennáll:

a) az adatkezelés már nem szükséges,
b) az érintett visszavonja a hozzájárulását és az adatkezelésnek nincs más jogalapja,
c) az érintett tiltakozik az adatkezelés ellen és nincs elsőbbséget élvező jogszerű ok az adatkezelésre,
d) a személyes adatokat jogellenesen kezelték,
e) a személyes adatokat a jogi kötelezettség teljesítéséhez kell törölni,
f) a személyes adatok gyűjtésére a közvetlenül gyermekeknek kínált, információs társadalommal összefüggő szolgáltatások kínálásával kapcsolatosan került sor.

29. A törlés nem alkalmazható, ha az adatkezelés jogi kötelezettség teljesítése érdekében történik (pl. a megőrzési időt jogszabály írja elő), vagy jogi igények előterjesztéséhez, érvényesítéséhez, védelméhez szükséges.

3.5 Adatkezelés korlátozásához való jog

30. Az érintett jogosult arra, hogy kérésére az adatkezelő korlátozza az adatkezelést, ha
a) az érintett vitatja a személyes adatok pontosságát (az ellenőrzéshez szükséges ideig),
b) az adatkezelés jogellenes és az érintett ellenzi az adatok törlését,
c) az adatkezelőnek már nincs szüksége a személyes adatokra, de az érintett igényli azokat védendő magánérdekből,
d) az érintett tiltakozott az adatkezelés ellen (amíg megállapításra nem kerül, hogy az adatkezelő jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben).

31. A korlátozást az automatizált nyilvántartási rendszerekben alapvetően technikai eszközökkel kell biztosítani (ideiglenes áthelyezés másik adatkezelő rendszerbe, megjelölés). Az adatokon a tárolás kivételével további adatkezelési műveletek nem végezhetők, az adatokat nem lehet megváltoztatni. Az adatkezelés korlátozásának feloldásáról az érintettet előzetesen tájékoztatni kell. A korlátozás alá eső személyes adatokat kezelni lehet, ha az érintett hozzájárul, méltányolható magánérdek védelme érdekében, más természetes vagy jogi személy jogainak védelme érdekében, illetve az Európai Unió vagy az állam fontos közérdekéből.

3.6 A személyes adatok helyesbítéséhez vagy törléséhez, illetve az adatkezelés korlátozásához kapcsolódó értesítési kötelezettség

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

3.7 Adathordozhatósághoz való jog

33. Az érintett jogosult arra, hogy a rá vonatkozó, általa az adatkezelő rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja, továbbá jogosult arra, hogy ezeket az adatokat egy másik adatkezelőnek továbbítsa anélkül, hogy ezt akadályozná az az adatkezelő, amelynek a személyes adatokat a rendelkezésére bocsátotta, ha
a) az adatkezelés hozzájáruláson vagy szerződésen alapul és
b) az adatkezelés automatizált módon történik.

3.8 Tiltakozáshoz való jog

34. Az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból bármikor tiltakozzon személyes adatainak kezelése ellen, az alábbi esetekben:

a) az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges,
b) az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges,
c) az adatkezelés tudományos és történelmi kutatási célból vagy statisztikai célból történik.

35. A tiltakozáshoz való jogra az érintett figyelmét legkésőbb az első kapcsolatfelvétel során fel kell hívni, és az erre vonatkozó tájékoztatást elkülönítve kell megjeleníteni.

3.9 Az érintetti jogok teljesítésének eljárásrendje

36. Az érintett a tájékoztatás, hozzáférés, helyesbítés, korlátozás vagy törlés, továbbá az adathordozás iránti kérelmét és tiltakozását a Társasághoz, az adatvédelmi tisztviselőhöz vagy a kérelemmel, tiltakozással érintett adatkezelést végző szervezeti egységhez nyújthatja be.

37. Az adatkezeléssel kapcsolatos tájékoztatást, a megtett intézkedést tartalmazó levelet az a szervezeti egység készíti elő, amely a tájékoztatással, intézkedéssel érintett adatkezelést végzi, abban az esetben is, ha a tájékoztatás, intézkedés iránti kérelem nem hozzá érkezett.

38. Az érintettnek való megküldés előtt a tájékoztatást, intézkedést tartalmazó levelet meg kell küldeni az adatvédelmi tisztviselőnek olyan időben, hogy a nyitva álló legfeljebb egy hónapból még legalább 5 munkanap rendelkezésre álljon. Az adatvédelmi tisztviselő megvizsgálja a levéltervezetben foglaltakat, szükség szerint egyeztet az érintett szervezeti egységgel, majd – amennyiben nem az adatvédelmi tisztviselő volt a kérelem címzettje – visszaküldi a tájékoztatást, intézkedést tartalmazó levelet, amelyet a megkeresett szervezeti egység küld meg az érintettnek.

39. Helyesbítés, korlátozás, törlés, illetve adathordozás és tiltakozás iránti kérelem esetén is egyeztetni szükséges az adatvédelmi tisztviselővel a kérelem teljesíthetőségéről, illetve annak módjáról. Ha az adatkezelő az érintett kérelmét nem teljesíti, illetve az intézkedést megtagadja, úgy a kérelem beérkezésétől számított egy hónapon belül közli az elutasítás okát és tájékoztatja az érintettet a jogorvoslati lehetőségekről.

40. A jogellenes adatkezeléssel okozott kárért az adatkezelő a vonatkozó jogszabályokban meghatározott szabályok szerint felel. Az adatkezelő az érintett adatainak jogellenes kezelésével vagy az adatbiztonság követelményeinek megszegésével okozott kárt köteles megtéríteni. Az érintettel szemben az adatkezelő felel az adatfeldolgozó által okozott kárért is. Az adatkezelő általános polgári jogi felelősségére a Ptk. vonatkozó rendelkezései az irányadók.

4 A Társaság adatvédelmi intézményrendszere

41. Az adatvédelmi előírások alkalmazása során az adatkezelő/adatfeldolgozó szerv vezetőjének a Társaság vezérigazgatója minősül.

42. A Társaság vezérigazgatója határozatlan időre az adatvédelmi jogot és gyakorlatot szakértői szinten ismerő adatvédelmi tisztviselőt nevez ki.

43. Az adatvédelmi tisztviselő
a) tájékoztat és szakmai tanácsot ad a Társaság, továbbá a munkatársak részére a GDPR, valamint az egyéb uniós vagy nemzeti adatvédelmi rendelkezések szerinti kötelezettségeikkel kapcsolatban;
b) ellenőrzi a GDPR-nak, valamint az egyéb uniós vagy nemzeti adatvédelmi rendelkezéseknek, továbbá a Társaság személyes adatok védelmével kapcsolatos belső szabályainak való megfelelést, ideértve a feladatkörök kijelölését, az adatkezelési műveletekben részt vevő személyzet tudatosság-növelését és képzését, valamint a kapcsolódó auditokat is;

c) kérésre szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomon követi a hatásvizsgálat elvégzését;
d) együttműködik a Hatósággal és
e) az adatkezeléssel összefüggő ügyekben – ideértve a GDPR 36. cikkében említett előzetes konzultációt is – kapcsolattartó pontként szolgál a Hatóság felé, valamint adott esetben bármely egyéb kérdésben konzultációt folytat vele.

44. Az adatvédelmi tisztviselő feladatait az adatkezelési műveletekhez fűződő kockázat megfelelő figyelembevételével, az adatkezelés jellegére, hatókörére, körülményére és céljára is tekintettel végzi.

45. A Társaság adatvédelmi tisztviselőjének munkáját a JSZI, a BI, az EIBI vezetői és munkatársai támogatják.

46. Az adatvédelmi tisztviselőhöz bármely érintett fordulhat.

47. A Társaság az adatvédelmi tisztviselő elektronikus és postai elérhetőségét közzéteszi a Társaság honlapján az alábbiak szerint: A Társaság adatvédelmi tisztviselője:
név: dr. Schubert István,
e-mail cím: adatvedelem@nisz.hu,
telefon: +3617954825.

5 A munkatársak, álláskeresők személyes adatainak kezelése

5.1 A Társaság toborzási, kiválasztási tevékenységével kapcsolatos adatkezelés

48. A Társaság lehetővé teszi az álláskeresők számára, hogy az internetes felületen regisztrálva jelentkezzenek a Társaságnál meghirdetett, betöltetlen álláshelyekre. A regisztrációhoz szükséges személyes adatok körét, az adatkezelés jogalapját, célját és időtartamát a toborzási célból létrehozott internetes felületen elhelyezett *Adatvédelmi tájékoztató toborzási és kiválasztási tevékenységet támogató elektronikus adatkezeléshez* tárgyú dokumentum tartalmazza.

49. A Társaság a különböző módokon beérkező pályázatokat egységesen a kiválasztási eljárás lezárultát követő 1 évig őrzi meg. A pályázatok toborzási időszakot követően történő megőrzése akkor lehetséges, ha ehhez az érintett álláskereső előzetesen hozzájárult.

5.2 A munkatársak személyes adatainak kezelése

50. A Társaság a munkatársainak személyes adatait a munkaviszony, munkavégzésre irányuló egyéb jogviszony létesítésével, fennállásával és megszüntetésével, valamint az abból származó jogok gyakorlásával és kötelezettségek teljesítésével összefüggésben kezelheti.

51. A személyügyi nyilvántartás vezetéséhez az érintett munkatárs saját magára vonatkozóan köteles adatot szolgáltatni. A nyilvántartás adatkörében beállt változásról az érintett köteles azonnali hatállyal írásban bejelentést tenni.

52. Törvényi felhatalmazás hiányában az adatkezelés alapjául kizárólag a munkaviszonyt, munkavégzésre irányuló egyéb jogviszonyt létrehozó szerződés teljesítése vagy a Társaság jogos érdeke, illetve a munkatárs számára egyértelműen kedvező, csak előnnyel járó esetekben a munkatárs, illetve új belépő munkatárs előzetes, megfelelő tájékoztatáson alapuló, önkéntes és határozott hozzájárulása szolgálhat, amelyben félreérthetetlen hozzájárulását adja a rá vonatkozó személyes adatok meghatározott célból és körben történő kezeléséhez.

53. A munkatárstól csak olyan nyilatkozat megtétele vagy adat közlése kérhető, amely a személyhez fűződő jogát nem sérti és a munkaviszony létesítése, teljesítése vagy megszüntetése szempontjából szükséges.

54. A munkatársat dokumentáltan tájékoztatni kell arról, hogy
    a) milyen adatait, milyen célból és jogalappal, mennyi ideig kívánja a Társaság kezelni,
    b) a Társaság mely szervezeti egysége és hol végzi az adatkezelést, illetve az adatfeldolgozást,
    c) az adatok továbbítására milyen célból és mely szervek részére kerülhet sor,
    d) az adatkezeléssel kapcsolatban milyen jogokkal rendelkezik (hozzáférés, helyesbítés, korlátozás, törlés kezdeményezése, adathordozás, tiltakozás),
    e) milyen jogorvoslati lehetőséggel rendelkezik.

55. A Társaság a munkatársra vonatkozó tényt, adatot, véleményt harmadik személlyel csak törvényben meghatározott esetben vagy az 53. pontban felsorolt jogalapok valamelyikének fennállása esetén közölhet. Törvényben meghatározott esetnek minősül a munkavállalói adatok közlése az adóhatóság és a társadalombiztosítási, munkaerő-piaci szervek felé is.

56. A Társaság a munkatársat a munkaviszonnyal összefüggő magatartása körében ellenőrizheti. A Társaság ellenőrzése és az annak során alkalmazott eszközök, módszerek nem járhatnak az emberi méltóság megsértésével. A munkatárs magánélete – különös tekintettel a személyes adatok különleges kategóriáiba tartozó adatokra – nem ellenőrizhető, kivéve a külön jogszabály által szabályozott, nemzetbiztonsági ellenőrzés, illetve a hatósági erkölcsi bizonyítvány bekérése esetén.

57. A Társaság előzetesen tájékoztatja a munkatársat azokról az eljárásokról, valamint technikai eszközöknek az alkalmazásáról, amelyek a munkatárs ellenőrzésére szolgálnak.

58. Új belépő munkatársat a fentiekről a HRI tájékoztatja a beléptetési folyamat során a Szabályzat, valamint a *69. Személy-, objektum- és vagyonvédelmi szabályzat* elektronikus példányához való hozzáféréssel, melynek megtörténtét a munkatárs az elektronikus felületen igazolja a *55. Munkaerőgazdálkodási szabályzat* szerint.

59. A Társaság köteles biztosítani, hogy a munkatárs a róla kezelt adatokat megismerhesse, a kezelt adatokat tartalmazó iratokról – titoktartási nyilatkozat megtételével – másolatot vagy kivonatot kaphasson.

60. A munkatárs
    a) kérheti adatai helyesbítését, illetve kijavítását,
    b) kérheti adatainak törlését a 3.4. alfejezetben foglaltak szerint,
    c) jogosult megismerni, hogy a személy- és munkaügyi nyilvántartásban kezelt adatait kinek, milyen célból és milyen adatkört érintően továbbították.

61. A Társaság korlátozza az adatkezelést, ha a munkatárs ezt kéri és a 30. pontban felsorolt esetek valamelyike fennáll. Korlátozás esetén az érintett adatokon a tárolás kivételével további adatkezelési műveletek nem végezhetők, az adatokat nem lehet megváltoztatni. Az adatkezelés korlátozásának feloldásáról az érintettet előzetesen tájékoztatni kell. A korlátozás alá eső személyes adatokat kezelni lehet, ha az érintett hozzájárul, méltányolható magánérdek védelme érdekében, más természetes vagy jogi személy jogainak védelme érdekében, vagy az Európai Unió, illetve az állam fontos közérdekéből.

62. A munkatárs hatósági erkölcsi bizonyítványával köteles igazolni, hogy nem szerepel Magyarország bűnügyi nyilvántartásában. Az adatkezelés jogalapja a Társaság által biztosított informatikai (távközlési, e-közigazgatási) szolgáltatások biztonsága érdekében megkövetelt magas szintű védelemhez fűződő jogos érdek, továbbá a szolgáltatások érdekében működtetett rendszerek, használt eszközök és műszaki-informatikai megoldások által képviselt jelentős vagyoni érdek. A hatósági erkölcsi bizonyítvány a munkaviszony létesítése szempontjából szükséges,

adatbiztonságot érintő tájékoztatást nyújt. Az adatkezelés jogszerűen folytatható, az adatkezelői érdekekkel szemben nem élveznek elsőbbséget az érintettek olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé. E megállapítást a *67-M1 Érdekmérlegelési teszt* támasztja alá.

63. Az Mt.-ben előírt munkaidő-nyilvántartás naprakészségének megteremtése érdekében a Társaságnál a beléptető rendszer rögzíti a munkaidő adatokat. Az adatkezelés jogalapja a Társaságnak, mint közpénzből gazdálkodó, állami tulajdonban lévő gazdasági társaságnak azon jogos érdeke, hogy az Mt.-ben előírt kötelezettségét a lehető leghatékonyabban és költségtakarékos módon, az irodaházakban rendelkezésre álló beléptető rendszerek által teljesítse. A beléptető rendszer keretén belül – bizonyos telephelyek esetén - biometrikus azonosítás is megvalósul, mely adatkezelés jogalapja a Társaság azon jogos érdeke, hogy kockázatokkal arányos módon érvényesítse a telephelyén meglévő értékek, üzleti titkok, személyes adatok védelmét. Az adatkezelés jogszerűen folytatható, az adatkezelői érdekekkel szemben nem élveznek elsőbbséget az érintettek olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé. E megállapítást a *67-M2 Érdekmérlegelési teszt*, valamint a *67-M6 biometrikus adatok kezelése tárgyában lefolytatott Érdekmérlegelési teszt* támasztja alá.

64. A személy- és munkaügyi nyilvántartás jogszerűségéért, a személyes adatok védelméért a HRI vezetője felelős.

65. A munkatárs személyi iratai körébe az alábbiak tartoznak:
   a) személyi anyag: az Mt. szerint kért vagy a munkavégzésre irányuló jogviszonyhoz szükséges és keletkezett iratok, a személyi adatlap, önéletrajz, a munkatárs felvételére vonatkozó javaslat, a munkaszerződés és annak módosítása, munkaviszonyt megszüntető irat, írásbeli figyelmeztetésre, kártérítési felelősség megállapítására vonatkozó irat,
   b) a munkatárs munkaviszonyával összefüggő egyéb irat,
   c) a munkatárs kérelmére kiállított vagy önként átadott adatokat tartalmazó irat.

66. A személyi iratokba jogosult betekinteni:
   a) a munkatárs a saját adataiba,
   b) a munkatárs felettese,
   c) a munkatárs kötelezettségszegése miatt indult eljárás során az azt lefolytató testület vagy személy,
   d) munkaügyi per kapcsán a bíróság,
   e) feladatkörükben eljárva a BI vezetője vagy az általa kijelölt személy az Nbtv. 1. §-ában meghatározott szervek megkereséseivel kapcsolatban,
   f) a munkaviszonnyal összefüggésben indult büntetőeljárásban a nyomozó hatóság, az ügyész és a bíróság,
   g) a személyes adatok kezelésével összefüggésben végzett vizsgálata során a NAIH,
   h) a személyügyi, munkaügyi és bérszámfejtői, valamint a képzési, toborzási, kiválasztási feladatokat ellátó szervezeti egység vagy személy.

67. A munkatársak személyi iratainak kezelése során az iratkezelő vagy folyamattámogató rendszerben a személyi iratnak csak a – néven kívül egyéb személyes adatot nem tartalmazó – fedőlapja továbbítható, a felelős személyek megjelölésekor a személyes adatok védelme érdekében különös figyelemmel kell lenni arra, hogy az adott személyes adatot csak az arra jogosult ismerhesse meg,

68. A munkavégzéssel összefüggésben a HRI-n kívül más szervezeti egységek is jogosultak egyes személyes adatok kezelésére. Ilyen adatkezelés szükségessége merül fel különösen a projektek elszámolásával, illetve egyes engedélyezésekkel kapcsolatosan. A kezelt személyes adatokat ezen szervezeti egységek közvetlenül az érintettől szerzik be, tájékoztatást adva az adatkezelés jogalapjáról, céljáról, időtartamáról. Az adatkezelést végző szervezeti egységek kötelesek ezen

tevékenységüket a Szabályzatban és a vonatkozó jogszabályokban foglaltaknak megfelelően végezni.

69. A BI vagy az általa kijelölt személy az Nbtv. 1. §-ában meghatározott nemzetbiztonsági szolgálatok a törvényben meghatározott feladataik ellátása során, azzal összefüggésben érkezett megkereséseivel kapcsolatban, valamint a nemzetbiztonsági ellenőrzésre kötelezett munkatársak esetében az érintett alábbi személyes adatait jogosult kezelni a vonatkozó törvényi előírások mellett:
a) születési idő és hely,
b) anyja neve,
c) lakcím.

70. Új belépő, nemzetbiztonsági ellenőrzés alá eső munkakörben foglalkoztatandó munkatársak esetében a fenti adatokat – a munkatárs tájékoztatása mellett – a HRI adja át a BI számára.

71. A KMI az új belépő munkatársról igazolványképnek megfelelő fényképet készít, amely – a munkatárs hozzájárulása esetén – jelenleg az intranet felületen található telefonkönyvben, az elektronikus levelezési rendszerben, valamint a NEXON4 HR rendszerben jelenik meg. A KMI továbbítja a fényképet a BI részére, a belépőkártya elkészítésének és a biztonságtechnikai beléptető rendszer működtetésének céljából. A BI általi adatkezelés jogalapja a Társaság jogos érdeke. E megállapítást a *67-M3 Érdekmérlegelési teszt* támasztja alá.

72. A HRI a munkatárssal kötött munkaszerződésben foglaltak alapján a szerződés teljesítéséhez szükséges adatkezelés, mint jogalap alapján kezeli a munkatárs egyéb jogviszonyával kapcsolatos, az *55-NY5 Bejelentés egyéb jogviszony fennállásáról vagy létesítéséről* nyomtatvány szerinti adatokat. Az adatkezelés célja az összeférhetetlenség vizsgálata. Az összeférhetetlenség vizsgálatában a HRI és a munkatárs által betöltendő vagy betöltött munkakör tekintetében az összeférhetetlenség vizsgálatához szükséges speciális szakértelemmel rendelkező vezető vesz részt.

73. A mobiltelefon számlák kiállítása érdekében az PSI az alábbi személyes adatokat jogosult kezelni:
a) munkatárs neve,
b) lakcíme.

74. Az EIBI az alábbi esetekben jogosult a munkatársak személyes adatainak kezelésére:
a) a nemzetbiztonsági szolgálatok megkereséseivel kapcsolatban,
b) a kormányzati célú hálózatokról szóló 346/2010. (XII.28.) Korm. rendelet 6. § (2) bekezdésében, a Be. 261-265. §-ában és a Pp. 322. §-ában meghatározott adatszolgáltatások teljesítése kapcsán,
c) a más szakterületek feladatkörébe utalt, nyilvántartásokat érintő információbiztonsági adatszolgáltatási, adatcserével összefüggő tevékenység során,
d) incidenskezelési és naplóelemzési tevékenység során.

75. A JSZI a Társaság arra kötelezett munkatársai által tett vagyonnyilatkozatokkal összefüggő személyes adatokat kezeli a *22. Vagyonnyilatkozat-tételi szabályzatban* foglalt előírások szerint.

76. A Társaság által kötött vagy kötendő azon szerződések esetében, amelyekben az érintett az egyik fél, vagy az adatkezelés a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges, a szerződés teljesítéséhez szükséges adatkezelés mint jogalap alapján a Társasággal szerződő fél a szükséges mértékben és ideig, legfeljebb azonban a szerződésből származó jogok érvényesíthetőségének elévüléséig jogosult a Társaság nevében és megbízásából eljáró munkatársak szerződésben feltüntetett alábbi személyes adatait kezelni:
a) munkatárs neve,
b) munkahelyi e-mail címe,
c) munkahelyi telefonszáma.

77. Amennyiben a munkatárs a Társaság valamely géptermébe kíván belépni, az engedélyezési eljárásban a GLÜO és a BI az alábbi személyes adatait jogosult kezelni, és adott esetben továbbítani a *48. Adatközpont és gépteremüzemeltetés biztonsági szabályzatban* foglalt előírások szerint annak az intézménynek, amelyben a gépterem található.

5.3 A munkahelyi számítógép, az e-mail és az internet, valamint a munkahelyi telefon használatának ellenőrzése

78. A fejezetben rögzített adatkezelés célja a munkaviszonyból származó kötelezettségek teljesítésének ellenőrzése, elszámolás, jogalapja az Mt. 11/A. §-a, valamint a GDPR (49) preambulum bekezdése szerinti jogos érdek.

79. A munkatársak a Társaság által munkavégzés céljából rendelkezésükre bocsátott infokommunikációs eszközöket (pl. számítógép, mobiltelefon) kizárólag munkavégzésre használhatják, melynek megvalósulását a Társaság ellenőrizheti. Az ellenőrzés során a Társaság a munkaviszonnyal összefüggő, a munkaviszony teljesítéséhez használt számítástechnikai eszközön tárolt adatokba tekinthet be addig, ameddig nem tudja eldönteni, hogy az adat magáncélú adat-e.

80. A Társaság által biztosított e-mail címhez tartozó postafiók esetében az *64. Informatikai biztonsági szabályzatban* kijelölt személy jogosult ellenőrizni, hogy annak használata csak munkavégzéssel összefüggően történt-e, azzal a feltétellel, hogy a magánjellegű levelek tartalma nem ismerhető meg.

81. Az a tény, hogy ki milyen online tartalmakat, internet oldalakat és milyen gyakorisággal tekint meg, személyes adatnak minősül. Tekintettel arra, hogy a Társaság a munkahelyi internethasználatot munkavégzés céljából teszi lehetővé, illetve a magánhasználatot az *64. Informatikai biztonsági szabályzat*korlátozza, a Társaság jogosult annak ellenőrzésére, hogy azt a munkatárs a munkaviszonyával összhangban használja-e. A Társaság nem vizsgálhatja az internethasználatból következő, abból kideríthető magánjellegű információkat. Az ellenőrzésnek annak megállapítására kell korlátozódnia, hogy az internethasználat megfelelő mértékben szolgálja-e a munkatárs munkaköri feladatainak ellátását, szakmai tájékozottságának növelését, illetve nem valósít-e meg a Társaság által tilosként deklarált tevékenységet. Az ellenőrzés során a munkatárs indoklását is figyelembe kell venni az olyan esetekben, amikor objektív szempontok alapján nem egyértelmű, hogy az internethasználat megfelel-e a Társaság elvárásainak, szabályainak.

82. A 80-81. pont szerinti ellenőrzésről értesíteni kell a munkatársat, lehetőséget biztosítva arra, hogy az ellenőrzésen az ÜT erre felkért tagja kíséretében részt vegyen és az ellenőrzés megállapításaival kapcsolatosan írásban észrevételt tegyen. Amennyiben az informatikai biztonság érdekében megteendő intézkedés sürgőssége indokolja, a munkatárs értesítése utólag is megtörténhet. A munkatárs ez esetben is megteheti észrevételeit.

83. Biztonsági esemény megelőzése, illetve észlelése esetén a Társaság annak vizsgálata céljából jogosult az elektronikus információs rendszerben tárolt adatokhoz való hozzáférésre, az adatok észlelésére. Az adatkezelés jogalapja a GDPR (49) preambulum bekezdése szerinti jogos érdek. A Társaság ilyen esetben akkor jogosult az adott személyes adat megismerésére, ha megalapozottan feltételezhető, hogy az adott adatot tartalmazó fájl, dokumentum stb. az okozója a biztonsági esemény közvetlen veszélyének vagy megtörténtének. A személyes adat megismeréséről az érintett munkatársat tájékoztatni kell, bemutatva a megismerés okait.

84. A mobiltelefon-hívások listázásával a Társaság nem ellenőrizheti a mobiltelefon-használatot. Mind a hívó, mind a hívott fél neve, telefonszáma, mind a köztük fennálló kapcsolat személyes adatnak minősül.

85. Az infokommunikációs eszközök használatára vonatkozó előírásokat az *64. Informatikai biztonsági szabályzat* tartalmazza.

5.4 GPS nyomkövetés

86. A Társaság által munkavégzéshez biztosított, GPS nyomkövető rendszerrel felszerelt kulcsos gépjárművek használati szabályait és a nyomkövető rendszerrel kapcsolatos tájékoztatási kötelezettség teljesítésével összefüggő szabályokat a *38. Gépjármű-használati szabályzat* tartalmazza. A GPS nyomkövető rendszer működésén keresztül megvalósuló adatkezelés jogalapja a Társaság által biztosított informatikai (távközlési, e-közigazgatási) szolgáltatások biztonsága érdekében megkövetelt magas szintű védelemhez fűződő jogos érdek. Az adatkezelés jogszerűen folytatható, az adatkezelői érdekekkel szemben nem élveznek elsőbbséget az érintettek olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé. E megállapítást a *67-M4 Érdekmérlegelési teszt* támasztja alá.

5.5 Biztonságtechnikai rendszerek

87. A Társaság által működtetett biztonságtechnikai rendszerek alkalmazásának szabályait a *69. Személy-, objektum- és vagyonvédelmi szabályzat* tartalmazza. A biztonságtechnikai rendszerek alkalmazásán keresztül megvalósuló adatkezelés jogalapja a Társaság által biztosított informatikai (távközlési, e-közigazgatási) szolgáltatások biztonsága érdekében megkövetelt magas szintű védelemhez fűződő jogos érdek. Az adatkezelés jogszerűen folytatható, az adatkezelői érdekekkel szemben nem élveznek elsőbbséget az érintettek olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé. E megállapítást a *67-M3 Érdekmérlegelési teszt* és a *67-M5 Érdekmérlegelési teszt* támasztja alá.

6 A Társaság munkatársai által alkalmazandó általános adatkezelési szabályok

88. A Társaság valamennyi munkatársa köteles a személyes adatok kezelése vonatkozásában az alábbi gyakorlati szabályokat megtartani:
   a) A munkavégzés során csak az ahhoz elengedhetetlenül szükséges személyes adatok kezelhetők, továbbíthatók, az adott feladatot ellátó szervezeti egység vezetőjének felelőssége a munkafolyamatok ennek megfelelő kialakítása (szükségtelen adathalmozás elkerülése).
   b) Az informatikai jogosultságok engedélyezésekor figyelemmel kell lenni arra, hogy személyes adathoz csak az férhessen hozzá, akinek a munkavégzéséhez az az adat, adatkör elengedhetetlenül szükséges (érvényesüljön a legkisebb jogosultság elve).
   c) Személyes adatot tartalmazó papír alapú dokumentum csak zárt borítékban továbbítható, illetve törekedni kell a személyes átadás megvalósulására.
   d) E-mailben személyes adatot tartalmazó dokumentum csak úgy továbbítható, hogy biztosított legyen, hogy azt csak az arra jogosult tekintheti meg, ennek érdekében – minimálisan – a személyes adatot csak a levél csatolmányaként lehet továbbítani, és a személyes adattartalomra utaló figyelmeztető mondatot kell elhelyezni a levél törzsszövegében a következők szerint: *„A csatolmány személyes adatokat tartalmaz, ennek megismerésére csak és kizárólag a levél címzettje jogosult.”*. A kiküldendő levelet a kiküldést megelőzően ellenőrizni kell, hogy a megfelelő e-mail címek szerepelnek-e a címzettek között (az illetéktelen megismerést elkerülendő), illetve azt is mérlegelni kell, hogy az e-mail címeket nem indokolt-e rejtett módon rögzíteni a „titkos másolat” funkcióval. A levélváltási előzményeket is vizsgálni szükséges, hogy tartalmaz-e védendő személyes adatot; indokolt esetben gondoskodni kell az előzmények törléséről vagy elhagyásáról. E követelmények teljesülésének ellenőrizhetősége

érdekében a küldő rögzíti a címzettek között az adatkezelést végző szervezeti egység vezetőjét is.

e) A szervezeti egységek által használt közös meghajtókon személyes adatot tartalmazó dokumentum csak akkor tárolható, ha biztosított, hogy azt csak az arra jogosultak tekintik meg, a közös meghajtók esetében a meghajtóért felelős szervezeti egységet meg kell jeleníteni, a közös meghajtón tárolt adatokért az adott szervezeti egység vezetője a felelős.

f) A *Public* meghajtóra személyes adatot tartalmazó dokumentum nem tölthető fel.

89. Az adatvédelmi tisztviselőnek lehetőség szerint gondoskodnia kell a munkatársak megfelelő adatvédelmi és adatbiztonsági képzéséről, továbbképzéséről.

7 A Társaság által az ellátotti kör és az állampolgárok részére nyújtandó szolgáltatások során megvalósuló adatkezelések szabályai

7.1 A Társaság, mint nyilvános elektronikus hírközlési szolgáltató adatvédelmi, adatbiztonsági és titoktartási kötelezettsége

90. Az Eht. és végrehajtási rendeletei alapján a Társaság az általa nyújtott hírközlési szolgáltatásra vonatkozó *Általános Szerződési Feltételek* részét képező *Adatvédelmi tájékoztató hírközlési szolgáltatásokhoz* című dokumentumban rögzíti az e tevékenységével kapcsolatos adatvédelmi és adatbiztonsági szabályokat.

7.2 A Társaság, mint kormányzati hitelesítés szolgáltató adatvédelmi, adatbiztonsági kötelezettsége

91. A vonatkozó jogszabályok (910/2014. EU Rendelet, az E-ügyintézési tv. és végrehajtási rendelete) alapján a Társaság által nyújtott elektronikus aláírással kapcsolatos bizalmi szolgáltatásra vonatkozóan a Társaság hiteles.gov.hu honlapján a Szabályozási dokumentációk alatt közzétett *Adatkezelési tájékoztató* kormányzati hitelesítés-szolgáltatásokhoz című dokumentum rögzíti az e tevékenységgel kapcsolatos adatvédelmi és adatbiztonsági szabályokat.

7.3 A Társaság, mint szabályozott elektronikus ügyintézési szolgáltatás, illetve kormányzati elektronikus ügyintézési szolgáltatás szolgáltató adatvédelmi, adatbiztonsági kötelezettsége

92. Az E-ügyintézési tv. és végrehajtási rendelete alapján a Társaság az általa nyújtott szabályozott elektronikus ügyintézési szolgáltatásokra (továbbiakban: SZEÜSZ), illetve kormányzati elektronikus ügyintézési szolgáltatásokra (továbbiakban: KEÜSZ) vonatkozó *Általános Szerződési Feltételek*ben és *Adatkezelési tájékoztató*kban rögzíti az e tevékenységével kapcsolatos adatvédelmi és adatbiztonsági szabályokat.

7.4 A Társaság, mint az országos telefonos ügyfélszolgálat működtetőjének adatvédelmi, adatbiztonsági kötelezettsége

93. A 451/2016. (XII.19.) Korm. rendelet alapján a Társaság által működtetett országos telefonos ügyfélszolgálati tevékenységre vonatkozóan a Társaság 1818.hu honlapján közzétett adatkezelési tájékoztató rögzíti az e tevékenyéggel kapcsolatos adatvédelmi és adatbiztonsági szabályokat.

7.5 A Társaság ellátotti köre és az állampolgárok részére nyújtandó szolgáltatásaival összefüggésben az EIBI által teljesítendő feladatok kapcsán megvalósuló adatkezelések

94. Az EIBI az alábbi esetekben jogosult az ellátotti kör és az állampolgárok személyes adatainak kezelésére:
   a) a nemzetbiztonsági szolgálatok megkereséseinek teljesítése,
   b) a 346/2010. (XII.28.) Korm. rendelet 6. § (2) bekezdésében, a Be. 261-265. §-ában és a Pp. 322. §-ában meghatározott adatszolgáltatások teljesítése,
   c) biztonsági incidensek kezelése, naplózási és logelemzési tevékenység.

8 A Társaság, mint adatfeldolgozó

95. A Társaság a nemzeti adatvagyon körébe tartozó egyes állami nyilvántartások, a Kormányzati Adattrezor, az egységes kormányzati ügyiratkezelő rendszer érkeztető rendszere, a Kormányzati Ügyfélvonal csatlakozó és együttműködő ügyfélszolgálatai által kezelt adatok, valamint a jogszabályokban meghatározott bizonyos SZEÜSZ-ök, KEÜSZ-ök és az ellátotti körbe tartozó intézmények számára üzemeltetett rendszerek vonatkozásában, mint jogszabály által kijelölt adatfeldolgozó jár el, amely tevékenysége során az alábbi előírások érvényesülnek:
   a) az adatfeldolgozó az adatkezelő által meghatározott adatkezelési műveleteket végzi, és e minőségében gyakorolja az adatkezelő által ráruházott jogosultságokat, teljesíti kötelezettségeit,
   b) adatfeldolgozó igénybevétele esetén az adatkezelés céljának és idejének, a kezelt adatok körének meghatározására, az adatkezelésre vonatkozó érdemi döntések meghozatalára továbbra is az adatkezelő jogosult és köteles, az adatkezelési műveletekre vonatkozó utasítások jogszerűségéért az adatkezelő felel,
   c) a Társaság adatfeldolgozóként az adatkezelést érintő érdemi döntést nem hozhat, a tudomására jutott személyes adatokat kizárólag az adatkezelő rendelkezései szerint dolgozhatja fel, saját céljára adatfeldolgozást nem végezhet, a személyes adatokat az adatkezelő rendelkezéseinek és a jogszabályi előírásoknak megfelelően köteles tárolni és megőrizni,
   d) az adatfeldolgozásra vonatkozó szerződést írásban kell megkötni, a GDPR 28. cikkének (3) bekezdésében felsorolt tartalmi elemekkel,
   e) a Társaság az adatfeldolgozó tevékenységi körén belül, illetve az adatkezelő által meghatározott keretek között felelős a személyes adatok kezeléséért,
   f) a Társaság mint adatfeldolgozó az adatkezelő rendelkezése szerint vehet igénybe további adatfeldolgozót,
   g) a Társaság mint adatfeldolgozó a feldolgozással érintett személyes adatokat harmadik személy vagy szerv részére az adatkezelő előzetes, dokumentált hozzájárulása nélkül nem továbbíthatja. Kivételt képez, amikor az adatfeldolgozót jogszabály kötelezi arra, hogy az adatokat továbbítsa az adatkérő hatóság, bíróság felé.

9 Adatbiztonság, adatvédelmi incidens

96. A Társaság gondoskodik az adatok biztonságáról. Ennek érdekében a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megteszi a szükséges technikai és szervezési intézkedéseket, amelyek az irányadó jogszabályok, adat- és titokvédelmi előírások érvényre

juttatásához szükségesek mind az elektronikus információs rendszerben tárolt, mind a hagyományos, papír alapú adathordozókon tárolt adatállományok tekintetében.

97. A Társaság az adatokat – az alkalmazott eljárásokkal és technikai eszközökkel – védi 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.

98. A Társaság az elektronikus információbiztonság és adatbiztonság szabályainak, valamint a nemzetbiztonsági érdekek érvényesítése céljából a munkatársak személyes adataiba és a Társaság által kezelt egyéb személyes adatokba betekinthet. Az adatkezelés jogalapja ezekben az esetekben a GDPR (49) preambulum bekezdése szerinti jogos érdek. E betekintési jogot a Társaság nevében a BI vezetője, az elektronikus információs rendszerben tárolt adatok esetén, a 83. pontban szabályozott biztonsági eseménnyel kapcsolatban az EIBI vezetője vagy az általuk kijelölt személyek gyakorolják.

99. Az elektronikus információbiztonság és adatbiztonság szabályainak érvényesüléséről, valamint e szabályok, továbbá a technikai és szervezési intézkedések hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárások kidolgozásáról az elektronikus információbiztonság tekintetében az EIBI, a fizikai biztonság tekintetében pedig a BI belső szabályozó eszközök kiadásával gondoskodik.

100. Az elektronikus információbiztonság feltételeinek érvényesítése érdekében az EIBI, a fizikai biztonság feltételeinek érvényesítése érdekében a BI – lehetőség szerint – gondoskodik az érintett munkatársak megfelelő felkészítéséről és továbbképzéséről.

101. A Társaság az adatok biztonságát szolgáló intézkedések meghatározásakor és alkalmazásakor tekintettel van a technika mindenkori fejlettségére. A Társaság a több lehetséges adatvédelmi és adatbiztonsági megoldás közül azt választja, amely a személyes adatok magasabb szintű védelmét biztosítja, kivéve, ha az aránytalan nehézséget jelentene.

102. A Társaság az elektronikus információs rendszerben tárolt adatok védelme körében gondoskodik különösen:
   a) az adminisztratív és a logikai védelmi intézkedésekről, beleértve a jogosulatlan hozzáférés elleni védelmet is,
   b) az adatállományok helyreállításának lehetőségét biztosító intézkedésekről, ezen belül a rendszeres biztonsági mentésről és a másolatok elkülönített, biztonságos kezeléséről,
   c) az adatállományok kártékony kódok elleni védelméről,
   d) az adatállományok, illetve az adatokat hordozó eszközök fizikai védelméről, ezen belül az objektumvédelmi intézkedések megtételéről, valamint a tűzkár, vízkár, villámcsapás, egyéb elemi kár elleni védelemről, illetve az ilyen események következtében bekövetkező károsodások helyreállíthatóságáról.

103. A Társaság a papír alapú nyilvántartások és adathordozók védelme körében gondoskodik különösen a 102. a) és d) alpont szerinti intézkedések értelemszerű alkalmazásáról.

104. A munkatársak és a Társaság érdekében eljáró személyek az általuk használt vagy birtokukban lévő, személyes adatokat is tartalmazó adathordozókat – függetlenül az adatok rögzítésének módjától – kötelesek biztonságosan őrizni és védeni a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés ellen.

105. Az elektronikus információbiztonságról részletesen az *64. Informatikai biztonsági szabályzat*, a fizikai biztonság részletszabályairól a *69. Személy-, objektum- és vagyonvédelmi szabályzat* rendelkezik.

106. Adatvédelmi incidens bekövetkezése esetén haladéktalanul értesíteni kell az adatvédelmi tisztviselőt, valamint – az incidens jellegétől függően – a BI és az EIBI vezetőjét, részletesen ismertetve az incidens valamennyi ismert részletét és az adatvédelmi incidens elhárítása érdekében esetlegesen már megtett intézkedéseket. Az adatvédelmi tisztviselő és az incidenst bejelentő, valamint az incidenssel érintett egyéb szervezeti egységek vezetői mérlegelik, hogy az incidens kockázattal jár-e a természetes személyek jogaira és szabadságaira nézve. Amennyiben igen, az adatvédelmi tisztviselő az incidenst bejelentő, valamint az incidenssel érintett egyéb szervezeti egységek vezetőinek közreműködésével indokolatlan késedelem nélkül, lehetőség szerint az adatvédelmi incidens tudomásra jutásától számított 72 órán belül az incidenst bejelenti a NAIH-nak.

107. Amennyiben a Társaság az incidenssel érintett adatkezelés tekintetében adatfeldolgozóként jár el, az incidensről való tudomásszerzését követően indokolatlan késedelem nélkül jelzi azt az adatkezelőnek.

108. A NAIH-nak való bejelentésben legalább
   a) ismertetni kell az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát,
   b) közölni kell az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit,
   c) ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket,
   d) ismertetni kell a Társaság által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

109. Amennyiben nem lehetséges az információkat egyidejűleg közölni, azok további indokolatlan késedelem nélkül később részletekben is közölhetők.

110. Az adatvédelmi tisztviselő elektronikusan nyilvántartja az adatvédelmi incidenseket, feltüntetve az adatvédelmi incidenshez kapcsolódó tényeket, annak hatásait és az orvoslására tett intézkedéseket.

10 Adattovábbítás

111. Adatok továbbítására minden esetben csak jogszerű jogalap fennállása esetén kerülhet sor.

112. A jogszabályon alapuló, eseti adatszolgáltatás esetén minden esetben meg kell győződni az adatkezelés jogalapjáról, kétség esetén az adatvédelmi tisztviselő közreműködését kell kérni. Személyes adatot továbbítani csak abban az esetben lehet, ha annak jogalapja egyértelmű, célja és az adattovábbítás címzettjének a személye pontosan meghatározott. Az adattovábbítást minden esetben dokumentálni kell oly módon, hogy annak menete és jogszerűsége bizonyítható legyen.

113. A papír alapú adathordozók kezelésére az *49. Iratkezelési szabályzat* előírásait értelemszerűen alkalmazni kell.

114. A jogszabály által előírt adattovábbítást a Társaság köteles teljesíteni.

115. Amennyiben az adattovábbításhoz az érintett hozzájárulására van szükség, a hozzájárulás megtörténtét dokumentálni kell. Az érintettek hozzájárulásához kötött adattovábbítás esetén az érintett írásbeli nyilatkozatát az adattovábbítás címzettje és célja ismeretében adja meg.

10.1 A személyes adatok harmadik országokba vagy nemzetközi szervezetek részére történő továbbítása

116. A személyes adatok harmadik országokba vagy nemzetközi szervezetek részére történő továbbítására kizárólag a GDPR V. fejezetében megállapított esetekben és garanciák mellett kerülhet sor.

11 Ellenőrzés

117. Az adatvédelemmel kapcsolatos jogszabályi előírások és belső szabályozó eszközök előírásainak megtartását az adatkezelést végző szervezeti egységek vezetői kötelesek folyamatosan ellenőrizni a Szabályzat alapján.

118. Az adatvédelmi tisztviselő jogosult az adatvédelemmel kapcsolatos általános és célellenőrzéseket végezni. Az adatbiztonsággal összefüggő ellenőrzések során az adatvédelmi tisztviselő és a BI, illetve az EIBI vezetője vagy az általuk kijelölt munkatársak kötelesek együttműködni.

119. Az ellenőrzésre feljogosított személy az ellenőrzés céljára figyelemmel az ellenőrzés érdekében minden olyan helyiségbe beléphet, ahol adatkezelés folyik, az adatkezelést végzőktől minden olyan kérdésben felvilágosítást kérhet, minden olyan adatkezelést megismerhet, vagy abba betekinthet, amely az ellenőrzött szerv adatkezelési tevékenységével összefügg.

120. Az adatvédelmi tisztviselő jogosult az irat- és adatkezeléssel kapcsolatos belső szabályozó eszközök, dokumentumok, jegyzőkönyvek és nyilvántartások áttekintésével ellenőrizni az adatkezelés rendjének megtartását. Jogszabálysértés esetén annak megszüntetésére szólítja fel az adatkezelő személyt vagy szervezeti egység vezetőjét, különösen súlyos jogszabálysértés esetén pedig a Társaság vezérigazgatójához fordul. Az adatvédelmi tisztviselő jogosult a személy- és munkaügyi nyilvántartások rendszerét ellenőrizni.

12 Az adatvédelmi rendelkezések megsértése esetén követendő eljárás

121. Amennyiben valamely személynek tudomására jut, hogy a vonatkozó jogszabályokban vagy a Szabályzatban foglalt adatvédelmi és adatbiztonsági rendelkezéseket megsértették, illetve ennek veszélye áll fenn, a Társaság vezérigazgatóját vagy az adatvédelmi tisztviselőt, az adatbiztonság megsértése esetén a BI vagy az EIBI vezetőjét haladéktalanul tájékoztatja.

122. A Társaság vezérigazgatója az adatvédelmi tisztviselő, illetve a BI vagy EIBI vezetőjének bevonásával haladéktalanul intézkedik:
   a) a személyes adatok védelmi rendszerének helyreállításáról,
   b) a rendelkezések megsértésére vezető okok, illetve az azt elősegítő körülmények feltárásáról,
   c) az érintett személy(ek) felelősségének tisztázásáról,
   d) a beszerzett adatok alapján a Társaság munkatársának vétkessége esetén az adott jogviszonyra irányadó szerződés vagy jogszabály alapján alkalmazandó szankció alkalmazásáról.

13 A NAIH vizsgálatában való közreműködés

123. A NAIH jogosult a Társaságnál ellenőrizni az adatvédelmi szabályok megtartását, illetve kivizsgálni a hozzá érkező panaszokban foglaltakat.

124. A NAIH-nál panasz benyújtásával bárki vizsgálatot kezdeményezhet arra hivatkozással, hogy a személyes adatok kezelésével kapcsolatban a Társaságnál jogsérelem következett be vagy annak közvetlen veszélye áll fenn.

125. A Társaság a NAIH-hal együttműködik, a NAIH kérésének a NAIH által megállapított határidőn belül eleget tesz, illetve amennyiben a NAIH által tett megállapításokkal, illetve a NAIH által meghatározott határozatokkal nem ért egyet, megteszi a GDPR-ban meghatározott lépéseket.

126. A 125. pontban meghatározott feladatok teljesítését az adatvédelmi tisztviselő koordinálja, a feladatok teljesítésében a vizsgálattal érintett szervezeti egység, valamint – érintettségtől függően – az EIBI és a BI vesz részt.

127. A NAIH elérhetőségei:
levelezési cím: 1363 Budapest, Pf.: 9.,
cím: 1055 Budapest, Falk Miksa utca 9-11.,
telefon: +36 (1) 391-1400,
fax: +36 (1) 391-1410,
internet: http:/www.naih.hu,
e-mail: ugyfelszolgalat@naih.hu.

14 Az adatkezelési tevékenységek nyilvántartása

128. A Társaság az általa végzett adatkezelési tevékenységekről nyilvántartást vezet. E nyilvántartás a következő információkat tartalmazza:
a) az adatkezelés céljai,
b) az érintettek kategóriáinak, valamint a személyes adatok kategóriáinak ismertetése,
c) adott esetben az olyan címzettek kategóriái, akikkel a személyes adatokat közlik vagy közölni fogják, ideértve a harmadik országbeli címzetteket vagy nemzetközi szervezeteket,
d) adott esetben a személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk, beleértve a harmadik ország vagy a nemzetközi szervezet azonosítását, valamint a GDPR 49. cikk (1) bekezdésének második albekezdés szerinti továbbítás esetében a megfelelő garanciák leírása,
e) ha lehetséges, a különböző adatkategóriák törlésére előirányzott határidők,
f) ha lehetséges, az adatbiztonság érdekében megtett technikai és szervezési intézkedések általános leírása.

129. A Társaság, mint adatfeldolgozó nyilvántartást vezet az adatkezelő nevében végzett adatkezelési tevékenységek minden kategóriájáról; a nyilvántartás a következő információkat tartalmazza:
a) minden olyan adatkezelő neve, amelynek vagy akinek a nevében az adatfeldolgozó eljár,
b) az egyes adatkezelők nevében végzett adatkezelési tevékenységek kategóriái,
c) adott esetben a személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítása, 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,
d) ha lehetséges, az adatbiztonság érdekében megtett technikai és szervezési intézkedések általános leírása.

130. A nyilvántartást az adatvédelmi tisztviselő elektronikus formában vezeti. A nyilvántartásban szereplő adatkezelésekre, adatfeldolgozásokra vonatkozó, a 128-129. pontban felsorolt információkat az adott adatkezelést, adatfeldolgozást végző szervezeti egység bocsájtja az adatvédelmi tisztviselő rendelkezésére. A nyilvántartásban szereplő adatkezelések, adatfeldolgozások, valamint az azokkal kapcsolatosan rögzített információk felülvizsgálatáról az adatvédelmi tisztviselő gondoskodik az érintett szervezeti egységek bevonásával.

131. Ha az adatkezelés időtartamát vagy szükségessége időszakos felülvizsgálatát törvény vagy az Európai Unió kötelező jogi aktusa nem határozza meg, az adott adatkezelést végző szervezeti egység az adatkezelés megkezdésétől számított legalább háromévente felülvizsgálja, hogy az általa,

illetve a Társaság megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által kezelt személyes adat kezelése az adatkezelés céljának megvalósulásához szükséges-e. E felülvizsgálat körülményeit és eredményét írásban kell dokumentálni. A felülvizsgálatba az adatvédelmi tisztviselőt be kell vonni, részére a felülvizsgálatot tartalmazó dokumentumot meg kell küldeni.

132. A Társaság – megkeresés alapján – a NAIH rendelkezésére bocsátja a nyilvántartást.

15 Érdekmérlegelési teszt, hatásvizsgálat

133. Amennyiben a Társaság által végzett adatkezelés jogalapja a GDPR 6. cikk (1) bekezdésének f) pontja szerinti jogos érdek, az adatkezelés megkezdése előtt érdekmérlegelési tesztet kell készíteni.

134. Az érdekmérlegelési tesztet az alábbi kérdések mentén kell elkészíteni:
   a) Adott célhoz feltétlenül kell-e személyes adatokat kezelni? (Ha enyhébb eszköz alkalmazható ugyanarra a célra, azt kell alkalmazni.)
   b) Az adatkezeléshez fűződő (munkáltatói) jogos érdek pontos meghatározása, pl. személy- és vagyonvédelem, adatbiztonság biztosítása, munkáltatói szabályok betartása, hatékonyabb szolgáltatások.
   c) Mi az adatkezelés célja, mely személyes adatok mennyi ideig tartó kezelését igényli?
   d) Annak meghatározása, hogy az érintetteknek/munkatársaknak mik lehetnek az érdekeik az adott adatkezelés vonatkozásában.
   e) Annak meghatározása, hogy miért korlátozza arányosan az adatkezelői/munkáltatói jogos érdek az érintetti/munkatársi jogokat, várakozásokat.

135. Az érdekmérlegelési tesztet az adatkezelést végző szervezeti egység az adatvédelmi tisztviselő közreműködésével készíti el, majd – amennyiben az adatkezelés a munkatársak személyhez fűződő jogait érinti – megküldi az ÜT számára. Az ÜT 10 napon belül megküldi észrevételeit az érintett szervezeti egység és az adatvédelmi tisztviselő számára.

136. Az elkészült érdekmérlegelési tesztet az adatkezelést végző szervezeti egység vezetője, az adatvédelmi tisztviselő és az ÜT elnöke – amennyiben az ÜT véleményezte az érdekmérlegelési tesztet –, valamint a Társaság vezérigazgatója aláírásával látja el (ideértve az elektronikus aláírást is), amely a Szabályzat mellékleteként kiadásra kerül (lásd *67-M1-M6* mellékletek).

137. Ha az adatkezelés valamely – különösen új technológiákat alkalmazó – típusa, figyelemmel annak jellegére, hatókörére, körülményére és céljaira, valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, a Társaság az adatkezelést megelőzően hatásvizsgálatot végez arra vonatkozóan, hogy a tervezett adatkezelési műveletek a személyes adatok védelmét hogyan érintik. Olyan, egymáshoz hasonló típusú adatkezelési műveletek, amelyek egymáshoz hasonló magas kockázatokat jelentenek, egyetlen hatásvizsgálat keretei között is értékelhetőek.

138. A hatásvizsgálatot az adott adatkezelést végző szervezeti egység köteles elvégezni az adatvédelmi tisztviselő közreműködésével, illetve – szükség szerint – az ÜT bevonásával.

139. A hatásvizsgálatot a NAIH által közzétett iránymutatás szerint kell elvégezni.

16 Kártérítés és sérelemdíj

140. Amennyiben az adatkezelő az érintett adatainak jogellenes kezelésével vagy az adatbiztonság követelményeinek megszegésével másnak kárt okoz, köteles azt megtéríteni. Amennyiben az adatkezelő az érintett adatainak jogellenes kezelésével vagy az adatbiztonság követelményeinek megszegésével az érintett személyiségi jogát megsérti, az érintett az adatkezelőtől sérelemdíjat követelhet.

141. Az érintettel szemben az adatkezelő felel az adatfeldolgozó által okozott kárért és az adatkezelő köteles megfizetni az érintettnek az adatfeldolgozó által okozott személyiségi jogsértés esetén járó sérelemdíjat is.

142. Az adatkezelő mentesül az okozott kárért való felelősség és sérelemdíj megfizetésének kötelezettsége alól, amennyiben bizonyítja, hogy a kárt vagy az érintett személyiségi jogának sérelmét az adatkezelés körén kívül eső elháríthatatlan ok idézte elő. Nem kell megtéríteni a kárt és nem követelhető sérelemdíj, amennyiben a kár a károsult vagy a személyiségi jog megsértésével okozott jogsérelem az érintett szándékos vagy súlyosan gondatlan magatartásából származott.

143. A kártérítés és sérelemdíj iránti követelések kivizsgálását az adatvédelmi tisztviselő koordinálja, bevonva az érintett szervezeti egységet, a JSZI-t, illetve – szükség szerint – az ÜT képviselőjét.

17 Mellékletek és nyomtatványok jegyzéke

Azonosító	Megnevezés
67-M1	Érdekmérlegelési teszt a GDPR 6. cikke (1) bekezdésének f) pontja szerinti jogos érdek fennállásának megállapítására a NISZ Zrt. által a munkaviszony létesítésekor kért hatósági erkölcsi bizonyítvánnyal összefüggésben
67-M2	Érdekmérlegelési teszt a GDPR 6. cikke (1) bekezdésének f) pontja szerinti jogos érdek fennállásának megállapítására a NISZ Zrt. által a beléptető rendszerből nyert munkaidő adatok alkalmazásával összefüggésben
67-M3	Érdekmérlegelési teszt a GDPR 6. cikke (1) bekezdésének f) pontja szerinti jogos érdek fennállásának megállapítására a NISZ Zrt. általi biztonságtechnikai beléptető rendszer alkalmazásával összefüggésben
67-M4	Érdekmérlegelési teszt a GDPR 6. cikke (1) bekezdésének f) pontja szerinti jogos érdek fennállásának megállapítására a NISZ Zrt. által a kulcsos gépjárművekbe szerelt GPS nyomkövető rendszer alkalmazásával összefüggésben
67-M5	Érdekmérlegelési teszt a GDPR 6. cikke (1) bekezdésének f) pontja szerinti jogos érdek fennállásának megállapítására a NISZ Zrt. általi biztonságtechnikai kamerás megfigyelő rendszer alkalmazásával összefüggésben
67-M6	Érdekmérlegelési teszt a GDPR 6. cikke (1) bekezdésének f) pontja szerinti jogos érdek fennállásának megállapítására a NISZ Zrt. általi, biometrikus adatok kezelésével járó beléptető rendszer alkalmazásával összefüggésben

18 Záró rendelkezések

144. A Szabályzat a kiadmányozást követően, a kihirdetést követő napon lép hatályba, ezzel egyidejűleg hatályát veszti a Szabályzat 2019. 08. 13-án kiadmányozott 3.0. verziója.

Budapest, 2021.

Bancsics Ferenc
vezérigazgató

19 Dokumentumtörténet

Verzió	Hatálybalépés dátuma	A módosítás rövid leírása
1	2013. 06. 25.	Első kiadás.
1.0	2016. 09. 30.	A szabályozás új szabályozási rendszerbe illesztése, valamint a jogszabályi változások miatt szükséges átdolgozása.
1.1	2017. 03. 30.	A 2017-ben történt szervezeti változás miatt szervezeti nevek és felelős személyek nevének aktualizálása, a *Belső adattovábbítási nyilvántartás* melléklet csatolása.
1.2	2017. 06. 09.	A KEKKH-tól átvett, személyes adatkezeléssel járó feladatok beépítése. Rögzítésre kerültek a munkatársak adatvédelemmel kapcsolatos alapvető kötelezettségei. Új előírásként lehetőség nyílik arra, hogy informatikai támadás veszélye vagy bekövetkezte esetén megteendő intézkedések során – a munkatárs egyidejű tájékoztatása mellett – a munkáltató megismerhesse a munkatársak számítógépén lévő személyes adatokat, amennyiben ez a veszély/kár elhárításához szükséges.
2.0	2018. 05. 25.	A GDPR 2018. május 25. napjától kötelezően alkalmazandó valamennyi tagállamban. A módosítás a GDPR-al való összhangot teremti meg.
3.0	2019. 08. 13.	Az Európai Unió adatvédelmi reformjának végrehajtása érdekében szükséges törvénymódosításokról szóló 2019. évi XXXIV. törvény hatálybalépése miatt szükségessé vált módosítások átvezetése, a *Belső adattovábbítási nyilvántartás* melléklet kivezetése, illetve egyéb aktualizálás. A munkaviszony létesítésekor kért hatósági erkölcsi bizonyítvánnyal összefüggésben készített érdekmérlegelési teszt módosítását a Munka Törvénykönyve módosításának 2019. április 26-án történt hatálybalépése tette szükségessé. A többi érdekmérlegelési teszt változatlanul marad hatályban.
4.0	2021.	A módosításokat belső környezeti változások (pl. kapcsolódó szabályzatok hatályba lépése), külső fejlemények (pl. NAIH adatainak változása), illetve az általánosságban rögzített adatvédelmi szabályok hatósági gyakorlat általi konkretizáltsága indokolták.

ZÁRADÉK

A dokumentum elektronikus aláírással hitelesített