9/2022. sz. Ügyvezetői utasítás

a Digitális Kormányzati Fejlesztés és Projektmenedzsment Korlátolt Felelősségű Társaság Adatvédelmi szabályzatáról

1. A Digitális Kormányzati Fejlesztés és Projektmenedzsment Kft. Adatvédelmi szabályzatáról a következő utasítást adom ki.
2. Az utasítás az aláírásának napján lép hatályba.
3. Jelen utasítás a munka törvénykönyvéről szóló 2012. évi I. törvény 17. § (2) bekezdésére tekintettel a közzététel napján a munkavállalókkal közöltnek tekintendő

	Kovács Zsolt János Digitálisan aláírta: Kovács Zsolt János Dátum: 2022.02.16 17:04:26 +01'00'
	Kovács Zsolt János *ügyvezető*
Jogi megfelelőség:	Dr. Hegedűs Dóra Digitálisan aláírta: Dr. Hegedűs Dóra Dátum: 2022.02.16 12:06:25 +01'00'
	dr. Hegedűs Dóra *jogi és beszerzési igazgató*

ADATVÉDELMI SZABÁLYZAT

Verziószám: 1.0

Tartalomjegyzék

I. Általános rendelkezések

I.1. A szabályzat célja

1) Jelen Adatvédelmi Szabályzat (a továbbiakban: Szabályzat) a Digitális Kormányzati Fejlesztés és Projektmenedzsment Korlátolt Felelősségű Társaság (a továbbiakban: DKF vagy Társaság) által vezetett és kezelt, személyes adatokat tartalmazó nyilvántartásokkal kapcsolatos legfontosabb adatvédelmi szabályokat tartalmazza az információs önrendelkezési jogról és információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) és AZ EURÓPAI PARLAMENT ÉS A TANÁCS 2016. április 27-i (EU) 2016/679 RENDELETE a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (a továbbiakban: „általános adatvédelmi rendelet" vagy „GDPR") alapján; különös tekintettel az adatkezeléssel, adatfeldolgozással és adattovábbítással kapcsolatos követelményekre.
2) A Szabályzat célja, hogy meghatározza a Társaságnál vezetett személyes adatokat tartalmazó nyilvántartások jogszabályoknak megfelelő kezelési rendjét, a Társaság adatvédelmi szervezetét, valamint biztosítsa az adatvédelem alkotmányos elveinek, az adatvédelem követelményeinek érvényesülését, és megakadályozza az adatokhoz történő jogosulatlan hozzáférést, azok megváltoztatását és jogosulatlan nyilvánosságra hozatalát.
3) A személyes adatok kezeléséhez kapcsolódó további szabályokat állapíthatnak meg a X. fejezetben (kapcsolódó szabályzatok) felsorolt szabályzatok, továbbá ott fel nem sorolt munkáltatói utasítások.

I.2. Személyi hatály

4) A Szabályzat hatálya kiterjed a Társaság valamennyi szervezeti egységére, valamint a Társasággal munkaviszonyban, vagy munkavégzésre irányuló egyéb jogviszonyban foglalkoztatott (együtt: Foglalkoztatott) személyre.
5) A Szabályzat hatálya kiterjed továbbá – a velük kötött szerződésben és a titoktartási nyilatkozatban foglalt mértékben – a Társasággal szerződéses jogviszonyban álló természetes személyekre, jogi személyekre és egyéb szervezetekre, valamint ezek alkalmazottaira is a velük kötött polgári jogi szerződésekben meghatározott mértékben.

I.3. Tárgyi hatály

6) A Szabályzat tárgyi hatálya kiterjed a Társaság minden szervezeti egységénél folytatott valamennyi olyan folyamatra, amely során a GDPR 4. cikk 1. pontjában meghatározott személyes adat kezelése megvalósul.

I.4. Alapfogalmak

7) A jelen Szabályzatban alkalmazott alapfogalmak a GDPR alapfogalmaival megegyezőek, illetve az adatvédelmi jogszabályok gyakorlati alkalmazása érdekében kerültek megfogalmazásra.
8) Adatgazda: Felelős a Társaság adatainak kezeléséért, és biztosítja az adatkezelés jogszerűségét.

9) Személyes adat: Azonosított vagy azonosítható természetes személyre („érintett”) vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható.
10) Adatkezelés: 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.
11) Adatfeldolgozó: Az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel.
12) Adatkezelőt képviselő személy: Az adatkezelő adatkezelést végző munkavállalója.
13) Adatkör-gazda: Az adott szervezeti egységnél vezető beosztásban levő, jelen Szabályzat mellékletében (1. számú melléklet) feltüntetett olyan kompetens személy, aki mind szakmailag, mind hatáskörben megfelelően képes a felelősségi körébe utalt adatkör felett rendelkezni.
14) Címzett: Az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, akivel vagy amellyel a személyes adatot közlik, függetlenül attól, hogy harmadik fél-e. Azon közhatalmi szervek, amelyek egy egyedi vizsgálat keretében az uniós vagy a tagállami joggal összhangban férhetnek hozzá személyes adatokhoz, nem minősülnek címzettnek; az említett adatok e közhatalmi szervek általi kezelése meg kell, hogy feleljen az adatkezelés céljainak megfelelően az alkalmazandó adatvédelmi szabályoknak.
15) Harmadik fél: Az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely nem azonos az érintettel, az adatkezelővel, az adatfeldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére felhatalmazást kaptak.
16) Az érintett hozzájárulása: 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 egy vagy több konkrét célból történő kezeléséhez.
17) Adatvédelmi incidens: A biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi.
18) Adattörlés: Az adatok felismerhetetlenné tétele oly módon, hogy a helyreállításuk többé nem lehetséges.
19) Közérdekű adat: Az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől, így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat.
20) NAIH: Nemzeti Adatvédelmi és Információszabadság Hatóság.
21) Nyilvánosságra hozatal: Az adat bárki számára történő hozzáférhetővé tétele.

22) Tiltakozás: Az érintett nyilatkozata, amellyel személyes adatainak kezelését kifogásolja, és az adatkezelés megszüntetését, vagy a kezelt adatok törlését kéri.

II. Adatkezelésre vonatkozó általános szabályok

II.1. Az adatkezelés alapelvei, általános előírások

23) A Társaság adatkezelésének alapelveit a Társaság általános adatkezelési tájékoztatója tartalmazza. Az érdemérlegelés jogalapja esetében az érdekmérlegelési tesztet a 2. számú melléklet szerint kell elvégezni.
24) A Társaságnál bevezetésre került az ún. beépített adatvédelem (privacy by design). Ennek biztosítása érdekében, az adatkezelés tényleges megkezdése előtt – már a projektelőkészítés szakaszában is – figyelemmel kell lenni a GDPR előírásaira, ezért a Társaság minden szervezeti egysége az adatkezelés megkezdése előtt köteles – szükség esetén a Társaság adatvédelmi tisztviselőjének bevonásával – megvizsgálni, hogy magvalósul-e az érintettek GDPR szerinti tájékoztatása, vagy az adatkezeléshez az érintettek hozzájárultak-e, és az adatkezelés során biztosítottak-e: az érintettek jogai, a szükséges és elégséges adatbiztonsági követelmények.
25) A Társaságnál kizárólag csak olyan adat kezelhető, amely az adott szervezeti egység feladatának ellátásához, illetve az adatkezelés céljának megvalósulásához elengedhetetlen, és a cél elérésére alkalmas. A személyes adat csak a cél megvalósulásához szükséges mértékben és ideig kezelhető.
26) Az adatkezelésnek minden szakaszában meg kell felelnie az adatkezelés céljának, az adatok felvételének és kezelésének tisztességesnek és törvényesnek kell lennie. Az adatkezelést a Társaságnál csak akkor lehet megkezdeni, ha az adatkezelés a vonatkozó valamennyi jogszabályi feltételnek megfelel és az érintettek jogai biztosítottak.
27) Ha a Szabályzat hatálya alatt álló személy tudomást szerez arról, hogy a Társaság által kezelt személyes adat hibás, hiányos vagy időszerűtlen, köteles a helyesbítését az adat rögzítéséért felelős munkatársnál kezdeményezni.
28) Az adatkezelési cél megszűnését követően az adatok törlésére az adatot ténylegesen kezelő munkavállaló köteles gondoskodni. A törlést az adatgazda, valamint az adatvédelmi tisztviselő bármikor jogosult ellenőrizni.
29) A Társaságnál minden Foglalkoztatott felelősséggel tartozik a feladatai teljesítése során végzett adatkezelés jogszerűségéért, jelen utasításban foglaltak betartásáért, különösen akkor, ha feladatai teljesítése során a jogszerűen megismert személyes adatot illetéktelen személy részére átadja, vagy hozzáférhetővé teszi, vagy a jogosulatlan adatlekérést hajt végre.
30) Ha valamely Foglalkoztatottnak tudomására jut, hogy a jogszabályban, vagy a jelen utasításban foglalt adatvédelmi vagy adatbiztonsági rendelkezéseket megsértették, vagy ennek veszélye áll fenn, az adatvédelmi tisztviselőt haladéktalanul tájékoztatja.
31) Az adatvédelmi szabályok betartását és betartatását az alábbi intézkedések biztosítják:

    a) éves adatvédelmi önellenőrzés (belső audit) lefolytatása,
    b) adatvédelmi oktatások tartása és számonkérés,
    c) adatvédelmi szabályzat kiadás, felülvizsgálat, módosítás,
    d) munkáltatói szankciós intézkedések

32) Az éves adatvédelmi belső auditok során az adatgazdáknak kötelezően vizsgálni kell

a) az adatok nyomon követhetőségét (különös tekintettel az adattovábbítási nyilvántartásokra);
b) az adatkezelés célhoz kötöttségét, jogalapját;
c) az adatbiztonsággal, irat- és adatkezeléssel kapcsolatos szabályzatok megfelelőségét;
d) az adattörlések végrehajtását és annak dokumentálását;
e) az érintettek megfelelő tájékoztatására vonatkozó bizonyítékokat;
f) az esetlegesen szükséges titoktartási nyilatkozatokat.

II.2. Adattovábbítás szabályai

33) Személyes adatok továbbítására kizárólag jogszabály felhatalmazása, vagy az érintett hozzájárulása alapján kerülhet sor. Ha az adattovábbítás feltétlei fennállnak, csak naprakész, pontos adat továbbítható.
34) A harmadik fél felé történő adattovábbítás esetén az adattovábbítást minden esetben írásban dokumentálni kell oly módon, hogy annak menete és jogszerűsége bizonyítható legyen. Az egyes adatkezelési tájékoztatókban tájékoztatni kell az érintetteket az adattovábbítások tényéről és címzettjeiről. Az adattovábbítás előtt az adatkezelést végző Foglalkoztatott az adatvédelmi tisztviselőt tájékoztatja az adattovábbítás lényeges jellemzőiről (a kezelt adatok továbbításának módja és időpontja, a továbbított adatkörök, az adattovábbítás jogalapja, az adattovábbítás címzettje, az adattovábbításért felelős neve és elérhetősége) szükség esetén kikéri álláspontját. Az adattovábbításokról az adatvédelmi tisztviselő naprakész nyilvántartást vezet.
35) Amennyiben az adatátadás nem elektronikus adatátviteli úton keresztül valósul meg, úgy az adatátadás kizárólag iktatott dokumentumon történhet a Társaság belső szabályzataiban írtaknak megfelelően.
36) A jogszabályon alapuló adattovábbítási kötelezettség esetén az adatgazda, illetve az adattovábbítást végző foglalkoztatott minden esetben köteles ellenőrizni az adattovábbítás jogalapjának meglétét, szükség esetén kikéri az adatvédelmi tisztviselő álláspontját.
37) Nem minősül adattovábbításnak:

a) egy nyilvántartáson (nyilvántartási rendszeren) belül az egymással alá- fölé- vagy mellérendeltségi kapcsolatban lévő szervezeti egységek adatfeldolgozási célú adatátadása;
b) az érintett saját adatairól történő tájékoztatása.

38) Az adattovábbítást regisztrálni kell (adattovábbítási nyilvántartás), annak érdekében, hogy megállapítható legyen, hogy milyen adat, kinek, milyen felhatalmazottság alapján, mikor került továbbításra vagy kiszolgáltatásra.
39) Az adatszolgáltatás feltételeit kétség esetén az adatgazda az adatvédelmi tisztviselő közreműködésével köteles ellenőrizni.
40) Harmadik személy vagy szerv által benyújtott adattovábbítási kérelem elbírálása – a törvényben kötelezően előírt adattovábbítás esetét kivéve – az adatvédelmi tisztviselő feladata.
41) Abban az esetben, ha az adatszolgáltatást nem lehet jogszerűen teljesíteni, vagy az igény elbírálásához szükséges információkat az adatigénylő a felkérést követően sem jelölte meg, úgy az adattovábbítást meg kell tagadni. Az adattovábbítás megtagadásáról – annak indokolásával együtt – írásban kell értesíteni az adatigénylőt.

42) Az adatgazda gondoskodik az adatok biztonságáról, különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés megakadályozásáról. Ezen biztonsági intézkedések sérelme esetén az adatgazda köteles az észlelést követően haladéktalanul értesíteni az adatvédelmi tisztviselőt a szükséges intézkedések megtétele érdekében.

II.3. Adattovábbítási nyilvántartás

43) Az adatkezelő szervezeti egység a kezelt személyes adat továbbításáról – a Szabályzat 3. számú. melléklete szerinti – nyilvántartást vezet, amely tartalmazza az általa kezelt személyes adatok továbbításának időpontját, az adattovábbítás jogalapját és címzettjét, a továbbított személyes adatok körének meghatározását, valamint az adatkezelést előíró jogszabályban meghatározott egyéb adatokat.
44) A fenti adattovábbítási nyilvántartás történhet adatbázisban, vagy papír alapú iktatott dokumentum formában.
45) Az adattovábbítási nyilvántartás megőrzési ideje 5 év.

II.4. Adatfeldolgozás szabályai

46) A Társaság csak olyan adatfeldolgozót vehet igénybe, amely megfelelő garanciákat nyújt az adatvédelmi követelmények teljesülését biztosító technikai és szervezési intézkedéseket végrehajtására és az adatkezelés biztonságára. Az adatfeldolgozónak a személyes adatok feldolgozásával kapcsolatos jogait és kötelezettségeit az adatkezelésre vonatkozó jogszabályok, és az adatfeldolgozásra vonatkozó, adatkezelő és adatfeldolgozó között létrejött szerződés határozza meg.
47) A Társaság és az adatfeldolgozó közötti adatfeldolgozásra vonatkozó rendelkezéseket szerződésbe kell foglalni.
48) Az adatfeldolgozó az adatkezelést érintő érdemi döntést nem hozhat, a tudomására jutott személyes adatokat kizárólag az adatkezelő rendelkezései szerint dolgozhatja fel, saját céljára adatfeldolgozást nem végezhet, továbbá a személyes adatokat az adatkezelő rendelkezései szerint köteles tárolni és megőrizni.
49) Az adatfeldolgozó tevékenységének ellátása során más adatfeldolgozót kizárólag a Társaság által előzetes, írásban tett eseti felhatalmazás alapján vehet igénybe.
50) Az adatfeldolgozással nem bízható meg olyan szervezet, amely a feldolgozandó személyes adatokat felhasználó üzleti tevékenységben érdekelt.
51) Az igénybe vett adatfeldolgozókról az adatvédelmi tisztviselő – az adatgazdák tájékoztatása alapján – nyilvántartást vezet.

II.5. Szervezeten belüli adatkezelés és az adatkezelések összekapcsolása

52) A Társaság szervezetén belül a munkavállalók és egyéb munkavégzésre irányuló jogviszonyban állók személyes adatai a feladat elvégzéséhez szükséges mértékben és ideig csak olyan szervezeti egységhez juttathatók el, amelyek a munkaviszonnyal vagy munkavégzésre irányuló egyéb jogviszonnyal kapcsolatos adminisztratív és szervezési feladatokat látnak el. Indokolt esetben az adatkezelést végző szervezeti egység vezetője hatáskörében az adatokhoz történő hozzáférés jogosultsági szintjei differenciáltan is megállapíthatók.
53) A Társaságnál folyó különböző célra irányuló adatkezelések csak törvényben meghatározottak alapján, indokolt esetben, ideiglenesen kapcsolhatók össze.

III. Az adatvédelem szervezete

III.1. Az ügyvezető

54) A Társaság mindenkori vezető tisztségviselője (ügyvezető) a Társaság sajátosságainak figyelembevételével meghatározza az adatvédelem szervezetét, az adatvédelemre, valamint az azzal összefüggő tevékenységre vonatkozó feladat- és hatásköröket, és kijelöli az adatkezelés felügyeletét ellátó személyt. Az ügyvezető

a) felelős az érintettek GDPR-ban meghatározott jogainak gyakorlásához szükséges feltételek biztosításáért;

b) felelős a Társaság által kezelt személyes adatok védelméhez szükséges személyi, tárgyi és technikai feltételek biztosításáért;

c) felügyeli az adatvédelmi tisztviselő tevékenységét;

d) adatvédelmi vizsgálatot rendelhet el;

e) kiadja a Társaság adatvédelemmel kapcsolatos belső szabályait.

III.2. Az adatvédelmi tisztviselő

55) A Társaság adatvédelmi rendszerének felügyeletét a vezető tisztségviselő által kijelölt adatvédelmi tisztviselő látja el.
56) Az adatvédelmi tisztviselőt szakmai rátermettség, és különösen az adatvédelmi jog és gyakorlat szakértői szintű ismerete, valamint a GDPR szerinti feladatok ellátására való alkalmasság alapján kell kijelölni.
57) A Társaság az adatvédelmi tisztviselő nevét és elérhetőségét közzéteszi honlapján, valamint bejelenti ezen adatokat a NAIH részére.
58) Az adatvédelmi tisztviselő jogállását és feladatait a jelen Szabályzat IX. pontja tartalmazza.

III.3. Adatgazdák

59) A Társaság szervezetén belül az adatkezelést végző szervezeti egységek vezetői, mint adatgazdák, felelősek az irányításuk alá tartozó szervezeti egységek adatkezelésének jogszerűségéért, jelen Szabályzat végrehajtásáért és betartatásáért.
60) Az adatgazdák jogosultak a jelen Szabályzattal összhangban az általuk vezetett szervezeti egység tekintetében az adatkezeléssel összefüggő eljárásrend, munkautasítások kiadására.
61) Jogosulatlan hozzáférés vagy az adatvédelmi előírások egyéb megsértésének észlelése esetén az adatvédelmi tisztviselő egyidejű tájékoztatása mellett intézkedést tesznek annak megszüntetésére, indokolt esetben kezdeményezik a felelősségre vonási eljárás lefolytatását.
62) Adatvédelmi incidens bekövetkezése esetén – az általuk vezetett szervezeti egység érintettsége esetén – részt vesznek az adatvédelmi tisztviselő által összehívott munkacsoport munkájában.
63) Felelősek az általuk irányított szervezeti egységeik tekintetében az adatkezelési nyilvántartás(ok) folyamatos, naprakész vezetéséről, és kötelesek azt az adatvédelmi tisztviselő részére hozzáférhetővé tenni.

III.4. Az adatkezelést végző foglalkoztatottak

64) A Foglalkoztatott köteles az általa kezelt adatokat a jogszabályok és a Társaság belső szabályzatai alapján kezelni, feldolgozni, tárolni és megőrizni. Köteles a tudomására jutott személyes adatokat titokként kezelni és a személyes adatokat csak az arra jogosult részére hozzáférhetővé tenni.
65) Adatvédelmi incidens gyanúja esetén köteles a jelen Szabályzat V. pontja szerint eljárni.
66) A Foglalkoztatott köteles a feladatellátása során felmerült adatkezelési problémáról, visszásságról az adatvédelmi tisztviselőt értesíteni, továbbá az adatvédelmi tisztviselő feladatai ellátásának elősegítése érdekében az adatvédelmi tisztviselő kérésére az adatkezeléssel kapcsolatos kérésére információt szolgáltatni.
67) A Foglalkoztatott köteles vezetője útján az éves adatvédelmi jelentéshez adatot szolgáltatni.
68) Az adatkezelést végző Foglalkoztatott az adatkezelést érintő érdemi döntést nem hozhat, saját céljára adatkezelést, adattárolást nem végezhet.

III.5. Az információbiztonsági felelős

69) Az információbiztonsági felelős tevékenyége ellátása során köteles kiemelt figyelmet fordítani a személyes adatokat érintő biztonsági intézkedések megvalósítására.
70) Az adatvédelmi tisztviselő bevonásával gondoskodik a Társaság elektronikus információs rendszere tekintetében az adatvédelem és adatbiztonság érvényesítéséről, és tevékenysége során együttműködik az adatvédelmi tisztviselővel a Társaság adatbiztonságának fenntartásában.
71) Adatvédelmi incidens esetén részt vesz a jelen Szabályzatban meghatározott adatvédelmi munkacsoport munkájában, az adatvédelmi incidens megoldásában.

IV. Adatbiztonság

72) Az adatkezelő szervezeti egység vezetője, valamint adott tevékenységi körében az adatfeldolgozó köteles gondoskodni a hatáskörében kezelt személyes adatok biztonságáról, továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek jelen Szabályzat, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.
73) Az adatokat az adatkezelőnek megfelelő intézkedésekkel védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen.
74) A különböző nyilvántartásokban elektronikusan kezelt adatállományok védelme érdekében megfelelő technikai megoldással biztosítani kell, hogy célhoz kötöttség elve érvényesüljön, és a nyilvántartásokban tárolt adatok – kivéve, ha azt törvény lehetővé teszi – közvetlenül ne legyenek összekapcsolhatók és az érintetthez rendelhetők.
75) A személyes adatok automatizált feldolgozása során az adatkezelő, és ha van, akkor az adatfeldolgozó is köteles biztosítani 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 az alábbiakat:

a) a jogosulatlan adatbevitel megakadályozását;
b) az automatikus adatfeldolgozó rendszerek jogosulatlan személyek általi, adatátviteli berendezés segítségével történő használatának megakadályozását;
c) annak ellenőrizhetőségét és megállapíthatóságát, hogy a személyes adatokat adatátviteli berendezés alkalmazásával mely szerveknek továbbították vagy továbbíthatják;
d) annak ellenőrizhetőségét és megállapíthatóságát, hogy mely személyes adatokat, mikor és ki rögzítette, vagy módosította az automatikus adatfeldolgozó rendszerekben;
e) a telepített rendszerek üzemzavar esetén történő helyreállíthatóságát és
f) azt, hogy az automatizált feldolgozás során fellépő hibákról jelentés készüljön.

76) Az adatkezelésben résztvevő szervezeti egység vezetője köteles az adatkezelési műveleteket úgy megtervezni és végrehajtani, hogy az adatkezelésre vonatkozó más szabályok alkalmazása során biztosítsa az érintettek magánszférájának védelmét, az adatvédelmi követelmények betartásával.

IV.1. A papír alapon kezelt adatok biztonsága

77) A papíralapon kezelt személyes adatok biztonsága érdekében a Társaság az alábbi intézkedéseket alkalmazza:

a) a személyes adatokat csak azon személyek részére teszi hozzáférhetővé, akiknek a személyes adatot tartalmazó dokumentum, irat felhasználása a feladata ellátáshoz szükséges, és csak olyan mértékben, amely az adott feladat ellátásához feltétlenül szükséges;
b) a személyes adatokat tartalmazó dokumentumokat, iratokat zárható, száraz, tűzvédelemmel ellátott helyiségben helyezi el;
c) a munkavégzés befejeztével a papíralapú adathordozók elzárásra kerülnek;
d) amennyiben a papíralapon kezelt személyes adatok digitalizálásra kerülnek, a digitálisan tárolt dokumentumokra irányadó biztonsági szabályokat alkalmazza a Társaság.

78) Amennyiben a papíralapon tárolt személyes adat kezelésének célja megvalósult, és nincs más jogalap az adatkezelésre vonatkozóan, vagy jogszabályi kötelezettség alapján nem kell az iratot tovább őrizni, úgy a Társaság intézkedik a papír, vagy amennyiben a személyes adatok adathordozója nem papír, hanem más fizikai eszköz, úgy a fizikai eszköz megsemmisítéséről.

IV.2. Elektronikus információs rendszerben kezelt személyes adatok biztonsága

79) A Társaság az elektronikus formában rögzített személyes adatok kezeléséhez az alkalmazott informatikai eszközöket úgy üzemelteti, hogy a kezelt adat:

a) csak az arra feljogosítottak számára legyen hozzáférhető (rendelkezésre állás)
b) hitelessége és hitelesítése biztosított (adatkezelés hitelessége);
c) változatlansága igazolható legyen (adatintegritás);
d) a jogosulatlan hozzáférés ellen védett legyen (adat bizalmassága).

80) A számítógépen, illetve hálózaton tárolt személyes adatok biztonsága érdekében a Társaságnál legalább az alábbi intézkedéseket kell alkalmazni:
   a) a számítógépen, és a hálózaton található adatokhoz csak érvényes, személyre szóló, azonosítható jogosultsággal – legalább felhasználói névvel és jelszóval – lehessen csak hozzáférni, a jelszavak cseréjéről rendszeresen, illetve indokolt esetben gondoskodni kell;
   b) az adatokkal történő művelet nyomon követhető módon naplózni kell;
   c) hálózati kiszolgáló gépen (a továbbiakban: szerver) tárolt adatokhoz csak megfelelő jogosultsággal és csakis az arra kijelölt személyek férhessenek hozzá;
   d) amennyiben az adatkezelés célja megvalósult, az adatkezelés határideje letelt, úgy az adatot tartalmazó fájl visszaállíthatatlanul törlni kell;
   e) a Társaság a hálózaton tárolt adatok biztonsága érdekében a szervereket magas rendelkezésre állású infrastruktúrával kell védeni, az adatvesztést biztonsági mentésekkel kell megakadályozza;
   f) a személyes adatokat kezelő hálózaton a vírusvédelemről folyamatosan és naprakészen gondoskodni kell;
   g) meg kell akadályozni illetéktelen személyek hálózati hozzáférését;
   h) számítástechnikai, távközlési eszközök és programok helyességének ellenőrzésére, felhasználók betanítására, oktatási célra, sajtónak adott tájékoztatásra valós személyes adatokat felhasználni tilos.

81) Az elektronikus információs rendszerben tárolt személyes adatok fizikai, logikai védelméről és szabályairól, így különösen a jogosultsági szabályokról, mentési rendről, hálózat védelmi intézkedésekről a Társaság informatikai biztonsági szabályzata rendelkezik.

IV.3. Jogosultságkezelés

82) A jogosultságkezelés szabályozásának célja, hogy a kiosztott jogosultságok pontosan nyomon követhetőek legyenek, dokumentált formában megőrzésre kerüljenek, valamint az egyes jogosultságokkal rendelkező személyek tevékenysége és az általuk felhasznált adatok köre ellenőrizhető legyen. Ezen adatok naprakészsége nagymértékben hozzásegíti a Társaságot a tőle elvárt, illetve általa elérhető biztonsági szint teljesítéséhez, továbbá a jogszabályi és szakmai normák szerinti tevékenység ellátására.
83) A jogosultságok változásait (létező jogosultságok, új jogosultságok kiosztása, módosítása, megszűnése) dokumentálni kell.
84) A személyes adatok biztonsága érdekében a Társaság az alábbi jogosultságkezelési előírásokat alkalmazza:
   a) új jogosultság beállítását, illetve jogosultság megváltoztatását az adatgazda felhatalmazása alapján rendszergazdai jogosultsággal rendelkező munkavállaló végzi;
   b) a jogosultságok megállapítása során kizárólag a munkavégzéshez szükséges és elégséges jogosultságokat lehet kiosztani;
   c) adminisztrátori jogosultsággal rendelkező nevesített felhasználót kell alkalmazni minden esetben, ahol ez lehetséges. A nem nevesített felhasználói jogosultságok használatát indokolni és dokumentálni kell;
   d) nem munkavállaló folyamatosan működő, korlátlan időre szóló hozzáférési jogosultsággal nem rendelkezhet.

85) A jogosultságkezelésre vonatkozó részletes szabályokat a Társaság belső szabályzata tartalmazza.

V. Adatvédelmi incidens

86) Az adatvédelmi incidens a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi, így különösen de nem kizárólag munkahelyi laptop, telefon, adathordozó elvesztése; honlap feltörése, hálózat elleni támadás, személyes adatok illetéktelen személyek számára történő rendelkezésre bocsátása, hozzáférhetővé tétele.

V.1. Az adatvédelmi incidens észlelése

87) A Társaság minden Foglalkoztatottja köteles a Társaságon belül történt adatvédelmi incidenst haladéktalanul, de legkésőbb 8 órán belül jelenteni a szervezeti egysége vezetőjének, vagy kapcsolattartójának, valamint ezzel egyidejűleg az adatvédelmi tisztviselőnek.
88) A bejelentést a szervezeti egység vezetőjének munkahelyi e-mail címére és az adatvedelem@dkfkft.hu e-mail címre kell megküldeni. A bejelentésnek tartalmaznia kell a bejelentő nevét, telefonszámát, beosztását, szervezeti egységének megnevezését, valamint az incidens tárgyát, rövid leírását és azt, hogy az incidens érinti-e a Társaság informatikai rendszerét.
89) Amennyiben az adatvédelmi incidens érinti a Társaság informatikai rendszerét is, akkor a bejelentést az Infokommunikációs Igazgatónak és információbiztonsági felelősnek is meg kell küldeni.
90) A bejelentés adatvédelmi tisztviselőhöz érkezését követően az adatvédelmi tisztviselő vezetésével haladéktalanul meg kell kezdi az adatvédelmi incidens kivizsgálását és értékelését.

V.2. Az adatvédelmi incidens kivizsgálása, értékelése

91) Az adatvédelmi tisztviselő – informatikai rendszert érintő incidens esetén Infokommunikációs Igazgatóval együttműködve – megvizsgálja a bejelentést és amennyiben szükséges, a bejelentőtől további adatokat kér az incidensre vonatkozóan. Az adatvédelmi tisztviselő felhívására a bejelentő köteles megadni: az adatvédelmi incidens bekövetkezésének időpontját és helyét, az adatvédelmi incidens egyéb körülményeit, az adatvédelmi incidens által érintett adatok körét, mennyiségét, az adatvédelmi incidenssel érintett személyek körét és számát, az adatvédelmi incidens várható hatásait, az adatvédelmi incidens megelőzésére, következményeinek enyhítésére megtett intézkedések felsorolását.
92) A bejelentő az adatszolgáltatást haladéktalanul, de legkésőbb 8 órán belül teljesíti az adatvédelmi tisztviselő részére.
93) Amennyiben az adatvédelmi tisztviselő megállapítása alapján az adatvédelmi incidens vizsgálatot igényel az adatvédelmi tisztviselő 24 órán belül munkacsoportot hoz létre, amelynek tagja a jogi és beszerzési igazgató és az érintett szervezeti egység vezetője és a Társaság információbiztonsági felelőse. Amennyiben az incidens a Társaság elektronikus információs rendszerét is érinti a munkacsoport tagja az Infokommunikációs igazgató is. A munkacsoport tagjainak érintettsége esetén a Társaság ügyvezetője jelöl az érintett tag helyett más munkavállalót.

94) A vizsgálat megállapításainak tartalmaznia kell, hogy az adatvédelmi incidens magas kockázattal jár-e az érintettek jogaira és kötelezettségeire nézve, milyen jellegű kockázatról van szó, és szükséges-e az érintettek tájékoztatása az incidensről. Amennyiben nem szükséges az érintettek tájékoztatása, a vizsgálat megállapításainak tartalmazni kell ennek indokait is.
95) A vizsgálat eredményeként a munkacsoport meghatározza az adatvédelmi incidens kezelésének módját és felhívja az intézkedésre jogosult személyt az incidens kezelésére és az adatvédelmi tisztviselő az adatvédelmi incidenst rögzíti az adatvédelmi incidensek nyilvántartásában.
96) A vizsgálatot legkésőbb a bejelentés adatvédelmi tisztviselőhöz érkezésétől számított 72 órán belül be kell fejezni és a vizsgálat eredményéről a Társaság vezető tisztségviselőjét az adatvédelmi tisztviselő tájékoztatja.

V.3. Az adatvédelmi incidens bejelentése a Hatóság részére

97) Az adatvédelmi tisztviselő az adatvédelmi incidenst a bekövetkezését követően haladéktalanul, de legkésőbb az incidens bekövetkezésétől számított 72 órán belül bejelenti a Hatóság részére, kivéve, ha az incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Ha a bejelentés nem történik meg határidőben, az adatvédelmi tisztviselő köteles ennek okát igazolni a Hatóság részére.

98) A hatósági bejelentésnek tartalmaznia kell:
- az adatvédelmi incidenssel érintett adatok körét és hozzávetőleges számát,
- az adatvédelmi incidenssel érintett személyek körét és hozzávetőleges számát,
- az adatvédelmi incidens jellegét, körülményeit,
- az adatvédelmi tisztviselő nevét és elérhetőségét,
- az adatvédelmi incidens valószínűsíthető következményeit és
- az adatvédelmi incidens orvoslására és enyhítésére megtett intézkedéseket.

V.4. Az érintettek tájékoztatása az adatvédelmi incidensről

99) Ha a vizsgálat eredményeként megállapítást nyert, hogy az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságára nézve és az érintettek tájékoztatása szükséges, az adatvédelmi tisztviselő haladéktalanul értesíti az érintetteket és a Társaság vezető tisztségviselőjét.

100) Nem kell az érintetteket tájékoztatni:
- ha a Társaság olyan technikai, szervezési, védelmi intézkedéseket hajtott végre az érintett adatokra vonatkozóan, amelyek megakadályozzák az illetéktelen személyek számára való hozzáférést az adatokhoz vagy megakadályozzák az adatok értelmezhetőségét;
- ha az adatvédelmi incidens bekövetkezését követően a Társaság olyan intézkedéseket tett, amelyek biztosítják, hogy a feltárt adatkezelési kockázat valószínűsíthetően nem valósul meg;
- ha a tájékoztatás aránytalan erőfeszítést tenne szükségessé. Ebben az esetben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, mely tájékoztatás elektronikus úton is megtörténhet.

V.5. Az adatvédelmi incidensek nyilvántartása

101) Az adatvédelmi incidensről az adatvédelmi tisztviselő nyilvántartást vezet.
102) A nyilvántartás tartalmazza:
- az érintett személyes adatok körét,
- az adatvédelmi incidenssel érintettek körét és számát,
- az adatvédelmi incidens időpontját,
- az adatvédelmi incidens körülményeit, hatásait,
- az elhárítására megtett intézkedéseket és
- egyéb jogszabályban előírt adatokat.

103) Az adatvédelmi incidensnyilvántartás (4. számú melléklet) pontos vezetéséről, aktualizálásáról az adatvédelmi tisztviselő gondoskodik.

VI. A nyilvántartásokkal és munkavégzéssel kapcsolatos általános szabályok

VI.1. Az adatok tárolása

104) Az adatok tárolása három típusú nyilvántartásban történik:
a) informatikai nyilvántartás,
b) manuális nyilvántartás,
c) vegyes nyilvántartás.

105) Az adatok tárolását úgy kell megválasztani, hogy – az esetleges eltérő törlési határidőre is tekintettel – törlésük elvégezhető és a törlés ténye ellenőrizhető legyen.
106) Az egyes nyilvántartásokban az alábbi típusú adatokat kezelnek:

a) személyes adatok,
b) közérdekű,
c) közérdekből nyilvános,
d) egyéb adatok,
e) technikai adatok.

107) Az alábbi technikai adatokat kell – a kezelt személyes adatok jogalapjának megszűnését és azok törlését követően – a számítógépes nyilvántartásba vett adathordozón 5 évig tárolni:

a) személyes adatok továbbításának dátuma,
b) személyes adatok törlésének dátuma.

VI.2. Ellenőrzési, intézkedési feladatok

108) Ha a Foglalkoztatott adatvédelemmel kapcsolatos jogszabálysértésekről tudomást szerez, köteles azt haladéktalanul, de legkésőbb az észlelés napját követő munkanapon a közvetlen vezetőjének jelenteni.
109) A személyes adatokat is kezelő rendszerek minden tervezett módosítását, bővítését megelőzően, az abban érintett munkavállalók kötelesek az adatkezelést végző szervezeti egység vezetője részére tájékoztatást nyújtani, szükség esetén őt a módosítással vagy bővítéssel kapcsolatos egyeztetésekbe bevonni.

VI.3. Adatvagyonnal kapcsolatos rendelkezések

110) Az adatgazda az adatvédelmi tisztviselő bevonásával a Társaság teljes adatvagyonát adatvédelmi osztályokba sorolja, kialakítja az adatköröket és kinevezi az adatkör-gazdákat, meghatározza az adatkezelés és adatfeldolgozás irányelveit.

111) A Társaság által kezelt valamennyi adat tekintetében – adatkörök kialakítása mellett –, valamennyi adatkörhöz adatkör-gazda kijelölése szükséges (ld. 1. számú. melléklet). Egy adatkörnek csak egy adatkör-gazdája lehet, míg egy személy több adatkör felett is rendelkezhet adatkör-gazdai jogkörrel.

VII. Az érintettek jogai és érvényesítésük

112) Az érintettek jogait és azok érvényesítésével kapcsolatos előírásokat a Társaság általános adatkezelési tájékoztatója tartalmazza, amelyet a Társaság a honlapján közzétesz.

113) A Társaság bármely szervezeti egységéhez, vagy munkavállalójához, megbízottjához beérkezett adatkezeléssel kapcsolatos kérelmeket, panaszokat haladéktalanul meg kell küldeni a Társaság adatvédelmi tisztviselőjének az adatvedelem@dkfkft.hu e-mail címre. A kérelem iktatására a Táraság iratkezelési szabályzata előírásai vonatkoznak.

114) Az adatvédelmi tisztviselő a kérelem kézhezvételét követő 3 munkanapon belül értesíti a kérelemről az adatkezeléssel érintett szervezeti egység vezetőjét, és bekéri a kérelem elbírálásához, illetve megválaszolásához szükséges információkat.

115) Az érintett szervezeti egység vezetője köteles az adatvédelmi tisztviselő kérésének a lehető legrövidebb idő alatt, de legfeljebb 5 munkanapon belül olyan módon és részletezettséggel eleget tenni, hogy az érintett kérelme teljesíthető, illetve megválaszolható legyen.

116) Ha kérelem teljesítése olyan összetettségű, hogy a 115. pontban rögzített határidő nem elegendő, akkor a szervezeti egység vezető indokolással alátámasztott elektronikus levélben javasolja az adatvédelmi tisztviselőnek a kérelem teljesítésére előírt határidő GDPR szerinti meghosszabbítását. Amennyiben a kérelemben foglaltak teljesítése kimutathatóan aránytalan dologi és/vagy személyi jellegű költséggel (papír/adathordozó költsége, aránytalan mértékű munkaerőráfordítás) jár, ennek mértékéről az adatgazda tételes kimutatást (a továbbiakban: költségkimutatás-tervezet) készít, amelyet szintén megküld az adatvédelmi tisztviselőnek.

117) Amennyiben az adatvédelmi tisztviselő az indokolás alapján a kérelem teljesítésének meghosszabbításáról dönt, úgy a kérelem beérkezésétől számított 30 napon belül az érintettnek címzett, a meghosszabbítás tényéről és indokairól, valamint az esetlegesen felmerülő költségekről szóló tájékoztató levelet köteles megküldeni.

118) Az érintett kérelmére az adatvédelmi tisztviselő – az adatgazdák, és az adatkezelést végző munkavállalók tájékoztatása alapján – tájékoztatást ad az érintettről kezelt, valamint a Társaság megbízott adatfeldolgozója által kezelt adatairól, azok forrásáról, az adatkezelés céljáról, jogalapjáról, időtartamáról, az adatfeldolgozó nevéről, címéről és az adatkezeléssel összefüggő tevékenységéről, továbbá – az érintett személyes adatainak nem minősített formában érkező kérés és továbbítás esetén - az adattovábbítás jogalapjáról és címzettjéről.

119) Az érintett adattovábbításra, törlésre, helyesbítésre, zárolásra irányuló kérelmére a Társaság mint adatkezelő nevében eljárva az adatvédelmi tisztviselő köteles a kérelem benyújtásától számított lehető legrövidebb idő alatt, de legfeljebb a törvényes határidőben közérthető formában írásban megadni, a megtörtént intézkedésekről a tájékoztatást.

120) Az érintett tájékoztatása csak jogszabályban meghatározott esetekben tagadható meg. A tájékoztatás megtagadása esetén az adatvédelmi tisztviselő írásban közli az érintettel, hogy a felvilágosítás megtagadására jogszabály mely rendelkezése alapján került sor. A felvilágosítás megtagadása esetén az érintettet tájékoztatni kell a bírósági jogorvoslat, továbbá a NAIH-hoz fordulása lehetőségéről.

121) Az elutasított kérelmekről az adatvédelmi tisztviselő a NAIH-ot évente a tárgyévet követő év január 31-éig tájékoztatja.

122) A kérelem teljesíthetősége esetén az adatgazda haladéktalanul, de legkésőbb az adatvédelmi tisztviselő felhívásától számított 5 munkanapon belül köteles a kérelmet teljesíteni, és a kérelem teljesítéséről az adatvédelmi tisztviselőt az adatvedelem@dkfkft.hu e-mail címen tájékoztatni.

123) A helyesbítésről, a zárolásról, a megjelölésről és a törlésről az érintettet, továbbá mindazokat értesíteni kell, akiknek korábban az adatot adatkezelés céljára továbbították. Az értesítés mellőzhető, ha ez az adatkezelés céljára való tekintettel az érintett jogos érdekét nem sérti.

124) Ha a Társaság az érintett helyesbítés, zárolás vagy törlés iránti kérelmét nem teljesíti, a kérelem kézhezvételét követő egy hónapon belül írásban közli a helyesbítés, zárolás vagy törlés iránti kérelem elutasításának ténybeli és jogi indokait. A helyesbítés, törlés vagy zárolás iránti kérelem elutasítása esetén az adatvédelmi tisztviselő tájékoztatja az érintettet a bírósági jogorvoslat, továbbá a NAIH-hoz fordulás lehetőségéről.

VIII. Az érintett előzetes tájékoztatásának követelménye

125) Az érintettel a személyes adata kezelésének megkezdése előtt közölni kell, hogy az adatkezelés hozzájáruláson alapul vagy kötelező.

126) Az érintettet az adatkezelés megkezdése előtt az érintettel kapcsolatba került adatkezelőt képviselőnek az érintettet egyértelműen és részletesen tájékoztatni kell az adatai kezelésével kapcsolatos minden tényről, így különösen
   a) az adatkezelés céljáról és jogalapjáról,
   b) az adatkezelésre és az adatfeldolgozásra jogosult személyéről,
   c) az adatkezelés időtartamáról,
   d) arról, ha az érintett személyes adatait a Társaság. mint adatkezelő továbbítja,
   e) arról, hogy kik ismerhetik meg az adatokat,
   f) az adatvédelmi tisztviselő elérhetőségéről,
   g) az érintett jogairól és jogérvényesítési lehetőségeiről.

127) Az érintettnek adott tájékoztatás tényét, tartalmát a személyes és elektronikus ügyintézés során egyaránt dokumentálni kell.

128) A tájékoztatásnak ki kell terjednie az érintett adatkezeléssel kapcsolatos jogaira és jogorvoslati lehetőségeire is. Kötelező adatkezelés esetén a tájékoztatás megtörténhet a fenti információkat tartalmazó jogszabályi rendelkezésekre való utalás nyilvánosságra hozatalával is.

129) Olyan adatkezelés esetén, amikor az érintettek személyes tájékoztatása lehetetlen vagy aránytalan költséggel járna, a tájékoztatás megtörténhet az alábbi információk nyilvánosságra hozatalával is:

   a) az adatgyűjtés ténye,
   b) az érintettek köre,
   c) az adatgyűjtés célja,
   d) az adatkezelés időtartama,

e) az adatok megismerésére jogosult lehetséges adatkezelők személye,
f) az érintettek adatkezeléssel kapcsolatos jogainak és jogorvoslati lehetőségeinek ismertetése, valamint
g) ha az adatkezelés adatvédelmi nyilvántartásba vétel köteles, akkor az adatkezelés nyilvántartási száma.

IX. Az adatvédelmi tisztviselő

IX.1. Az adatvédelmi tisztviselő jogállása

130) A Társaság biztosítja, hogy az adatvédelmi tisztviselő a személyes adatok védelmével kapcsolatos összes ügyben megfelelő módon és időben bekapcsolódjon.
131) A Társaság támogatja az adatvédelmi tisztviselőt feladatai ellátásában.
132) Az adatvédelmi tisztviselő a feladatai ellátásával kapcsolatban utasításokat senkitől nem fogadhat el. Az adatvédelmi tisztviselőt feladatai ellátásával összefüggésben a Társaság nem bocsáthatja el és szankcióval nem sújthatja. Az adatvédelmi tisztviselő közvetlenül a Társaság ügyvezetőjének tartozik felelősséggel.
133) Az érintettek a személyes adataik kezeléséhez és az e rendelet szerinti jogaik gyakorlásához kapcsolódó valamennyi kérdésben az adatvédelmi tisztviselőhöz fordulhatnak.
134) Az adatvédelmi tisztviselőt feladatai teljesítésével kapcsolatban uniós vagy tagállami jogban meghatározott titoktartási kötelezettség vagy az adatok bizalmas kezelésére vonatkozó kötelezettség köti.
135) Az adatvédelmi tisztviselő más feladatokat is elláthat. Az adatkezelő vagy az adatfeldolgozó biztosítja, hogy e feladatokból ne fakadjon összeférhetetlenség.

IX.2. Az adatvédelmi tisztviselő feladatai

136) Az adatvédelmi tisztviselő tevékenységi körében:

a) közreműködik, és segítséget nyújt az adatkezeléssel összefüggő döntések meghozatalában, valamit az érintettek jogainak biztosításában;
b) az érintett szervezeti egységek bevonásával megválaszolja a Társasághoz beérkezett adatkezeléssel kapcsolatos megkereséseket, panaszokat;
c) kérésre szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomon követi a hatásvizsgálat elvégzését;
d) regisztrálja a jelen Szabályzat értelmében hozzá beérkezett adatvédelemmel kapcsolatos eseteket;
e) az adatvédelmi tisztviselő jogosult az adatvédelemre vonatkozó előírások betartását ellenőrizni a Társaság szervezeti egységeinél;
f) az önellenőrzésekről készült jegyzőkönyveket összesíti és az éves tevékenységéről a felső vezetés számára tárgyévet követő május 31-ig összefoglaló jelentést készít;
g) jogszabályi változás, vagy egyéb szükséges esetben kezdeményezi jelen Szabályzat aktualizálását;
h) gondoskodik az adatvédelmi ismeretek oktatásáról;
i) tájékoztat és szakmai tanácsot ad a Társaság és annak adatkezelést végző munkavállalói részére a GDPR, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezések szerinti kötelezettségeikkel kapcsolatban;

j) nyilvántartást vezet az adatvédelmi incidensekről;
k) együttműködik a felügyeleti hatósággal;
l) vezeti a jelen Szabályzat szerinti egyéb nyilvántartásokat;
m) részt vesz NAIH által szervezett adatvédelmi tisztviselők konferenciáján;
n) az adatkezeléssel összefüggő ügyekben kapcsolattartó pontként szolgál a NAIH felé, valamint bármely egyéb kérdésben konzultációt folytat a Hatósággal.

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

138) Feltárt törvénysértés, adatvédelmi incidens vagy aggályos működési gyakorlat esetén az illetékes terület vezetője értesíti az esetről az adatvédelmi tisztviselőt, és a jogért felelős szakterület bevonásával közösen meghatározzák a szakterület teendőit a megfelelőség helyreállítására. A terület vezetője az egyeztetett határidőre elvégzi a meghatározott intézkedést, melyről az adatvédelmi tisztviselő útján az ügyvezetőnek jelentést tesz.

139) Az éves adatvédelmi önellenőrzések során az adatvédelmi tisztviselőnek vizsgálni kell:

a) az adatvédelmi nyilvántartásokat;
b) az adattovábbítás, a statisztikai adatközlés, a tájékoztatás és a tiltakozás nyilvántartását;
c) az adatvédelmi oktatások megtörténtét, azok dokumentálását.

IX.3. Adatvédelmi nyilvántartás

140) Az adatvédelmi tisztviselő által vezetett adatvédelmi nyilvántartás kötelező tartalmi elemeit a GDPR 30. cikkének (1) bekezdése és az Infotv. 25/E. § (1) bekezdése határozzák meg.

IX.4. Belső adatvédelmi audit

141) A Társaság adatvédelmi tisztviselője jogosult általános és célellenőrzéseket végezni a Társaságnál folytatott adatkezelések vonatkozásában minden szervezeti egységnél. Az ellenőrzés megkezdéséről az ügyvezetőt - az ellenőrzés megkezdéséig, vagy azzal egyidejűleg - tájékoztatni köteles.

142) Az adatvédelmi tisztviselő 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.

143) Az adatvédelmi tisztviselő jogosult az irat és adatkezeléssel kapcsolatos belső dokumentumok, jegyzőkönyvek és nyilvántartások áttekintésével ellenőrizni az adatkezelés törvényes rendjének megtartását.

144) Az adatvédelmi tisztviselő részére a belső hálózaton az ellenőrzéshez szükséges mértékben és ideig hozzáférési jogosultságot kell biztosítani.

145) Az adatvédelmi auditról az adatvédelmi tisztviselő jegyzőkönyvet köteles felvenni, és az adatvédelmi audit megállapításairól és az esetleges jogsértések megszüntetésére tett javasolt intézkedésekről köteles a Társaság ügyvezetőjét értesíteni.

X. Kapcsolódó szabályozások

146) Külső szabályozás - törvények, jogszabályok

a) AZ EURÓPAI PARLAMENT ÉS A TANÁCS 2016. április 27-i (EU) 2016/679 RENDELETE a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről („általános adatvédelmi rendelet" vagy „GDPR")
b) Az információs önrendelkezési jogról és információszabadság szóló 2011. évi CXII. törvény (Infotv.)
c) A statisztikáról szóló 1993. évi XLVI. törvény
d) A Munka Törvénykönyvéről szóló 2012. évi I. törvény

147) Belső szabályozás:

a) Adatvédelmi tájékoztatók

Mellékletek

1. sz. melléklet Érdemérlegelési teszt minta
2. sz. melléklet Adatkör-gazdák listája
3. sz. melléklet Adattovábbítási nyilvántartás
4. sz. melléklet Adatvédelmi incidensnyilvántartás