NISZ Nemzeti Infokommunikációs Szolgáltató Zrt.
H-1081 Budapest, Csokonai utca 3.

Egyedi azonosító:	67.	Verziószám:	2.0
Kiadmányozó:	vezérigazgató		
Hatályos:	2018. 05. 25.		
Mellékletek száma:		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 rendelet), 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 és ezek alkalmazottai (továbbiakban: külső támogatók) vonatkozásában, továbbá biztosítani kell, hogy az érintett személyek a Szabályzatot (eseti kivonatát) a szükséges mértékben megismerjék; a szerződésnek erre vonatkozóan utalást kell tartalmaznia.

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

7. A Szabályzat rendelkezéseit irányadónak kell tekinteni a Társaság leányvállalatai – önálló szabályozási jogkörben készítendő – adatvédelmi szabályozásának kidolgozása során.

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

1.3 Hivatkozások

9. 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 rendelet),
   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) 1998. évi XIX. 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.

10. A Szabályzatot az alábbi belső szabályozó eszközökkel összhangban kell alkalmazni:
    a) 22. Vagyonnyilatkozat-tételi szabályzat (VNYSZ),
    b) 38. Gépjármű-használati szabályzat (GHSZ),
    c) 49. Iratkezelési szabályzat (ISZ),
    d) 51. Közadat szabályzat,
    e) 64. Informatikai biztonsági szabályzat (IBSZ) és az abban hivatkozott szabályzatok,
    f) 69. Személy-, objektum- és vagyonvédelmi szabályzat (SZOVSZ),
    g) 58. Munkaviszony létesítése és megszüntetése szabályzat,
    h) 2016/06. számú VIG utasítás a munkavállalók munkaviszony létesítésekor valamint megszűntekor esedékes nyilatkozat-tétele a titoktartási kötelezettség megtartásáról.

1.4 Fogalommeghatározások

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

Fogalom	Definíció
adatfeldolgozó:	GDPR rendelet 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 rendelet 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 rendelet 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 rendelet 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;
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:	SZOVSZ alapján: távfelügyeleti átjelzéssel vagy anélkül üzemeltetett behatolásjelző, beléptető, kamera- és tűzjelző rendszer;
érintett:	GDPR rendelet 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 rendelet 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 HPI által vezetett, a munkavállaló – munkaviszonnyal összefüggésben keletkezett és azzal kapcsolatban álló – adatait tartalmazó nyilvántartás;
személyes adat:	GDPR rendelet 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

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

Rövidítés	Definíció
BI	Biztonsági igazgatóság
EIBI	Elektonikus információbiztonsági igazgatóság
HPI	Humánpolitikai igazgatóság
JSZI	Jogi és szabályozási igazgatóság
PSAO	Pénzügyi és számviteli adminisztrációs osztály
RÜI	Rendszerüzemeltetési igazgatóság
SZTI	Szolgáltatásfejlesztési és termékmenedzsment igazgatóság
ÜT	Üzemi Tanács

2 Adatvédelmi alapelvek

13. A Társaság által végzett adatkezelések, adatfeldolgozások során az alábbi adatvédelmi alapelveknek kell érvényesülniük.

2.1 Jogszerűség, tisztességes eljárás és átláthatóság

14. 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 a jogai gyakorlásának módjáról megfelelő tájékoztatást kapott. A tájékoztatásnak könnyen hozzáférhetőnek és közérthetőnek kell lennie.

2.2 A célhoz kötöttség elve

15. 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 az, hogy az adatkezelés csak pontosan meghatározott és jogszerű célból történhet.

2.3 Az adattakarékosság elve

16. A személyes adatok az adatkezelés céljai szempontjából megfelelőek és relevánsak kell, hogy legyenek, 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

17. 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 kapcsolat felvételi adatokat tartalmazó nyilvántartások).

2.5 A korlátozott tárolhatóság elve

18. 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

19. 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

20. 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

21. A Társaság az érintettet az adatkezelést megelőzően tájékoztatja. A tájékoztatás megtörténhet úgy is, hogy az adatkezelés részleteiről szóló tájékoztatót az Adatkezelő közzéteszi és erre az érintett figyelmét felhívja.

22. Az érintett kérelmére az Adatkezelő tájékoztatást ad az Adatkezelő kilétéről és elérhetőségéről, az adatvédelmi tisztviselő elérhetőségéről, az érintett általa kezelt, illetve az általa megbízott adatfeldolgozó által feldolgozott adatairól, azok forrásáról, az adatkezelés céljáról, jogalapjáról, időtartamáról, az adatfeldolgozó nevéről, címéről, az adatkezeléssel összefüggő tevékenységéről, az érintett személyes adatainak továbbítása esetén az adattovábbítás jogalapjáról és címzettjéről, továbbá az érintett által gyakorolható jogokról, illetve a Nemzeti Adatvédelmi és Információszabadság Hatósághoz (NAIH) címzett panasz benyújtásának jogáról.

23. Az Adatkezelő elősegíti az érintett jogainak a gyakorlását. Az Adatkezelő köteles a kérelem benyújtásától számított legrövidebb időn belül, legfeljebb azonban egy hónapon belül közérthető formában a tájékoztatást megadni. A tájékoztatás csak akkor tagadható meg, ha az Adatkezelő bizonyítja, hogy az érintettet nem áll módjában azonosítani. Ha 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.

24. A tájékoztatást és intézkedést díjmentesen biztosítja az Adatkezelő. 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.

25. A kérelem egyértelműen megalapozatlan vagy túlzó jellegének bizonyítása az Adatkezelőt terheli.

3.2 Hozzáféréshez való jog

26. 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,
    d) adattárolás időtartama,
    e) érintetti jogok,
    f) jogorvoslat,
    g) adatok forrása, ha nem az érintettől gyűjtötték.

27. Az Adatkezelő az adatkezelés tárgyát képező személyes adatok másolatát az érintett rendelkezésére bocsátja. Ha 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

28. 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

29. 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.

30. 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

31. 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).

32. 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, vagy az Európai Unió vagy az állam fontos közérdekéből.

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

33. 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

34. 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

35. 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.

36. 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

37. 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.

38. 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.

39. 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.

40. 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, úgy egy hónapon belül közli az elutasítás okát és tájékoztatja az érintettet a jogorvoslati lehetőségekről.

41. 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 irányadóak.

4 A Társaság adatvédelmi intézményrendszere

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

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

44. Az adatvédelmi tisztviselő
    a) tájékoztat és szakmai tanácsot ad a Társaság, továbbá a munkatársak részére a GDPR rendelet, valamint az egyéb uniós vagy nemzeti adatvédelmi rendelkezések szerinti kötelezettségeikkel kapcsolatban;
    b) ellenőrzi a GDPR rendeletnek, 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 rendelet 36. cikkében említett előzetes konzultációt is – kapcsolattartó pontként szolgál a Hatóság felé, valamint adott esetben bármely egyéb kérdésben konzultációt folytat vele.

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

46. A Társaság adatvédelmi tisztviselőjének munkáját a JSZI, a BI és az EIBI vezetője és munkatársai támogatják.

47. Az adatvédelmi tisztviselőhöz bármely érintett fordulhat.

48. A Társaság az adatvédelmi tisztviselő elektronikus és postai elérhetőségét közzéteszi a Társaság honlapján az alábbiak szerint: A Társaság adatvédelmi tisztviselője:
    név: dr. Bihary-Buzás Melitta,
    e-mail cím: adatvedelem@nisz.hu,
    telefon: +36-1-896-4049.

5 A munkatársak, álláskeresők személyes adatainak kezelése

5.1 A Társaság toborzási, kiválasztási tevékenységével kapcsolatos adatkezelés

49. 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* című dokumentum tartalmazza.

50. 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

51. 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.

52. 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.

53. 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.

54. 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.

55. A munkatársat dokumentáltan tájékoztatni kell arról, hogy
    a) milyen adatait, milyen célból és jogalappal, mennyi ideig kívánja a Társaság kezelni,
    b) 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.

56. 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.

57. A Társaság a munkatársat csak 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.

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

59. Új belépő munkatársat fentiekről a Szabályzat, valamint a SZOVSZ átadásával tájékozatja a HPI a beléptetési folyamat során. A tájékoztatás megtörténtét a munkatárs az *58. Munkaviszony létesítése és megszüntetése szabályzat 58-NY3 Személyi adatlap nyomtatvány*ának aláírásával elismeri és igazolja.

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

61. 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.

62. A Társaság korlátozza az adatkezelést, ha a munkatárs ezt kéri és a 31. 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.

63. 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. A hatósági erkölcsi bizonyítvány a munkaviszony létesítése szempontjából szükséges, adatbiztonságot érintő tájékoztatást nyújt.

64. 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 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.

65. A személy- és munkaügyi nyilvántartás jogszerűségéért, a személyes adatok védelméért a HPI vezetője felelős.

66. 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, erkölcsi bizonyítvány, a munkatárs legmagasabb iskolai végzettségére, szakképzettségére, idegen nyelv ismeretére vonatkozó iratok másolatai, 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.

67. 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.

68. 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,

69. A munkavégzéssel összefüggésben a HPI-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.

70. 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.

71. Új belépő, nemzetbiztonsági ellenőrzés alá eső munkakörben foglalkoztatandó munkatársak esetében a fenti adatokat a HPI adja át a BI számára.

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

73. 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. Korm. rendelet 6. § (2) bekezdésében, a Be. 71. §-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.

74. A JSZI a Társaság arra kötelezett munkatársai által tett vagyonnyilatkozatokkal összefüggő személyes adatokat kezeli a VNYSZ-ben foglalt előírások szerint.

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

75. A fejezetben rögzített adatkezelés célja a munkaviszonyból származó kötelezettségek teljesítésének ellenőrzése, elszámolás, jogalapja az Mt. 11. § (1) és (2) bekezdése, valamint a GDPR rendelet (49) preambulum bekezdése szerinti jogos érdek.

76. A munkatársak a Társaság által munkavégzés céljából rendelkezésükre bocsátott infokommunikációs eszközöket (pl. számítógép, mobiltelefon) kizárólag munkavégzésre használhatják. Erre tekintettel a Társaság jogosult ellenőrizni a munkatársak e-mailjeit oly módon, hogy a magánjellegű levelek tartalma nem ismerhető meg.

77. A Társaság által biztosított e-mail címhez tartozó postafiók esetében a belső szabályozó eszközökben kijelölt személy jogosult ellenőrizni, hogy annak használata csak munkavégzéssel összefüggően történt-e.

78. Az a tény, hogy ki milyen internet oldalakat és milyen gyakorisággal tekint meg, személyes adatnak minősül. Tekintettel arra, hogy a Társaság az internethasználatot kizárólag munkavégzés céljából engedélyezi, a Társaság jogosult annak ellenőrzésére, hogy azt a munkatárs valóban a munkavégzésre használja-e.

79. A 77-78. 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.

80. 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 rendelet (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.

81. 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.

82. Az infokommunikációs eszközök használatára vonatkozó előírásokat az IBSZ tartalmazza.

5.4 GPS nyomkövetés

83. A Társaság által munkavégzéshez biztosított, GPS nyomkövető rendszerrel felszerelt kulcsos gépjárművek használati szabályait és a nyomkövető rendszerrel kapcsolatos tájékoztatási kötelezettség teljesítésével összefüggő szabályokat a GHSZ 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.

5.5 Biztonságtechnikai rendszerek

84. A Társaság által működtetett biztonságtechnikai rendszerek alkalmazásának szabályait a SZOVSZ 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.

6 A Társaság munkatársai által alkalmazandó általános adatkezelési szabályok

85. 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,

c) személyes adatot tartalmazó papír alapú dokumentum csak zárt borítékban továbbítható,
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.".*
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.

86. Az adatvédelmi tisztviselőnek 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

87. 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 ezen tevékenységével kapcsolatos adatvédelmi és adatbiztonsági szabályokat.

7.2 A Társaság mint kormányzati hitelesítés szolgáltató adatvédelmi, adatbiztonsági kötelezettsége

88. Az 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 ezen tevékenységgel kapcsolatos adatvédelmi és adatbiztonsági szabályokat.

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

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

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

90. A 451/2016. Korm. rendelet alapján a Társaság által működtetett országos telefonos ügyfélszolgálati tevékenységre vonatkozóan a Társaság 1818.hu honlapján közzétett, Tájékoztató az országos telefonos ügyfélszolgálat belső adatvédelmi szabályairól című dokumentum rögzíti az ezen tevékenységgel 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

91. 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. Korm. rendelet 6. § (2) bekezdésében, a Be. 71. §-ában és a Pp. 322. §-ában meghatározott adatszolgáltatások teljesítése,
   c) biztonsági incidensek kezelése, naplózási és logelemzési tevékenység,
   d) a *Biztonságos internet Hotline* üzemeltetése.

8 A Társaság mint adatfeldolgozó

92. 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 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 adatkezelési műveletekhez kapcsolódó technikai feladatokat 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 rendelet 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

93. 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.

94. 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.

95. A Társaság fenntartja azt a jogot, hogy az adatbiztonság szabályainak, valamint a nemzetbiztonsági érdekek érvényesítése céljából a munkatársak személyes adataiba és a Társaság által kezelt egyéb személyes adatokba betekintést nyerjen. Az adatkezelés jogalapja ezekben az esetekben a GDPR rendelet (49) preambulum bekezdése szerinti jogos érdek. Ezen betekintési jogot a Társaság nevében a BI vezetője, az elektronikus információs rendszerben tárolt adatok esetén, a 80. pontban szabályozott biztonsági eseménnyel kapcsolatban az EIBI vezetője vagy az általuk kijelölt személyek gyakorolják.

96. Az 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.

97. Az elektronikus információbiztonság feltételeinek érvényesítése érdekében az EIBI, a fizikai biztonság feltételeinek érvényesítése érdekében pedig a BI az gondoskodik az érintett munkatársak megfelelő felkészítéséről és továbbképzéséről.

98. 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.

99. 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.

100. A Társaság a papír alapú nyilvántartások és adathordozók védelme körében gondoskodik különösen a 99. a) és d) alpont szerinti intézkedések értelemszerű alkalmazásáról.

101. 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.

102. Az elektronikus információbiztonságról részletesen az IBSZ, a fizikai biztonság részletszabályairól a SZOVSZ rendelkezik.

103. Adatvédelmi incidens bekövetkezése esetén haladéktalanul értesíteni kell az adatvédelmi tisztviselőt, valamint a BI és az EIBI vezetőjét, megjelölve az incidens valamennyi ismert részletét. Az adatvédelmi tisztviselő és az incidenssel érintett egyéb szervezeti egységek vezetői mérlegelik, hogy az incidens kockázattal jár-e a természetes személyek jogaira és szabadságaira nézve. Amennyiben igen, úgy a Társaság indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, az incidenst bejelenti a NAIH-nak.

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

105. 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.

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

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

10 Adattovábbítás

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

109. A jogszabályon alapuló, eseti adatszolgáltatás esetén minden esetben meg kell győződni az adatkezelés jogalapjáról, kétség esetén jogi szakértő közreműködést 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.

110. A papír alapú adathordozók kezelésére az ISZ előírásait értelemszerűen alkalmazni kell.

111. Az adattovábbítás tényét és tartalmát az adattovábbítási nyilvántartás rögzíti. A nyilvántartást az adattovábbítást végző szervezeti egységek vezetői kötelesek vezetni. A dokumentálásra elsősorban az adatszolgáltatást kérő, illetve az annak teljesítéséről rendelkező, megfelelően kiadmányozott iratok szolgálnak.

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

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

114. A Társaság az adattovábbításokat naplózza annak érdekében, hogy megállapítható legyen, a személyes adatokat kinek, milyen jogalappal és célból továbbítják. Az érintett az adattovábbításra vonatkozó adatokat tartalmazó naplóba betekinthet, kivéve, ha az adattovábbítás tényéről az érintett jogszabály rendelkezése alapján nem szerezhet tudomást.

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

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

11 Ellenőrzés

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

117. 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.

118. Az ellenőrzésre feljogosított 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.

119. 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

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

121. 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

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

123. 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.

124. 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 rendeletben meghatározott lépéseket.

125. A 124. 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.

126. A NAIH elérhetőségei:
levelezési cím: 1534 Budapest, Pf. 834.,
cím: 1125 Budapest, Szilágyi Erzsébet fasor 22/c,
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

127. A Társaság az általa végzett adatkezelési tevékenységekről nyilvántartást vezet. E nyilvántartás a következő információkat tartalmazza:
a) az Adatkezelő neve és elérhetősége, valamint – ha van ilyen – a közös adatkezelőnek, az adatkezelő képviselőjének és az adatvédelmi tisztviselőnek a neve és elérhetősége,
b) az adatkezelés céljai,
c) az érintettek kategóriáinak, valamint a személyes adatok kategóriáinak ismertetése,
d) olyan címzettek kategóriái, akikkel a személyes adatokat közlik vagy közölni fogják, ideértve a harmadik országbeli címzetteket vagy nemzetközi szervezeteket,
e) 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 rendelet 49. cikk (1) bekezdésének második albekezdés szerinti továbbítás esetében a megfelelő garanciák leírása,
f) ha lehetséges, a különböző adatkategóriák törlésére előirányzott határidők,
g) ha lehetséges, az adatbiztonság érdekében megtett technikai és szervezési intézkedések általános leírása.

128. A Társaság mint adatfeldolgozó nyilvántartást vezet az adatkezelő nevében végzett adatkezelési tevékenységek minden kategóriájáról; a nyilvántartás a következő információkat tartalmazza:
a) az adatfeldolgozó vagy adatfeldolgozók neve és elérhetőségei, és minden olyan adatkezelő neve és elérhetőségei, amelynek vagy akinek a nevében az adatfeldolgozó eljár, továbbá – ha van ilyen – az adatkezelő vagy az adatfeldolgozó képviselőjének, valamint az adatvédelmi tisztviselőnek a neve és elérhetőségei,
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 rendelet 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.

129. A nyilvántartást az adatvédelmi tisztviselő elektronikus formában vezeti. A nyilvántartásban szereplő adatkezelésekre, adatfeldolgozásokra vonatkozó, a 127-128. pontban felsorolt információkat az adott adatkezelést, adatfeldolgozást végző szervezeti egység bocsájtja az adatvédelmi tisztviselő rendelkezésére. A nyilvántartásban szereplő adatkezeléseket, adatfeldolgozásokat, valamint az azokkal kapcsolatosan rögzített információkat az érintett szervezeti egységek bevonásával az adatvédelmi tisztviselő minden év május 31-éig felülvizsgálja.

130. 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 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. Ezen felülvizsgálat körülményeit és eredményét írásban kell dokumentálni. A felülvizsgálatba az adatvédelmi tisztviselőt be kell vonni, részére a felülvizsgálatot tartalmazó dokumentumot meg kell küldeni.

131. A Társaság megkeresés alapján a NAIH rendelkezésére bocsátja a nyilvántartást.

15 Érdekmérlegelési teszt, hatásvizsgálat

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

133. 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, milyen személyes adatok, meddig 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.

134. 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.

135. Az elkészült érdekmérlegelési tesztet az adatkezelést végző szervezeti egység vezetője, az adatvédelmi tisztviselő – amennyiben az ÜT véleményezte az érdekmérlegelési tesztet –, az ÜT elnöke, valamint a Társaság vezérigazgatója aláírásával látja el, és a Szabályzat mellékleteként kiadásra kerül (67-M2-M6 melléklet).

136. 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, akkor 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.

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

138. A Társaság által végzett adatkezelések tekintetében a hatásvizsgálatot akkor kell elvégezni, amennyiben a NAIH által összeállított és nyilvánosságra hozott azon adatkezelési műveletek típusainak a jegyzékében szereplő adatkezelést végez, amelyre vonatkozóan a NAIH álláspontja szerint hatásvizsgálatot kell végezni.

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

16 Kártérítés és sérelemdíj

140. Ha az adatkezelő az érintett adatainak jogellenes kezelésével vagy az adatbiztonság követelményeinek megszegésével másnak kárt okoz, köteles azt megtéríteni. Ha 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, ha 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 annyiban, 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	Belső adattovábbítási nyilvántartás
67-M2	80001/152/15/1 2018. 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 2018. 05. 14.
67-M3	80001/152/15/2 2018. 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 2018. 05. 14.
67-M4	80001/152/15/3 2018. Érdekmérlegelési teszt a GDPR 6. cikke (1) bekezdésének f) pontja szerinti jogos érdek fennállásának megállapítására a NISZ Zrt. általi biztonságtechnikai beléptető rendszer alkalmazásával összefüggésben 2018. 05. 14.
67-M5	80001/152/15/4 2018. 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 2018. 05. 14.
67-M6	80001/152/15/5 2018. 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 2018. 05. 14.

18 Záró rendelkezések

144. A Szabályzat megnevezésének rövidítése: AASZ.

145. A Szabályzat a kiadmányozás napján lép hatályba, ezzel egyidejűleg hatályát veszti a *NISZ Zrt. adatvédelmi és adatbiztonsági szabályzata* 2017. 06. 09-én kiadmányozott, 1.2. verziója.

146. Az 86. pontban foglalt képzések, továbbképzések (e-learning) rendszerét, tematikáját az adatvédelmi tisztviselő 2018. december 31-éig a HPI-vel közösen határozza meg.

147. A Szabályzatot a Társaság intranetes honlapján (https://intranet) és külső honlapján közzé kell tenni.

Budapest, 2018. május "25.".

Szabó Zoltán Attila
vezérigazgató

19 Dokumentumtörténet

Verzió	Hatálybalépés/ változás dátuma	A módosítás rövid leírása
1.	2013. 06. 25.	Első kiadás.
1.0	2016. 09. 30.	A szabályozás új szabályozási rendszerbe illesztéseként 1.0 első kiadás. A szabályozás átdolgozását ezen felül a jogszabályi változások tették szükségessé. A szabályozás a 2013. június 24.-én kiadott szabályozást váltja le.
1.1	2017. 03. 30.	A 2017-ben történt szervezeti változás miatt szervezeti nevek és felelős személyek nevének aktualizálása, az M1 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 rendelet 2018. május 25. napjától kötelezően alkalmazandó valamennyi tagállamban. A módosítás a GDPR rendelettel való összhangot teremti meg.

ADATTOVÁBBÍTÁSI NYILVÁNTARTÁS

Adatkérés tárgya	Adatkérés jogalapja	Érintett szervezeti egység	Tájékoztatásra vonatkozó adatok (adattovábbítás formája, címzett, időpont, elutasítás esetén ennek indoka)

NISZ

IM: 80001/152/15/1 2018.

NISZ Nemzeti Infokommunikációs Szolgáltató Zrt.
H-1081 Budapest, Csokonai utca 3.

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

1. Adott célhoz feltétlenül kell-e személyes adatokat kezelni?

A kamerás megfigyelő rendszer alkalmazásának célja, hogy 0-24 órában biztosítsa a kamera által megfigyelt területek, berendezések vagyonvédelmét, valamint a területre belépők vagy ott tartózkodók életének és testi épségének védelmét, cselekményeinek figyelemmel kísérését. E cél miatt elkerülhetetlen a kamera által rögzített képmás, mint személyes adat kezelése.

2. Munkáltatói jogos érdek pontos meghatározása, pl. személy-és vagyonvédelem, adatbiztonság biztosítása, munkáltatói szabályok betartása, hatékonyabb szolgáltatások.

A NISZ Zrt. által a közigazgatási, állami intézmények részére biztosítandó informatikai szolgáltatások olyan fokú védelemben részesítendők, amely a nemzetbiztonsági szempontokat is figyelembe véve a lehető legmagasabb szinten biztosítja a géptermek, berendezések állapotának, sértetlenségének és a NISZ Zrt. épületeibe belépő vagy ott tartózkodó személyek kilétének és cselekményeinek figyelemmel kísérését.

3. Mi az adatkezelés célja, milyen személyes adatok, meddig tartó adatkezelését igényli?

Az adatkezelés célja a NISZ Zrt. által ellátott feladatokat figyelembe véve az informatikai berendezések és a személyek lehető legmagasabb szintű védelme, tehát a vagyonvédelem és a személyvédelem, illetve az események figyelemmel kísérése. Ennek megteremtése a kamerák által rögzített képmás, mint személyes adat kezelését igényli. Tekintettel arra, hogy a kamerás megfigyeléssel elérendő cél az informatikai szolgáltatások biztosításával összefüggésben megfogalmazott nemzetbiztonsági elvárásoknak történő megfelelés, a kamerák által rögzített adatokra 30 napig van szükség az esetleges incidensek, biztonsági események kivizsgálása és bizonyíthatósága érdekében.

4. **Annak meghatározása, hogy a munkavállalóknak mik lehetnek az érdekeik az adott adatkezelés vonatkozásában (Üzemi Tanács bevonásával).**

A munkavállalók személyhez fűződő jogait érinti, korlátozza a kamerás megfigyelés, képmásuk és mozgásuk rögzítése miatt. A kamerás megfigyelés a munkavállalókban a folyamatos megfigyelés, ellenőrzés érzetét kelti, amely fokozott pszichés terhelést jelent számukra.

5. **Annak meghatározása, hogy miért korlátozza arányosan a munkáltatói jogos érdek a munkavállalói jogokat, várakozásokat.**

A NISZ Zrt., mint állami gazdasági társaság fő feladataként a minisztériumok és egyéb állami intézmények számára nyújt informatikai szolgáltatásokat. Ezen szolgáltatások zavartalan biztosítása nemzetbiztonsági érdek, amely érdeket figyelembe véve a munkavállalók személyiségi jogának a kamerás megfigyelés útján történő korlátozása arányosnak tekinthető.

Budapest, 2018. 05. 14.

Kárpáti Miklós
biztonsági igazgató

Szabó Zoltán Attila
vezérigazgató

dr. Bihary-Buzás Melitta
belső adatvédelmi felelős

dr. Mózes Nikoletta
üzemi tanács elnöke

Ikt: 80001/152/15/2 20B.

NISZ Nemzeti Infokommunikációs Szolgáltató Zrt.
H-1081 Budapest, Csokonai utca 3.

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

1. **Adott célhoz feltétlenül kell-e személyes adatokat kezelni?**

   A GPS nyomkövető rendszer alkalmazásának célja, hogy a NISZ Zrt. kulcsos gépjárműveinek, valamint a gépjárművekben szállított informatikai berendezéseinek, eszközeinek vagyonvédelmét biztosítsa. E cél miatt elkerülhetetlen a GPS nyomkövető rendszer által rögzített személyes adatok kezelése.

2. **Munkáltatói jogos érdek pontos meghatározása, pl. személy-és vagyonvédelem, adatbiztonság biztosítása, munkáltatói szabályok betartása, hatékonyabb szolgáltatások.**

   A NISZ Zrt. által a közigazgatási, állami intézmények részére biztosítandó informatikai szolgáltatások olyan fokú védelemben részesítendők, amely a nemzetbiztonsági szempontokat is figyelembe véve a lehető legmagasabb szinten biztosítja a szolgáltatások ellátásához szükséges vagyonelemek, berendezések és eszközök állapotának sértetlenségét.

3. **Mi az adatkezelés célja, milyen személyes adatok, meddig tartó adatkezelését igényli?**

   Az adatkezelés célja a NISZ Zrt. által ellátott feladatokat figyelembe véve a vagyontárgyak, informatikai berendezések és eszközök lehető legmagasabb szintű védelme, tehát a vagyonvédelem, illetve az események figyelemmel kísérése. Ennek megteremtése a GPS nyomkövető rendszer által rögzített név, jelszó, valamint útvonal adatok, mint személyes adatok kezelését igényli. A GPS által rögzített adatokra 5 évig van szükség a jogszabályokban előírt kötelezettségek teljesítése érdekében.

4. **Annak meghatározása, hogy a munkavállalóknak mik lehetnek az érdekeik az adott adatkezelés vonatkozásában (Üzemi Tanács bevonásával).**

   A munkavállalók személyhez fűződő jogait érinti, korlátozza a GPS nyomkövető rendszer alkalmazása, a kulcsos gépjárművel megtett útvonaladatok rögzítése miatt, különös tekintettel arra, hogy a rendszer nem kapcsolható ki akkor sem, ha a kulcsos gépjárművet a munkavállaló engedéllyel a lakó-vagy tartózkodási helyére viszi. A GPS

nyomkövető rendszer a munkavállalókban a folyamatos megfigyelés, ellenőrzés érzetét kelti, amely fokozott pszichés terhelést jelent számukra.

5. **Annak meghatározása, hogy miért korlátozza arányosan a munkáltatói jogos érdek a munkavállalói jogokat, várakozásokat.**

A NISZ Zrt., mint állami gazdasági társaság fő feladataként a minisztériumok és egyéb állami intézmények számára nyújt informatikai szolgáltatásokat. Ezen szolgáltatások zavartalan biztosítása nemzetbiztonsági érdek, amely érdeket figyelembe véve a munkavállalók személyiségi jogának a GPS nyomkövető rendszer alkalmazása útján történő korlátozása arányosnak tekinthető.

Budapest, 2018.05.14.

Kopcsányi Tibor
beszerzési és logisztikai
igazgató

Szabó Zoltán Attila
vezérigazgató

dr. Bihary-Buzás Melitta
belső adatvédelmi felelős

dr. Mózes Nikoletta
üzemi tanács elnöke

NISZ

Ikt: 80001/152/15/3 20R.

NISZ Nemzeti Infokommunikációs Szolgáltató Zrt.
H-1081 Budapest, Csokonai utca 3.

Érdekmérlegelési teszt

a GDPR 6. cikke (1) bekezdésének f) pontja szerinti jogos érdek fennállásának megállapítására a NISZ Zrt. általi biztonságtechnikai beléptető rendszer alkalmazásával

összefüggésben

1. **Adott célhoz feltétlenül kell-e személyes adatokat kezelni?**

   A biztonságtechnikai beléptető rendszer alkalmazásának célja, hogy ellenőrizhető legyen az objektumba belépők és az objektumon belül mozgók személyazonossága, ezzel biztosítva a védett területek, berendezések vagyonvédelmét, valamint a területre belépők vagy ott tartózkodók életének és testi épségének védelmét, cselekményeinek figyelemmel kísérését. E cél miatt elkerülhetetlen a beléptető által rögzített mozgási adatok és a hozzájuk tartozó személy azonosításához, ezáltal a belépési jogosultság megállapításához szükséges adatok, mint személyes adat kezelése.

2. **Munkáltatói jogos érdek pontos meghatározása, pl. személy-és vagyonvédelem, adatbiztonság biztosítása, munkáltatói szabályok betartása, hatékonyabb szolgáltatások.**

   A NISZ Zrt. által a közigazgatási, állami intézmények részére biztosítandó informatikai szolgáltatások olyan fokú védelemben részesítendők, amely a nemzetbiztonsági szempontokat is figyelembe véve a lehető legmagasabb szinten biztosítja a géptermek, berendezések állapotának, sértetlenségének és a NISZ Zrt. épületeibe belépő vagy ott tartózkodó személyek kilétének, belépési jogosultságának menedzselését és mozgásának figyelemmel kísérését.

3. **Mi az adatkezelés célja, milyen személyes adatok, meddig tartó adatkezelését igényli?**

   Az adatkezelés célja a NISZ Zrt. által ellátott feladatokat figyelembe véve az informatikai berendezések és a személyek lehető legmagasabb szintű védelme, tehát a vagyonvédelem és a személyvédelem, illetve a belépő személyek mozgásának figyelemmel kísérése. Ennek megteremtése a beléptető rendszerben rögzített adatok, mint személyes adat kezelését igényli. Tekintettel arra, hogy a beléptető rendszer alkalmazásával elérendő cél az informatikai szolgáltatások biztosításával összefüggésben megfogalmazott nemzetbiztonsági elvárásoknak történő megfelelés, a beléptető rendszerben tárolt adatokra 6 hónapig van szükség az esetleges incidensek, biztonsági események kivizsgálása és bizonyíthatósága érdekében.

4. **Annak meghatározása, hogy a munkavállalóknak mik lehetnek az érdekeik az adott adatkezelés vonatkozásában (Üzemi Tanács bevonásával).**

A munkavállalók személyhez fűződő jogait érinti, korlátozza a beléptető rendszerrel megvalósított adatgyűjtés, azonosító adataik és mozgásuk rögzítése miatt. A beléptető rendszer által folytatott adatgyűjtés a munkavállalókban a folyamatos megfigyelés, ellenőrzés érzetét kelti, amely fokozott pszichés terhelést jelent számukra.

5. **Annak meghatározása, hogy miért korlátozza arányosan a munkáltatói jogos érdek a munkavállalói jogokat, várakozásokat.**

A NISZ Zrt., mint állami gazdasági társaság fő feladataként a minisztériumok és egyéb állami intézmények számára nyújt informatikai szolgáltatásokat. Ezen szolgáltatások zavartalan biztosítása nemzetbiztonsági érdek, amely érdeket figyelembe véve a munkavállalók személyiségi jogának a beléptető rendszer útján történő korlátozása arányosnak tekinthető.

Budapest, 2018. 05. 14.

Kárpáti Miklós
biztonsági igazgató

Szabó Zoltán Attila
vezérigazgató

dr. Bihary-Buzás Melitta
belső adatvédelmi felelős

dr. Mózes Nikoletta
üzemi tanács elnöke

Ikt: 80001/152/15/4 2018.

NISZ Nemzeti Infokommunikációs Szolgáltató Zrt.
H-1081 Budapest, Csokonai utca 3.

Érdekmérlegelési teszt

a GDPR 6. cikke (1) bekezdésének f) pontja szerinti jogos érdek fennállásának megállapítására a NISZ Zrt. által a beléptető rendszerből nyert munkaidőadatok alkalmazásával

összefüggésben

1. **Adott célhoz feltétlenül kell-e személyes adatokat kezelni?**

   A beléptető rendszerből nyert munkaidő alkalmazásának célja a Munka törvénykönyvében előírt munkaidő nyilvántartás naprakészségének megteremtése. A munkaidő nyilvántartáshoz feltétlenül szükséges személyes adatokat kezelni, hiszen a munkaidő teljesítése csak személyhez kötötten értelmezhető.

2. **Munkáltatói jogos érdek pontos meghatározása, pl. személy-és vagyonvédelem, adatbiztonság biztosítása, munkáltatói szabályok betartása, hatékonyabb szolgáltatások.**

   A munkaidő adatok beléptető rendszerből történő kinyerése a munkaidő nyilvántartás leghatékonyabb módja jelenleg a NISZ Zrt. számára, tekintve, hogy az irodaházakban a beléptető rendszerek rendelkezésre állnak, költséghatékony módját megteremtve a NISZ Zrt-nek, mint közpénzből gazdálkodó állami gazdasági társaságnak a Mt. előírásainak való megfelelésnek.

3. **Mi az adatkezelés célja, milyen személyes adatok, meddig tartó adatkezelését igényli?**

   Az adatkezelés célja az Mt. szerinti munkaidő nyilvántartási kötelezettségnek való megfelelés.
   A munkaidő nyilvántartáshoz szükséges személyes adatok az érintett neve, törzsszáma, jelenléti és távolléti adatai. Az adatok a munkaidő elszámolásának alapját képezik, így ezzel összefüggésben a vonatkozó törvényekben meghatározott időtartamig kezelni kell ezeket.

4. **Annak meghatározása, hogy a munkavállalóknak mik lehetnek az érdekeik az adott adatkezelés vonatkozásában (Üzemi Tanács bevonásával).**

   A munkavállalók személyhez fűződő jogait érinti, korlátozza a munkaidő adatok beléptető rendszerből történő kinyerése, mozgásuk rögzítése miatt. A beléptető rendszer által folytatott adatgyűjtés a munkavállalókban a folyamatos megfigyelés, ellenőrzés érzetét kelti, amely fokozott pszichés terhelést jelent számukra.

5. **Annak meghatározása, hogy miért korlátozza arányosan a munkáltatói jogos érdek a munkavállalói jogokat, várakozásokat.**

A munkaidő adatok beléptető rendszerből való kinyerésével a NISZ Zrt. az Mt-ben megfogalmazott kötelezettségét teljesíti, ugyanakkor ezen adatok nem szolgálnak a munkavállalók teljesítményének mérésére.
Fentieket figyelembe véve a munkavállalók személyiségi jogának ezen adatkezeléssel történő korlátozása arányosnak tekinthető.

Budapest, ...2018. 05. 14.....

Bertényi Réka
Humánerőforrás igazgató

Szabó Zoltán Attila
Vezérigazgató

dr. Bihary-Buzás Melitta
belső adatvédelmi felelős

dr. Mózes Nikoletta
üzemi tanács elnöke

Ikt.: 8000/152/15/5 2018.

NISZ Nemzeti Infokommunikációs Szolgáltató Zrt.
H-1081 Budapest, Csokonai utca 3.

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

1. **Adott célhoz feltétlenül kell-e személyes adatokat kezelni?**

   A hatósági erkölcsi bizonyítvány bekérésének célja az arról való meggyőződés, hogy a NISZ Zrt-hez belépő munkavállaló büntetlen előéletű és nem áll foglalkoztatástól eltiltás hatálya alatt sem. Ezen célból feltétlenül szükséges személyes adatokat kezelni, mivel a hatósági erkölcsi bizonyítvány a munkavállaló vonatkozásában több személyes adatot is tartalmaz.

2. **Munkáltatói jogos érdek pontos meghatározása, pl. személy-és vagyonvédelem, adatbiztonság biztosítása, munkáltatói szabályok betartása, hatékonyabb szolgáltatások.**

   A NISZ Zrt. által a közigazgatási, állami intézmények részére biztosítandó informatikai szolgáltatások olyan fokú védelemben részesítendők, amely megköveteli, hogy a NISZ Zrt. minden új munkavállalója tekintetében meggyőződjön az erkölcsi feddhetetlenségről, igazodva a NISZ Zrt. ellátotti körébe tartozó minisztériumok és egyéb kormányzati intézmények által követett gyakorlathoz.

3. **Mi az adatkezelés célja, milyen személyes adatok, meddig tartó adatkezelését igényli?**

   A hatósági erkölcsi bizonyítvány bekérésének célja az arról való meggyőződés, hogy a NISZ Zrt-hez belépő munkavállaló büntetlen előéletű és nem áll foglalkoztatástól eltiltás hatálya alatt sem. Az adatkezelés körébe azon személyes adatok tartoznak, amelyek a hatósági erkölcsi bizonyítványon szerepelnek.
   Az erkölcsi bizonyítványban szereplő személyes adatokat a bizonyítvány érvényességi idejének lezártáig kezeljük. Az átadott erkölcsi bizonyítvány számát és keltét, valamint a büntetlen előélettel és a foglalkoztatástól való eltiltással kapcsolatos megállapítását az általános munkajogi elévülési ideig kezeljük.

4. **Annak meghatározása, hogy a munkavállalóknak mik lehetnek az érdekeik az adott adatkezelés vonatkozásában (Üzemi Tanács bevonásával).**

   A munkavállalók személyhez fűződő jogait érinti, korlátozza hatósági erkölcsi bizonyítvány bekérése, mivel az – részben –a magánélet ellenőrzésére irányul.

5. **Annak meghatározása, hogy miért korlátozza arányosan a munkáltatói jogos érdek a munkavállalói jogokat, várakozásokat.**

A NISZ Zrt., mint állami gazdasági társaság fő feladataként a minisztériumok és egyéb állami intézmények számára nyújt informatikai szolgáltatásokat. Ezen szolgáltatások zavartalan biztosítása nemzetbiztonsági érdek, amely érdeket figyelembe véve a munkavállalók személyiségi jogának a hatósági erkölcsi bizonyítvány bekérése útján történő korlátozása arányosnak tekinthető.

Budapest, 2018.05.14.

Bertényi Réka
humánerőforrás igazgató

Szabó Zoltán Attila
vezérigazgató

dr. Bihary-Buzás Melitta
belső adatvédelmi felelős

dr. Mózes Nikoletta
üzemi tanács elnöke