Az NKE Campus XXI. Szolgáltató Nonprofit Korlátolt Felelősségű Társaság ügyvezető igazgatója által kiadott

24/2021. számú szabályzat

AZ ADATVÉDELEM SZABÁLYAIRÓL

A Szabályzat célja, hogy a NKE Campus XXI. Szolgáltató Nonprofit Kft. (a továbbiakban: Társaság) a tevékenysége során az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvényben (a továbbiakban: Info. tv.), valamint az Európai Parlament és a Tanács 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 (EU) 2016/679 rendeletében (a továbbiakban: GDPR) foglaltaknak megfelelően eljárva biztosítsa az adatvédelem alapelveinek az információs önrendelkezési jognak és az adatbiztonság követelményeinek érvényesülését.

I. Fejezet
Általános rendelkezések

1. A szabályzat alkalmazhatósága

1. A Szabályzat alkalmazására a Társaság valamennyi munkavállalója és más jogviszony keretében foglalkoztatott dolgozója (a továbbiakban együtt: Munkavállaló) köteles.

2. A Társaságnak biztosítania kell a Szabályzat rendelkezéseinek érvényesülését a Társasággal szerződéses jogviszonyban álló magánszemélyekre, jogi személyekre és egyéb szervezetekre és ezek tagjaira, Foglalkoztatottaira is, továbbá biztosítani kell, hogy az érintett személyek a Szabályzatot a szükséges mértékben megismerjék.

3. A Szabályzat nem alkalmazható az informatikai és biztonságtechnikai eszközökkel összefüggő konkrét adatbiztonsági intézkedések meghatározására. Az iratok és az informatikai eszközök kezelése során az NKE Informatikai Biztonsági Szabályzata (a továbbiakban: IBSZ) szerint (https://www.uni-nke.hu/informatikai-biztonsagi-szabalyzat) kell eljárni.

2. Értelmező rendelkezések

4. Jelen szabályzat alkalmazásában használt fogalmak:
   a) **Adatbiztonság**: a személyes adatok jogosulatlan kezelése, így különösen jogosulatlan megszerzése, feldolgozása, megváltoztatása és megsemmisítése elleni szervezési, technikai megoldások, valamint eljárási szabályok összessége; az adatkezelés azon állapota, amelyben az adatok sérülésének, illetéktelen felhasználásának, megsemmisülésének kockázati tényezőit – és ezáltal a fenyegetettséget – a szervezési, műszaki megoldások és intézkedések a minimálisra csökkentik.

b) **Adatfeldolgozó**: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel.

c) **Adatkezelés**: az alkalmazott eljárástól függetlenül az adaton végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adat további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése vagy az adatokba való betekintés.

d) **Adatkezelő**: az a természetes vagy jogi személy, közhatalmi szerv, illetve jogi személyiséggel nem rendelkező bármely szervezet, aki, vagy amely önállóan vagy másokkal együtt az adat kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja.

e) **Adatvédelmi hatásvizsgálat**: amennyiben valamely tervezett adatkezelés – figyelemmel annak jellegére, hatókörére, körülményeire és céljaira, ideértve különösen az új technológiák alkalmazásának esetét – valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, a Társaság hatásvizsgálatot végez, amelynek célja annak megállapítása, hogy a tervezett adatkezelés a személyes adatok védelmét hogyan érinti. Az adatvédelmi hatásvizsgálat egy olyan eljárás, amelynek során az adatkezelő a tervezett adatkezelési műveletet vagy műveleteket áttekinti, megvizsgálja az adatkezelés érintettekre gyakorolt esetleges hatását, felméri annak kockázatait, a kockázatok kezelésének módját, és mindezt megfelelően dokumentálja.

f) **Adatvédelmi incidens**: személyes adat jogellenes kezelése vagy feldolgozása, így különösen a jogosulatlan közlés vagy azokhoz való hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, elvesztés, valamint a véletlen megsemmisülés és sérülés.

g) **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.

h) **Érdekmérlegelési teszt**: jogos érdeken alapuló adatkezelés folytatása vagy tervezett bevezetése esetén annak írásbeli dokumentálása, hogy az adatkezelő számba vette az adatkezelést megalapozó érdekeket, érveket, valamint az érintettek személyes adatok védelméhez fűződő – a tervezett adatkezelés ellen ható – jogait és érdekeit, és ezen érdekek és érvek összevetésével megalapozza az adatkezelés bevezetését vagy a bevezetés elutasítását.

i) **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.

j) **Harmadik ország**: minden olyan állam, amely nem EGT-állam.

k) **Személyes adat**: az azonosított vagy azonosítható természetes személyre („érintettre") 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.

3. Az adatvédelem alapelvei

5. Az adatvédelem alapelvei:
   a) A ***jogszerűség, tisztességes eljárás és átláthatóság elve*** szerint a személyes adatok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni.
   b) A ***célhoz kötöttség elve*** alapján az adatgyűjtés során ügyelni kell arra, hogy azok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történjen, és azokat nem lehet ezekkel a célokkal össze nem egyeztethető módon kezelni. Nem minősül az eredeti céllal össze nem egyeztethetőnek a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból történő további adatkezelés.
   c) Az ***adattakarékosság elve*** értelmében a kezelt adatok az adatkezelés céljai szempontjából megfelelőek és relevánsak kell hogy legyenek és a szükséges mértékre kell korlátozódniuk.
   d) A ***személyes adatoknak pontosnak és szükség esetén naprakésznek kell lenniük*** és az adatkezelőnek minden észszerű intézkedést meg kell tennie annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatok haladéktalanul törlésre vagy helyesbítésre kerüljenek.
   e) A ***korlátozott tárolhatóság elvé***re figyelemmel 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 akkor kerülhet sor, amennyiben a személyes adatok kezelésére a jogszabályi előírásoknak megfelelően közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból kerül sor, az érintettek jogainak és szabadságainak védelme érdekében előírt megfelelő technikai és szervezési intézkedések végrehajtására is figyelemmel.
   f) Az ***integritás és bizalmas jelleg elvét*** biztosítandó, a személyes adatok kezelését olyan 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.
   g) A Társaság, mint adatkezelő felelős az alapelveknek való megfelelésért (GDPR 5. cikk (1) bekezdés), továbbá az ***elszámoltathatóság elvé***nek megfelelően képesnek kell lennie e megfelelés igazolására is (GDPR 5. cikk (2) bekezdés). A megfelelőség igazolása különösen az adatkezeléshez kapcsolódó döntéseket megalapozó körülmények és a döntések (pl. az adatkezelés feltételeit meghatározó döntéselőkészítő iratok), az érintetteknek szóló adatkezelési tájékoztatók, az érintettektől származó nyilatkozatok (pl. hozzájáruló nyilatkozatok, az adatkezelési tájékoztató megismerését igazoló dokumentumok), továbbá a személyes adatokat tartalmazó (elektronikus vagy papír alapú) dokumentumok szervezeten belüli vagy azon kívüli mozgásának megfelelő dokumentálásával történik. A Társaság – a GDPR 30. cikkének megfelelően – nyilvántartást vezet az általa végzett adatkezelésekről.

II. Fejezet
Az adatvédelmi tevékenység szervezete és irányítása a Társaságnál

6. Az adatvédelmi tevékenység irányításában és ellátásában a Társaság munkavállalói – a Társaság Szervezeti és Működési Szabályzatában (a továbbiakban: SZMSZ) meghatározott feladatkörükön belül – az alábbiak szerint vesznek részt azzal, hogy a Társaság központi irányítási – ide nem értve értelemszerűen az adatvédelmi tisztviselőt, illetve a tűz-és munkavédelmi koordinátort – és a szakmai szervezeti egységei adatvédelmi kapcsolattartóval rendelkeznek.

4. Az ügyvezető igazgató feladatai

7. Az ügyvezető igazgató felelős azért, hogy a Társaság – mint adatkezelő, illetve adatfeldolgozó – működése az adatvédelmi szabályoknak megfeleljen. Ennek érdekében:
   a) gondoskodik az adatvédelmi tevékenység irányításában és ellátásában résztvevő személyek kijelöléséről, feladataik, az adatvédelmi tárgyú ügyekkel kapcsolatos döntési jogkörök meghatározásáról, az egyes adatkezelési döntési szintek kialakításáról,
   b) biztosítja az adatvédelmi tevékenység irányításához és ellátásához, valamint az érintett jogai gyakorlásához szükséges személyi és tárgyi feltételeket,
   c) felelős az adat- és titokvédelmi, valamint biztonsági és információbiztonsági szabályzatok kiadásáért és betartatásáért,
   d) gondoskodik arról, hogy az adatvédelmi tevékenység során esetleg előforduló, feltárt hiányosságok megszűntetéséről, szükség szerint a felelősségre vonásról,
   e) kinevezi a Társaság adatvédelmi tisztviselőjét.

8. Az ügyvezető az adatvédelemmel kapcsolatos egyes feladat- és hatásköröket – jogszabály eltérő rendelkezése hiányában – delegálhatja.

5. Az adatvédelmi tisztviselő feladatai

9. Az adatvédelmi tisztviselőt a Társaság ügyvezető igazgatója bízza meg.

10. Az adatvédelmi tisztviselőnek ismernie kell a Társaság működését, feladatait, illetve munkafolyamatait. Az adatvédelmi tisztviselőnek rendelkeznie kell továbbá az alapvető adatvédelmi és IT folyamatok, valamint az európai uniós, illetve a hazai adatvédelemmel kapcsolatos főbb szabályozók, hatósági és bírósági határozatok, iránymutatások ismeretével.

11. Az adatvédelmi tisztviselő:

   a) tájékoztat és szakmai tanácsot ad az adatkezelő vagy az adatfeldolgozó részére a GDPR, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezések szerinti kötelezettségeikkel kapcsolatban,
   b) ellenőrzi az GDPR-nak, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezéseknek való megfelelést, továbbá az adatkezelő vagy az adatfeldolgozó személyes adatok védelmével kapcsolatos belső szabályainak való megfelelést, ideértve a feladatkörök kijelölését, az adatkezelési műveletekben 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 és közreműködik abban a személyes adatot is kezelő új informatikai rendszer belső fejlesztéssel történő bevezetése, valamint új folyamatok vezetése során,
   d) az adatvédelmi incidens kezeléssel kapcsolatban ellátja a Szabályzat szerinti feladatokat,
   e) felülvizsgálja az adatvédelmi szabályzatot, illetve az informatikai biztonsági szabályzatot, valamint közreműködik azok hatályosításában,
   f) közreműködik, illetve segítséget nyújt az adatkezeléssel összefüggő döntések meghozatalában, valamint az érintettek jogainak biztosításában.

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

13. Az adatvédelmi tisztviselő nyilvántartást vezet:
    a) A Társaságnál végzett adatkezelési tevékenységekről (Adatkezelési nyilvántartás).

       A nyilvántartás tartalmazza az adatkezelés szervezeten belüli helyét, az adatokhoz való hozzáférésre jogosult személyek körének meghatározását (elsősorban munkakör szerint), valamint – ha van ilyen – a közös adatkezelőnek, az adatkezelő képviselőjének és az adatvédelmi felelősnek a nevét és elérhetőségét, az adatkezelés céljait, jogalapját, az érintettek kategóriáinak, valamint a személyes adatok kategóriáinak ismertetését, olyan címzettek kategóriáit, akikkel a személyes adatokat közlik vagy közölni fogják, adott esetben a személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információkat (beleértve a megfelelő garanciák leírását), ha lehetséges, a különböző adatkategóriák törlésére előirányzott határidőket, ha lehetséges, az adatvédelmi biztonsági technikai és szervezési intézkedések általános leírását, valamint az alkalmazott adatfeldolgozási technológia megnevezését.

       A nyilvántartás tartalmazza továbbá az adatok forrását, az adatok kezelésének időtartamát, a továbbított adatok fajtáját, címzettjét és a továbbítás jogalapját, az adatfeldolgozó nevét és címét, a tényleges adatkezelés, illetve az adatfeldolgozás helyét és az adatfeldolgozónak az adatkezeléssel összefüggő tevékenységét, az adatkezelés kockázati besorolását, illetve az adatkezelés módszerének meghatározását (manuális, számítógépes, vegyes).

       A nyilvántartást írásban vagy elektronikus formában kell megőrizni, és folyamatosan naprakészen tartani.

    b) A Társaságnál észlelt adatvédelmi incidensekről.

       A nyilvántartás az adatvédelmi incidenssel kapcsolatos intézkedések ellenőrzése, valamint az érintett tájékoztatása céljából tartalmazza az érintett személyes adatok körét, az adatvédelmi incidenssel érintettek körét és számát, az adatvédelmi incidens időpontját, körülményeit, hatásait és az elhárítására megtett intézkedéseket, valamint az adatkezelést előíró jogszabályban meghatározott egyéb adatokat a Szabályzat 1. számú mellékletében meghatározottak szerint.

    c) A Társaságnál végzett adattovábbításról.

       Az adattovábbítási nyilvántartás az adattovábbítás jogszerűségének ellenőrzése, valamint az érintett tájékoztatása céljából tartalmazza a kezelt személyes adatok továbbításának időpontját, az adattovábbítás jogalapját és címzettjét, a továbbított személyes adatok körének meghatározását, valamint az adatkezelést előíró jogszabályban meghatározott egyéb adatokat a Szabályzat 2. mellékletében meghatározottak szerint.

14. Az adatvédelmi tisztviselő köteles a felsővezetők által kijelölt adatvédelmi kapcsolattartók részére tájékoztatást, illetve képzést tartani az adatvédelemmel és az információszabadsággal összefüggő hatályos jogszabályi előírásokról, a felügyeleti hatóság joggyakorlatáról.

6. A Társaság felsővezetőinek feladatai

15. A Társaság felsővezetői az irányításuk alatt álló munkavállalók tekintetében:
    a) betartják és betartatják az adat- és titokvédelmi, valamint a biztonsági és információbiztonsági előírásokat,

b) gondoskodnak arról, hogy az irányításuk alá tartozók felelősségi körébe tartozó nyilvántartási rendszerek naprakészek, megbízhatóak legyenek,

c) gondoskodnak arról, hogy az irányításuk alatt álló személyek az adatkezelés meghatározott feltételeinek megfelelően járjanak el [GDPR 32. cikk (4) bek.],

d) az adatvédelmi tisztviselő előterjesztésére – a Társaság döntéselőkészítésre vonatkozó szabályainak megfelelően – döntenek a jelen utasításban, illetve az adatkezeléssel járó folyamatot szabályozó egyéb belső szabályzatokban a feladat- és hatáskörükbe utalt kérdésekben.

16. A Társaság felsővezetői az irányításuk alá tartozók tevékenységi körén belül:

a) előkészítik az adatkezeléssel kapcsolatos, az adatkezelőt terhelő döntéseket, illetve abban közreműködik,

b) gondoskodnak az adatkezeléshez kapcsolódó adminisztratív teendők ellátásáról (az adatkezeléssel összefüggő döntések dokumentálása, érdekmérlegelési teszt elvégzése, hatásvizsgálat lefolytatása, az adatkezeléssel összefüggő szerződések előkészítése, az adatkezelések nyilvántartásának naprakészen tartása stb.), illetve abban közreműködnek,

c) együttműködnek egymással, a közvetlen vezetőkkel, valamint az adatvédelmi tisztviselővel,

d) közreműködnek az érintettek jogai gyakorlásának biztosításában,

e) közreműködnek az adatvédelmi incidensek következményeinek elhárításában,

f) közreműködnek az adatkezelési nyilvántartás elkészítésében,

g) közreműködnek a Társaság kezelésében lévő adatok biztonsági osztályba sorolásában,

h) ellátják a Szabályzat szerint hatáskörükbe utalt, valamint adatvédelmi jellegű eseti feladatokat,

i) az általuk irányított területen adatvédelmi kapcsolattartó kijelölésére jogosultak.

17. A Társaság felsővezetői az adatbiztonsági intézkedéseket érintően:

a) információk szolgáltatásával közreműködnek az adatkezelés biztonságát fenyegető kockázatok felmérésében és meghatározásában,

b) az informatikai feladatok ellátásáért felelős munkatárssal együttműködve közreműködnek azon információbiztonságot érintő feladatok végrehajtásában, amelyek az adatbiztonsági követelmények megvalósulásához szükségesek,

c) figyelemmel kísérik az adatbiztonsági előírások érvényre juttatását az irányításuk alá tartozó területen, felhívják az irányításuk alatt álló munkavállalók figyelmét a szabályok betartására, jelzik a szabályok megsértését a munkáltatói jogkörgyakorlónak, közreműködik az irányításuk alatt álló munkavállalók adatvédelmi tudatosságának növelésében.

7. Az adatvédelmi kapcsolattartók feladatai

18. Az adatvédelmi kapcsolattartó feladatai:

a) kapcsolatot tartanak és együttműködnek a Társaság adatvédelmi tisztviselőjével,

b) az adatvédelmi incidens lehetőségének felmerülése, vagy a már bekövetkezett adatvédelmi incidens esetén az adatvédelmi tisztviselőt haladéktalanul tájékoztatják,

c) az adatvédelmi tisztviselő által kért adatokat szolgáltatják.

8. Az informatikai feladatok ellátásáért felelős

19. A Társaság informatikai hátterét a Nemzeti Közszolgálati egyetem biztosítja. Az informatikai feladatok ellátásáért felelős Nemzeti Közszolgálati Egyetem:

a) ellátja az informatikai biztonsággal kapcsolatos adatvédelmi feladatokat;

b) az informatikai fejlesztéseknél és beszerzéseknél ellátja a beépített és alapértelmezett adatvédelem elvének érvényesüléséhez szükséges informatikai feladatokat,

c) az informatikai üzemeltetés területén ellátja a személyes adatok kezelésével kapcsolatos technikai védelem megvalósítását, ellátja a hatáskörébe tartozó információbiztonsági feladatokat, valamint tárolt és továbbított személyes adatok bizalmasságának védelmét, az incidensfelderítési és -kezelési tevékenység támogatását,

d) gondoskodik a Társaság honlapján vagy más, a kezelésében álló közösségi felületén közzétett adatkezelési tájékoztatók aktualizálásáról, archiválásáról és megőrzéséről.

III. Fejezet
Adatkezelők, adatfeldolgozás és közös adatkezelés

20. A Társaságban mindazon, a jelen szabályzat személyi hatálya alá tartozó személy, aki személyes adat birtokába jut, ilyet munkaköre vagy tisztsége alapján kezel, köteles védeni és őrizni a személyes adatokat, és minden erőfeszítést megtenni annak érdekében, hogy azok megfelelő védelmét biztosítsa.

21. Az adatokat 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.

22. A Társasággal jogviszonyban állók a munkakörükből, velük kötött szerződésből, tisztségükből adódó feladataik teljesítése során kötelesek bizalmasan kezelni minden olyan adatot, információt vagy dokumentumot – függetlenül attól, hogy ahhoz milyen formában és milyen módon jutottak hozzá –, amely előttük a feladataik teljesítése során vagy azzal összefüggésben vált ismertté.

23. A Társasággal jogviszonyban álló adatkezelést vagy adatfeldolgozást végző személyek felelősséggel tartoznak minden olyan kárért, amely adatkezelési, adatvédelmi kötelezettségük megsértéséből származik.

24. Ha az adatkezelést a Társaság nevében más végzi, a Társaság kizárólag olyan adatfeldolgozókat vehet igénybe, akik, vagy amelyek megfelelő garanciákat nyújtanak az adatkezelés követelményeinek való megfelelésért és az érintettek jogainak védelmét biztosító, megfelelő technikai és szervezési intézkedések végrehajtására. Az adatfeldolgozói megállapodás tartalmi követelményeivel kapcsolatos rendelkezéseket és a szerződéskötés eljárásrendjét a VI.4. pont tartalmazza részletesen.

25. Közös adatkezelésnek minősül, ha az adatkezelés céljait és eszközeit a Társaság egy vagy több másik adatkezelővel közösen határozza meg. (GDPR 26. cikk) A közös adatkezelői megállapodás tartalmi követelményeivel kapcsolatos rendelkezéseket és a szerződéskötés eljárásrendjét a VI.5. pont tartalmazza részletesen.

IV. Fejezet
Az adatkezelés bevezetésével, módosításával és megszüntetésével kapcsolatos feladatok

9. Adatkezelés bevezetésével kapcsolatos feladatok

26. Új, személyes adatokra is kiterjedő nyilvántartási kötelezettség bevezetése ügyvezető igazgatói utasítással történik. Az ügyvezető igazgatói utasítás tartalmazza:
    a) az adatkezelésért felelős munkavállalók adatkezeléssel kapcsolatos feladatait, így különösen:
        aa) az adatok felvételének, módosításának, törlésének rendjét,
        ab) adatszolgáltatási kötelezettségek meghatározását az adatok naprakészen tartása érdekében,
        ac) a nyilvántartási rendszerből történő adattovábbítást, az ahhoz való hozzáférés rendjét.
    b) mellékletként:
        ba) a GDPR-nak, az Infotv.-nek és egyéb alkalmazandó jogszabályoknak megfelelő adatkezelési tájékoztatót,
        bb) hozzájáruláson alapuló adatkezelés esetén a hozzájáruló nyilatkozat mintáját.
27. Az adatkezelésért felelős, illetékes felsővezetőt és az adatvédelmi tisztviselőt az új adatkezelés bevezetésére vonatkozó igény megfogalmazásától kezdve be kell vonni az adatkezelés feltételeinek kidolgozása folyamatába. Amennyiben az új adatkezelés bevezetése több felsővezetőt érint, az adatkezelésért felelős valamennyi érintettet be kell vonni az adatkezelés feltételeinek kidolgozási folyamatába.

28. Az adatkezelés bevezetésével, az adatkezelés feltételeinek meghatározásával kapcsolatban a leendő adatkezelésért annak tárgya szerint felelős vezetője:
    a) meghatározza az adatkezelés célját, az adatkezelés jogalapját, a kezelendő adatok körét, az adatkezelés egyéb feltételeit, és írásbeli összefoglalót készít (GDPR 4. cikk 7. és 16. pont),
    b) amennyiben az adatkezelés jogalapja a jogos érdek lehet, elkészíti az érdekmérlegelési teszt dokumentumának tervezetét [GDPR 6. cikk (1) bek. f) pont],
    c) az adatvédelmi tisztviselő véleményének kikérése után javaslatot tesz az ügyvezető igazgatónak adatvédelmi hatásvizsgálat elvégzésére; az ügyvezető igazgató erre vonatkozó pozitív döntése esetén elvégzi a hatásvizsgálatot, elkészíti ennek dokumentumát, és kikéri róla az adatvédelmi felelős véleményét [GDPR 35. cikk (1)-(2) és (9) bek.],
    d) előterjesztést tesz az ügyvezető igazgatónak arról, hogy az adatkezelést közös adatkezelésként indokolt-e ellátni, illetve indokolt-e adatfeldolgozót bevonni,
    e) javaslatot tesz automatizált döntéshozatali módszer, illetve profilalkotási módszer alkalmazására [GDPR 22. cikk (1) bek.],
    f) megszövegezi a hozzájáruló nyilatkozat mintáját [GDPR 7. cikk (2) bek.], illetve a megfelelő szerződéses rendelkezéseket,
    g) megfogalmazza az adatkezelésről szóló tájékoztatást (GDPR 13-14. cikk) és gondoskodik az adatkezelésről szóló tájékoztatás könnyen hozzáférhető módon való közzétételéről [GDPR 12. cikk (1) bek.],
    h) az adatkezelés bevezetéséről való döntést követően gondoskodik az új adatkezelés, illetve a nyilvántartott adatokban bekövetkezett valamennyi változás adatkezelési nyilvántartásban történő rögzítéséről [GDPR 30. cikk (1) bek.],

i) amennyiben ennek szükségessége felmerül, egyedi esetben előterjesztést tesz az ügyvezető igazgatónak az érintett vagy harmadik személy létfontosságú érdeke fennállásáról [GDPR 6. cikk (1) bek. d) pont, 9. cikk (2) bek. d) pont] mint az adatkezelés lehetséges jogalapjáról,

j) amennyiben ennek szükségessége felmerül, egyedi esetben előterjesztést tesz az ügyvezető igazgatónak arról, hogy személyes adatok harmadik országba továbbíthatók-e egyedi ügyekben [GDPR 49. cikk (1) bek.].

29. Amennyiben az adatkezelés feltételei kidolgozásában részt vevő munkavállalók között véleményeltérés van, az adatvédelmi tisztviselő javaslatot tesz a lehetséges megoldásra.

30. Az adatvédelmi tisztviselő véleményét az adatkezelés bevezetéséről való döntést kezdeményező előterjesztésben ismertetni kell. Az adatvédelmi tisztviselő véleményétől való eltérést az előterjesztésben részletesen meg kell indokolni.

10. Az érdekmérlegelési teszt elvégzésének módszertana

31. Amennyiben a Társaság valamely adatkezelésének a Társaság vagy harmadik személy jogos érdeke a jogalapja [GDPR 6. cikk (1) bekezdés f) pont], dokumentált formában érdekmérlegelési tesztet kell elvégezni. Jogos érdek az a törvényes, kellően pontosan megfogalmazott, valós és fennálló, illetve elérhető előny, amelyet az adatkezelő származtat – vagy a harmadik személy származtathat – az adatkezelésből.

32. Az érdekmérlegelési tesztet a tervezett adatkezelésért felelős vezető végzi el az adatvédelmi tisztviselő közreműködése mellett. Az érdekmérlegelési tesztet írásban kell elvégezni. A jogos érdeken alapuló adatkezelés kizárólag az érdekmérlegelési teszt elvégzését követően kezdhető meg.

33. Az érdekmérlegelési teszt részei:

a) a tervezett adatkezelés leírása és az annak keretében kezelni tervezett személyes adatok meghatározása,

b) az adatkezelő vagy azon harmadik fél jogos érdekének azonosítása, akinek az adatkezelés érdekében áll,

c) az érintett érdekeinek, jogainak azonosítása,

d) a Társaság (vagy harmadik fél) és az érintettek érdekeinek összevetése,

e) a kockázatot megszüntető vagy mérséklő intézkedési terv meghatározása,

f) az érdekmérlegelési teszt eredménye, az érdekmérlegelés végkövetkeztetéseinek leírása.

11. Adatkezelés megszüntetésével kapcsolatos feladatok

34. Amennyiben a kezelt adatokra a továbbiakban már nincs szükség, vagy az adatok kezelését meg kell szüntetni, az adatkezelés tárgya szerint illetékes vezető javaslatot tesz az ügyvezető felé az adatkezelés egészének vagy egyes adatfajták nyilvántartásának megszüntetésére, vagy a nyilvántartási rendszer egészének vagy egyes adatfajták, illetve adatok törlésére.

12. Az adatfeldolgozó igénybevételének feltételei, az adatfeldolgozói megállapodás

35. Az adatfeldolgozó igénybevételének szükségességét az adatkezelés bevezetéséről való döntés előkészítése részeként kell megvizsgálni. Ezt a szabályt kell alkalmazni akkor

is, ha az adatfeldolgozó igénybevételéről a folyamatban lévő adatkezelés során születik döntés. A döntés meghozatalára az adatvédelmi tisztviselő állásfoglalásának ismeretében az ügyvezető igazgató jogosult. Amennyiben döntés születik az adatfeldolgozó igénybevételéről, az adatkezelés tárgya szerint illetékes vezető előkészíti az adatfeldolgozóval kötendő szerződés tervezetét.

36. Az adatfeldolgozó által végzett adatkezelést olyan – az adatkezelés tárgyát, időtartamát, jellegét és célját, a személyes adatok típusát, az érintettek kategóriáit, valamint az adatkezelő kötelezettségeit és jogait meghatározó – szerződésnek vagy más jogi aktusnak kell szabályoznia, amely köti az adatfeldolgozót a Társasággal szemben. A szerződés kizárólag írásban köthető meg, és abban a GDPR 28. cikk (3) bekezdésében rögzített tartalmat is rögzíteni szükséges, így különösen előírni, hogy az adatfeldolgozó:

a) a személyes adatokat kizárólag az adatkezelő írásbeli utasításai alapján kezeli, – beleértve a személyes adatoknak valamely harmadik ország vagy nemzetközi szervezet számára való továbbítását is –, kivéve akkor, ha az adatkezelést az adatfeldolgozóra alkalmazandó uniós vagy tagállami jog írja elő; ebben az esetben erről a jogi előírásról az adatfeldolgozó az adatkezelőt az adatkezelést megelőzően értesíti, kivéve, ha az adatkezelő értesítését az adott jogszabály fontos közérdekből tiltja,

b) biztosítja azt, hogy a személyes adatok kezelésére feljogosított személyek titoktartási kötelezettséget vállalnak vagy jogszabályon alapuló megfelelő titoktartási kötelezettség alatt álljanak,

c) meghozza az adatkezelés biztonsága érdekében szükséges, a GDPR 32. cikkében előírt intézkedéseket,

d) a további adatfeldolgozó igénybevételére vonatkozóan tiszteletben tartja a GDPR 28. cikk (2) és (4) bekezdésben említett feltételeket,

e) az adatkezelés jellegének figyelembevételével megfelelő technikai és szervezési intézkedésekkel a lehetséges mértékben segíti az adatkezelőt abban, hogy teljesíteni tudja kötelezettségét az érintett GDPR III. fejezetében foglalt jogainak gyakorlásához kapcsolódó kérelmek megválaszolása tekintetében,

f) segíti az adatkezelőt a GDPR 32–36. cikk szerinti kötelezettségeinek – így elsősorban az adatvédelmi incidens bejelentése, az adatvédelmi hatásvizsgálat lefolytatása és az előzetes konzultáció - teljesítésében, figyelembe véve az adatkezelés jellegét és az adatfeldolgozó rendelkezésére álló információkat,

g) az adatkezelési szolgáltatás nyújtásának befejezését követően az adatkezelő döntése alapján minden személyes adatot töröl vagy visszajuttat az adatkezelőnek, és törli a meglévő másolatokat, kivéve, ha az uniós vagy a tagállami jog az személyes adatok tárolását írja elő,

h) az adatkezelő rendelkezésére bocsát minden olyan információt, amely a fenti kötelezettségek teljesítésének igazolásához szükséges, továbbá amely lehetővé teszi és elősegíti az adatkezelő által vagy az általa megbízott más ellenőr által végzett auditokat, beleértve a helyszíni vizsgálatokat is. Az adatfeldolgozó köteles haladéktalanul tájékoztatni az adatkezelőt, ha úgy véli, hogy annak valamely utasítása sérti a GDPR vagy a tagállami vagy uniós adatvédelmi rendelkezéseket,

i) köteles közreműködni az érintettől származó kérelmek, panaszok megválaszolásában, az erről szóló eljárásrendet a szerződésben rögzíteni szükséges,

j) rögzíteni szükséges az adatfeldolgozó kötelezettségeit az adatvédelmi incidens észlelése esetén, így különösen

ja) az adatvédelmi incidens tudomására jutása esetén a Társaságot haladéktalanul értesíteni köteles,

jb) köteles együttműködni a Társasággal az adatvédelmi incidens okának feltárásában és következményeinek felszámolásában,

jc) köteles együttműködni az adatvédelmi incidens bejelentésének teljesítésében,

k) rögzíteni szükséges az adatfeldolgozó kötelezettségét az adatvédelmi hatásvizsgálat elvégzésében, illetve a hatásvizsgálatban azonosított kockázatok alakulásának figyelemmel kísérésében, az adatkezeléssel járó kockázatok változásának jelzésében, illetve az adatvédelmi hatásvizsgálatok utóellenőrzésében.

37. Az adatfeldolgozással nem bízható meg olyan szervezet, amely a feldolgozandó személyes adatokat felhasználó üzleti tevékenységben érdekelt.

38. Az adatbiztonsági intézkedések megfelelőségének megítélése az informatikai feladatok ellátásáért felelős munkavállaló hatáskörébe tartozik, beleértve azt is, hogy az adatfeldolgozó által egy magatartási kódexhez vagy tanúsítási mechanizmushoz való csatlakozás elegendő garanciát jelent-e az adatbiztonsági szabályok megfelelőségére.

39. Az adatfeldolgozói szerződés megkötését követően – az adatkezelések nyilvántartására vonatkozó szabályok szerint – az adatfeldolgozó adatait (név és cím, kapcsolattartó neve és elérhetősége) rögzíteni kell az adatkezelési nyilvántartásban.

40. Az adatkezelő és az adatfeldolgozó intézkedéseket hoz annak biztosítására, hogy az adatkezelő vagy az adatfeldolgozó irányítása alatt eljáró, a személyes adatokhoz hozzáféréssel rendelkező természetes személyek kizárólag az adatkezelő utasításának megfelelően kezelhessék az említett adatokat, kivéve, ha az ettől való eltérésre uniós vagy tagállami jog kötelezi őket.

13. A közös adatkezelés feltételei, a közös adatkezelői megállapodás

41. A közös adatkezelés szükségességét az adatvédelmi tisztviselő az adatkezelés bevezetéséről való döntés előkészítése részeként vizsgálja meg. A döntés meghozatalára az adatvédelmi tisztviselő álláspontjának ismeretében az ügyvezető igazgató jogosult.

42. Amennyiben döntés születik a közös adatkezelés bevezetéséről, az adatkezelés tárgya szerint illetékes vezető előkészíti a közös adatkezelésről szóló megállapodás tervezetét és azt felterjeszti a szerződés megkötésére jogosult személynek.

43. A közös adatkezelésről szóló megállapodásban meg kell határozni különösen

a) az adatkezelés célját, a kezelendő adatok körét, az adatkezelés időtartamát, az alkalmazandó adatbiztonsági intézkedéseket, az adatkezelés egyéb feltételeit,

b) azt, hogy a közös adatkezelésben érintett egyes adatkezelők

ba) mely adatkezelési műveleteket (pl. hozzájáruló nyilatkozatok felvétele, adatok tárolása, adatok felhasználása stb.) végzik,

bb) az érintett tájékoztatását hogyan végzik (pl. melyik adatkezelő készíti el az adatkezelési tájékoztatót és bocsátja az érintettek rendelkezésére stb.),

bc) az érintett jogainak gyakorlását hogyan biztosítják (pl. egyesített vagy elkülönített ügyfélszolgálat stb.),

bd) az esetleges jogellenes adatkezelés következményeit milyen arányban viselik;

be) az adatvédelmi incidens észlelése esetén követendő eljárást, különösen azt, hogy

bea) az adatvédelmi incidens tudomásra jutása esetén a másik adatkezelő kapcsolattartóját haladéktalanul kötelesek értesíteni az adatvédelmi rendellenességről vagy incidensről,

beb) egymással kötelesek együttműködni az adatvédelmi rendellenesség vagy incidens okának kiderítésében és következményeinek felszámolásában,

bec) az egyes adatkezelőket mely adatvédelmi incidensek tekintetében terheli a bejelentési kötelezettség;

c) azt, hogy kijelölnek-e kapcsolattartót az érintettek számára, és ha igen, a kapcsolattartó személyét és elérhetőségét naprakészen kell tartani,

d) a megállapodásról az érintett rendelkezésére bocsátandó összefoglalót, amelynek – a GDPR 13-14. cikkeiben írtakon túl – tartalmaznia kell az adatkezelők által végzett adatkezelési műveleteket, és azt, hogy az érintett hogyan gyakorolhatja jogait a közös adatkezelés tekintetében.

V. Fejezet
Az érintettektől származó kérelmek, panaszok megválaszolásának rendje

14. Az adatvédelmi bejelentések típusai

44. Az érintettől különösen a következő, személyes adatai Társaság általi kezelését érintő beadványok érkezhetnek:

a) bejelentheti a Társaság által nyilvántartott adatok megváltozását,

b) tájékoztatást kérhet személyes adatai tekintetében (milyen személyes adatokat milyen célból, milyen jogalapon, milyen forrásból szerezve meddig kezeli a Társaság, alkalmaz-e automatizált döntéshozatalt és/vagy profilalkotást az adatkezelés során, és a személyes adatokat kinek, milyen jogalapon továbbítja) – hozzáféréshez való jog (GDPR 15. cikk),

c) kérheti pontatlanul nyilvántartott személyes adatai helyesbítését, illetve vitathatja a nyilvántartott személyes adatok pontosságát – helyesbítéshez való jog (GDPR 16. cikk),

d) kérheti nyilvántartott személyes adatai törlését – törléshez való jog (GDPR 17. cikk),

e) kérheti személyes adatai kezelésének korlátozását (a pontatlan adat helyesbítéséig terjedő időre; a jogellenesen kezelt személyes adatok törlése helyett; jogszerűen kezelt, de szükségtelenné vált adatok törlése helyett az érintett kérésére az érintett jogi igényének előterjesztéséhez, érvényesítéséhez vagy védelméhez; jogos érdeken alapuló adatkezelés elleni tiltakozás elbírálásáig) – az adatkezelés korlátozásához való jog (GDPR 18. cikk),

f) kérheti, hogy a rá vonatkozó, általa a Társaság rendelkezésére bocsátott és elektronikus adatbázisban kezelt adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja – adathordozhatósághoz való jog (GDPR 20. cikk),

g) tiltakozhat személyes adatai kezelése ellen, ha az adatkezelés jogalapja az adatkezelő vagy harmadik személy jogos érdeke, illetve közérdekű feladat vagy közfeladat ellátása, beleértve mindkét esetben a profilalkotást is – tiltakozási jog gyakorlása (GDPR 21. cikk),

h) automatizált döntéshozatal alkalmazása esetén az adatkezelő részéről emberi beavatkozást kérhet, közölheti álláspontját (GDPR 22. cikk (3) bek.),

i) kifogást nyújthat be az automatizált döntéshozatal alkalmazásával meghozott döntéssel szemben (GDPR 22. cikk (3) bek.),

j) panaszt nyújthat be a személyes adatok kezelését, illetve a GDPR szerinti jogaik gyakorlását érintően (GDPR 77. cikk, 38. cikk (4) bek.),

k) az elhunyt érintett életében tett meghatalmazottjaként vagy közeli hozzátartozójaként gyakorolni kívánja az érintett egyes jogait (Infotv. 25. §).

15. Az adatvédelmi beadványok elintézése

45. A Társasághoz érkező megkereséseket a GDPR 12. cikkében írt határidők figyelembevételével – kell elintézni, azzal, hogy az érintettnek saját adatairól tájékoztatás csak egyértelmű azonosítása után adható.

VI. Fejezet

Az érintettek jogai, azok érvényesítése

16. Tájékoztatási kötelezettség

46. Az érintettek részére a személyes adatok megszerzésének időpontjában tájékoztatást kell adni a személyes adatok kezelésének tényéről, céljáról, jogalapjáról, a kezelt adatok köréről, az adatkezelés módjáról, időtartamáról vagy az időtartam meghatározásának szempontjairól, az adattovábbítás szabályairól és a felügyeleti hatósághoz címzett panasz benyújtásának jogáról.

47. Amennyiben az érintettek köre pontosan nem határozható meg vagy ez egyébként indokolt, az adatkezelési tájékoztatót a Társaság honlapján kell közzétenni. Egyéb esetben a Társaság olyan módon köteles eleget tenni tájékoztatási kötelezettségének, hogy az az érintettek számára elérhető legyen.
48. Az érintett figyelmét kifejezetten fel kell hívni a tiltakozáshoz való jog érvényesítésének lehetőségére, és az erre vonatkozó tájékoztatást egyértelműen és minden más információtól elkülönítve kell megjeleníteni.

49. A Társaság minden olyan címzettet tájékoztat a személyes adatot érintő valamennyi helyesbítésről, törlésről vagy adatkezelés-korlátozásról, akivel, illetve amellyel a személyes adatot közölte, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel. Az érintettet kérésére a Társaság tájékoztatja ezen címzettek köréről.

17. Az érintett tájékoztatáshoz való joga – hozzáféréshez való jog

50. Az érintett – jogosultsága igazolását követően befogadott – kérelmére a Társaság az adatkezelés tárgya szerint illetékes vezető útján a kérelem beérkezésétől számított 30 napon belül tájékoztatást ad az érintett vonatkozásában folyamatban lévő adatkezelésről.

51. Szükség esetén, figyelembe véve a kérelem összetettségét és a kérelmek számát, ez a határidő maximum további két hónappal meghosszabbítható a tájékoztatást kérő személy előzetes tájékoztatása mellett.

52. Az érintett jogosult arra, hogy a személyes adatokhoz és a következő információkhoz hozzáférést kapjon:

    a) az adatkezelés céljai,

    b) az érintett személyes adatok kategóriái,

    c) azon címzettek vagy címzettek kategóriái, akikkel, illetve amelyekkel a személyes adatokat közölték vagy közölni fogják, ideértve különösen a harmadik országbeli címzetteket, illetve a nemzetközi szervezeteket,

    d) adott esetben a személyes adatok tárolásának tervezett időtartama, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjai,

    e) az érintett azon joga, hogy kérelmezheti az adatkezelőtől a rá vonatkozó személyes adatok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen,

    f) a valamely felügyeleti hatósághoz címzett panasz benyújtásának joga,

    g) ha az adatokat nem az érintettől gyűjtötték, a forrásukra vonatkozó minden elérhető információ,

    h) automatizált döntéshozatal ténye, ideértve a profilalkotást is, valamint legalább ezekben az esetekben az alkalmazott logikára és arra vonatkozó érthető információk, hogy az ilyen adatkezelés milyen jelentőséggel bír, és az érintettre nézve milyen várható következményekkel jár.

53. A személyes adatokhoz való hozzáférést úgy kell biztosítani, hogy ez alatt az érintett más személy adatait ne ismerhesse meg.

54. Az érintett részére készítendő válasz tervezetét az adatkezelés tárgya szerint illetékes vezető köteles összeállítani, szükség esetén az adatvédelmi tisztviselővel együttműködve.

18. A helyesbítéshez való jog

55. Az érintett – jogosultsága igazolását követően befogadott – kérelmére az adatkezelésért felelős vezető – szükség esetén az adatvédelmi tisztviselő előzetes tájékoztatása és jóváhagyása mellett – indokolatlan késedelem nélkül helyesbíti az érintettre 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 is.

19. Az adatkezelés korlátozásához való jog

56. Az érintett – jogosultsága igazolását követően befogadott – kérelmére az adatkezelést végző vezető tájékoztatása alapján korlátozható az adatkezelés, ha az alábbi feltételek valamelyike teljesül:

    a) az érintett vitatja a személyes adatok pontosságát, ez esetben a korlátozás arra az időtartamra vonatkozik, amely lehetővé teszi, hogy a Társaság ellenőrizze a személyes adatok pontosságát,

    b) az adatkezelés jogellenes, és az érintett ellenzi az adatok törlését, és ehelyett kéri azok felhasználásának korlátozását,

    c) a Társaságnak már nincs szüksége a személyes adatokra adatkezelés céljából, de az érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez, vagy

d) az érintett tiltakozási jogával élt az adatkezelés ellen; ez esetben a korlátozás arra az időtartamra vonatkozik, amíg megállapításra nem kerül, hogy az adatkezelő jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben.

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

58. Az érintettet, akinek a kérésére korlátozták az adatkezelést, az adatkezelés korlátozásának feloldásáról előzetesen tájékoztatni kell.

20. Adathordozhatósághoz való jog

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

a) az adatkezelés az érintett hozzájárulásán, vagy az érintettel kötendő vagy megkötött szerződésen alapul és

b) az adatkezelés automatizált módon történik.

60. Az adatok hordozhatóságához való jog gyakorlása során az érintett jogosult arra, hogy – ha ez technikailag megvalósítható – kérje a személyes adatok adatkezelők közötti közvetlen továbbítását. Az adattovábbításhoz való jog érvényesítésére irányuló igény technikai megvalósíthatóságáról, illetve annak feltételeiről az informatikai feladatok ellátásáért felelős munkavállaló dönt.

61. Az adatok hordozhatóságához való jog gyakorlása nem sértheti az adatok törléséhez való jog érvényesítését, és nem érintheti hátrányosan mások jogait és szabadságait, különös tekintettel a joggal való visszaélés szabályaira.

62. Az adatok hordozhatóságához való jog nem érvényesül abban az esetben, ha az adatkezelés közérdekű feladat végrehajtásához szükséges.

21. A törléshez való jog

63. Az érintett – jogosultsága igazolását követően befogadott – kérelmére a Társaság indokolatlan késedelem nélkül törli az érintett személyes adatait vagy azoknak az érintett által meghatározott körét, feltéve, hogy az alábbi esetek valamelyike fennáll:

a) a személyes adatokra már nincs szükség abból a célból, amelyből azokat gyűjtötték vagy más módon kezelték,

b) az érintett visszavonja az adatkezelés alapját képező hozzájárulását, és az adatkezelésnek nincs más jogalapja,

c) az érintett tiltakozik az adatkezelés ellen, és nincs elsőbbséget élvező jogszerű ok az adatkezelésre,

d) a személyes adatokat jogellenesen kezelték,

e) a személyes adatokat a Társaságra alkalmazandó uniós vagy tagállami jogban előírt jogi kötelezettség teljesítéséhez törölni kell,

f) a személyes adatok gyűjtésére az információs társadalommal összefüggő szolgáltatások kínálásával kapcsolatosan került sor.

64. Ha a Társaság nyilvánosságra hozta a személyes adatot, és a fentiek értelmében azt törölni köteles, az elérhető technológia és a megvalósítás költségeinek figyelembevételével megteszi az észszerűen elvárható lépéseket – ideértve az indokolt és szükséges technikai intézkedéseket – a szóban forgó személyes adatokra mutató linkek vagy e személyes adatok másolatának, illetve másodpéldányának törlése érdekében.

65. A Társaság a személyes adatok törlését a jogszerű kérelem ellenére sem végezheti el, amennyiben az adatkezelés szükséges:

a) a véleménynyilvánítás szabadságához és a tájékozódáshoz való jog gyakorlása céljából,

b) a személyes adatok kezelését előíró, a Társaságra alkalmazandó uniós vagy tagállami jog szerinti kötelezettség teljesítése céljából,

c) közérdekből végzett feladat végrehajtása céljából,

d) közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból, amennyiben az adattörlés valószínűsíthetően lehetetlenné tenné vagy komolyan veszélyeztetné ezt az adatkezelést,

e) jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez.

22. A tiltakozáshoz való jog

66. Amennyiben a Társaság az érintett adatait azon a jogalapon kezeli, miszerint

a) az adatkezelés közérdekű feladat végrehajtásához szükséges, vagy

b) az adatkezelés a Társaság vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges,

úgy az érintett ezen személyes adatok kezelése ellen tiltakozhat, ideértve az említett rendelkezéseken alapuló profilalkotást is. Ebben az esetben a Társaság a személyes adatokat nem kezelheti tovább, kivéve, ha bizonyítja, hogy az adatkezelést olyan kényszerítő erejű jogos okok indokolják, amelyek elsőbbséget élveznek az érintett érdekeivel, jogaival és szabadságaival szemben, vagy amelyek jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódnak.

67. Ha a személyes adatok kezelése közvetlen üzletszerzés érdekében történik, az érintett jogosult arra, hogy bármikor tiltakozzon a rá vonatkozó személyes adatok e célból történő kezelése ellen, ideértve a profilalkotást is, amennyiben az a közvetlen üzletszerzéshez kapcsolódik. Ha az érintett tiltakozik a személyes adatok közvetlen üzletszerzés érdekében történő kezelése ellen, akkor a személyes adatok a továbbiakban e célból nem kezelhetők.

23. Jogorvoslathoz való jog

68. Adatkezeléssel kapcsolatos jogainak megsértése esetén az érintett megkeresheti a Társaságot. Az adatkezelés tárgya szerint illetékes vezető a panaszt megvizsgálja, és ha azt megalapozottnak találja, intézkedést kezdeményez, ellenkező esetben a panaszt elutasítja.

69. A Társaság a panasz elutasításáról a panaszost a kérelem kézhezvételét követő 30 napon belül írásban tájékoztatja, a kérelem elutasításának ténybeli és jogi indokait is közölve. A panaszost tájékoztatni kell a bírósági jogorvoslat, továbbá a felügyeleti szervhez fordulás lehetőségéről és módjáról.

70. Az érintett bejelentéssel élhet a felügyeleti hatóságnál, valamint lehetősége van személyes adatainak védelme érdekében bírósághoz fordulni, amely az ügyben soron

kívül jár el. A per során a Társaságot terheli annak bizonyítása, hogy a sérelmezett adatkezelés a jogszabályi előírásoknak megfelelően történt.

VII. Fejezet

Az adatkezelés biztonsága

24. Adatkezelési nyilvántartás, kockázatelemzés, adatbiztonság

71. A személyes adatok biztonságának biztosítása érdekében a Társaság felméri és nyilvántartja az általa végzett valamennyi személyes adatkezelési tevékenységet. Az adatkezelési nyilvántartást az adatvédelmi tisztviselő vezeti.

72. Az adatkezelési nyilvántartás célja a Társaság, mint adatkezelő adatkezelési tevékenysége átláthatóságának biztosítása, és ezzel a szükségtelen, párhuzamos adatkezelések elkerülése.

73. Az adatkezelési tevékenységek nyilvántartása alapján a Társaság kockázatelemzést végez annak felmérése érdekében, hogy az egyes adatkezelések pontosan milyen feltételek szerint valósulnak meg, illetve azok során mely kockázati tényezők milyen mértékű sérelmet, milyen lehetséges adatvédelmi incidenst okozhatnak.

74. A kockázatelemzést a ténylegesen megvalósuló adatkezelési tevékenység alapján kell elvégezni. A kockázatelemzés célja olyan biztonsági szabályok, valamint intézkedések meghatározása, amelyek a Társaság működéséhez, tevékenységéhez igazodva hatékonyan biztosítják a személyes adatok megfelelő védelmét.

75. A Társaság az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre annak biztosítása és bizonyítása céljából, hogy a személyes adatok kezelése a személyes adatok kezelésére vonatkozó jogszabályi előírásokkal összhangban történjen. Ilyen intézkedés lehet például:

    a) a személyes adatok álnevesítése és titkosítása,

    b) a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítása, integritása, rendelkezésre állása és ellenálló képessége,

    c) fizikai vagy műszaki incidens esetén az arra való képessége, hogy a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását kellő időben vissza lehessen állítani,

    d) az adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedések hatékonyságának rendszeres tesztelése, felmérése és értékelése.

76. biztonság megfelelő szintjének meghatározásakor kifejezetten figyelembe kell venni az adatkezelésből eredő olyan kockázatokat, amelyek különösen a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítéséből, elvesztéséből, megváltoztatásából, jogosulatlan nyilvánosságra hozatalából vagy az azokhoz való jogosulatlan hozzáférésből erednek.

77. A Társaság megfelelő technikai és szervezési intézkedéseket hajt végre annak biztosítására, hogy alapértelmezés szerint kizárólag olyan személyes adatok kezelésére kerüljön sor, amelyek az adott konkrét adatkezelési cél szempontjából szükségesek.

78. Személyes adatot tartalmazó irat nem hagyható olyan helyen, ahol harmadik személy is hozzáférhet. Az ilyen iratok elzárásáról azokban az irodákban, illetve személyzeti

helyiségekben is gondoskodni kell, ahol az illetékes iratkezelőkön kívül más, harmadik személy is megfordulhat.

79. Az adathordozó képek és dokumentációk elhelyezésének-, fizikai védelmének biztonságáról az ügyvezető igazgató az adatvédelmi tisztviselővel egyetértésben dönt.

80. Személyes adatokat ért sérülés vagy megsemmisülés esetén a rendelkezésre álló egyéb adatforrásokból meg kell kísérelni a lehetséges mértékig a károsodott adatok pótlását. A pótolt adatokon a pótlás tényét fel kell tüntetni.

25. Adatvédelmi hatásvizsgálat és előzetes konzultáció

81. 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.

82. Az adatvédelmi hatásvizsgálat elvégzéséért a tervezett adatkezelésért felelős vezető felelős. A hatásvizsgálat megállapításait írásban kell rögzíteni.

83. Az adatvédelmi hatásvizsgálatot különösen az alábbi esetekben kell elvégezni:

    a) természetes személyekre vonatkozó egyes személyes jellemzők olyan módszeres és kiterjedt értékelése, amely automatizált adatkezelésen – ideértve a profilalkotást is – alapul, és amelyre a természetes személy tekintetében joghatással bíró vagy a természetes személyt hasonlóképpen jelentős mértékben érintő döntések épülnek;

    b) a személyes adatok különleges kategóriái, vagy büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó személyes adatok nagy számban történő kezelése; vagy

    c) nyilvános helyek nagymértékű, módszeres megfigyelése.

84. A hatásvizsgálat kiterjed legalább:

    a) a tervezett adatkezelési műveletek módszeres leírására és az adatkezelés céljainak ismertetésére, beleértve adott esetben az adatkezelő által érvényesíteni kívánt jogos érdeket;

    b) az adatkezelés céljaira figyelemmel az adatkezelési műveletek szükségességi és arányossági vizsgálatára;

    c) az érintett jogait és szabadságait érintő kockázatok vizsgálatára; és

    d) a kockázatok kezelését célzó intézkedések bemutatására, ideértve a személyes adatok védelmét és a GDPR-ral való összhang igazolását szolgáló, az érintettek és más személyek jogait és jogos érdekeit figyelembe vevő garanciákat, biztonsági intézkedéseket és mechanizmusokat.

85. Adatvédelmi hatásvizsgálatot a GDPR 35. cikk (3) bekezdésében, illetve a felügyeleti hatóság által közzétett jegyzékben szereplő adatkezelések, adatkezelési műveletek esetén kell végezni.

86. A hatásvizsgálat módszertanát minden esetben a tervezett adatkezelés figyelembevételével kell megválasztani.

87. A hatásvizsgálat első részében összefoglalóan le kell írni a tervezett adatkezelést, különösen

    a) az adatkezelés jogalapját, célját (az adatkezeléstől várt előnyöket, az adatkezelés szükségességét), terjedelmét (időben és a kezelt adatok volumenében),

    b) az adatkezeléssel érintettek körét, a kezelendő adatok körét, az adatok megőrzésének tervezett idejét,

    c) az esetlegesen bevonni tervezett adatfeldolgozó vagy közös adatkezelés esetében a többi adatkezelő megjelölését,

    d) azon adatkezelők megjelölését, akiknek az adatot továbbítani tervezik, különösen, ha harmadik országba vagy nemzetközi szervezet felé tervezik az adattovábbítást,

    e) az adatkezelésre vonatkozó további előírásokat, követelményeket (jogszabályi követelmények vagy magatartási kódexből, szabványból eredő követelmények),

    f) az adatkezelés folyamatának a leírását.

88. A hatásvizsgálat második részében ki kell fejteni és meg kell indokolni

    a) az adatkezelés szükségességének és arányosságának garanciáit,

    b) az érintett jogait biztosító garanciák érvényesülését.

89. A hatásvizsgálat harmadik részében azonosítani és értékelni kell az adatkezelés potenciális kockázatait, és a kockázatok enyhítésére tervezett, elfogadott intézkedéseket, megoldásokat.

90. A hatásvizsgálat negyedik része tartalmazza a tervezett adatkezelés értékelését:

    a) az első, második, valamint a harmadik részben meghatározott szempontok értékelését a tekintetben, hogy azok egyenként megfelelőek, további intézkedésekkel megfelelőek lehetnek, illetve nem megfelelőek;

    b) a tervezett kiegészítő intézkedések végrehajtásának ütemtervét;

    c) annak egyértelmű rögzítését, hogy a tervezett adatkezelés valószínűsíthetően magas kockázattal jár-e a természetes személyek jogaira nézve, és ennek alapján az adatkezelés megkezdhető-e, illetve szükség van-e az adatvédelmi felügyeleti hatósággal való konzultációra.

91. A Társaság – a kereskedelmi érdekek vagy a közérdek védelmének vagy az adatkezelési műveletek biztonságának sérelme nélkül – kikérheti az érintettek vagy képviselőik véleményét a tervezett adatkezelésről.

92. A Társaság szükség szerint, de legalább az adatkezelési műveletek által jelentett kockázat változása esetén ellenőrzést folytat le annak értékelése céljából, hogy a személyes adatok kezelése a korábban lefolytatott adatvédelmi hatásvizsgálatnak megfelelően történik-e.

93. Ha az adatvédelmi hatásvizsgálat megállapítja, hogy az adatkezelés az adatkezelő által a kockázat mérséklése céljából tett intézkedések hiányában valószínűsíthetően magas kockázattal jár, a személyes adatok kezelését megelőzően előzetes konzultációt kell lefolytatni a felügyeleti hatósággal, amelynek során tájékoztatja:

    a) adott esetben az adatkezelésben részt vevő adatkezelő, közös adatkezelők és adatfeldolgozók feladatköreiről, különösen vállalkozáscsoporton belüli adatkezelés esetén;

    b) a tervezett adatkezelés céljairól és módjairól;

c) az érintettek GDPR értelmében fennálló jogainak és szabadságainak védelmében hozott intézkedésekről és garanciákról;

d) az adatvédelmi hatásvizsgálatról; és

e) a felügyeleti hatóság által kért minden egyéb információról.

94. A hatásvizsgálatot legalább háromévente felül kell vizsgálni, és szükség esetén újra el kell végezni.

26. Adatvédelmi incidens, és kezelése

95. Az adatvédelmi incidensre vonatkozó szabályokat kell alkalmazni a Társaság által kezelt személyes adatokat érintően bekövetkező valamennyi adatvédelmi incidensre, függetlenül attól, hogy a személyes adatok kezelése papír alapon vagy elektronikusan történik. Az információbiztonsági incidens egyben adatvédelmi incidensnek is minősül, amennyiben az személyes adatokat érint. A jelen szabályzat adatvédelmi incidens kezelésére vonatkozó rendelkezéseinek alkalmazása nem mentesít az elektronikus információs rendszereket érintő biztonsági vagy egyéb események kezelésére vonatkozó szabályok betartása alól.

96. Amennyiben a Társaság nevében eljáró adatkezelő személy akár saját, akár más, a Társaság nevében végzett adatkezelése körében adatvédelmi incidens megtörténtét észleli, vagy arról szerez tudomást, azt haladéktalanul jeleznie kell az adatvédelmi felelős számára. Ennek elmulasztása esetén az észlelő személy felelősséggel tartozik. Az adatvédelmi incidens bejelentésére szolgáló űrlapot a szabályzat 3. sz. melléklete tartalmazza.

97. Az adatvédelmi incidenst a Társaság indokolatlan késedelem nélkül, legkésőbb 72 órával azután, hogy az adatvédelmi incidens észlelésre került, bejelenti az adatvédelmi felügyeleti hatóságnak, kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Ha a bejelentés nem történik meg 72 órán belül, a bejelentéshez mellékelni kell a késedelem igazolására szolgáló indokokat is.

98. Az adatvédelmi felügyeleti hatóság felé történő 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) feltüntetni a bejelentő nevét és elérhetőségét;

c) közölni kell az adatvédelmi felelős vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;

d) ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket;

e) 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.

99. Ha és amennyiben nem lehetséges az információkat egyidejűleg közölni, azok további indokolatlan késedelem nélkül később részletekben is közölhetők.

100. Adatvédelmi incidens bekövetkezése esetén a Társaság adatvédelmi tisztviselője megvizsgálja, és a súlyosságának megfelelően kategorizálja a bekövetkezett incidenst és meghatározza az esetleges elhárítás érdekében szükséges további intézkedéseket.

101. A bekövetkezett incidens előzetes vizsgálata során az alábbi szempontokat szükséges figyelembe venni:

a) a bejelentés személyes adatot érint-e,
b) amennyiben a bejelentés személyes adatot érint, megállapítható-e a személyes adatok köre,
c) megállapítható-e az incidensben érintett személyek köre,
d) a hatályos jogszabályok és belső szabályok alapján megállapítható-e, hogy személyes adat jogellenes kezelése vagy feldolgozása történt,
e) az incidens valószínűsíthetően magas kockázattal jár-e az érintettek jogaira és szabadságaira nézve,
f) melyek az adatvédelmi incidensből eredő, valószínűsíthető következmények,
g) a Társaság által alkalmazott technikai és szervezési védelmi intézkedések alkalmasak-e arra, hogy az incidensben érintett személyes adatokhoz való hozzáférésre nem jogosult személyek számára értelmezhetetlenné tegyék az adatokat (pl. álnevesítés útján).

102. Az incidens kockázati besorolása szerint:

a) magas kockázatúnak minősül az az incidens, amely vagyoni vagy nem vagyoni károkat okozhat az érintetteknek, az érintettek elveszítik a személyes adataik feletti rendelkezés jogát, fennáll annak a reális lehetősége, hogy az incidens hátrányos megkülönböztetést, személyazonosság-lopást vagy személyazonossággal való visszaélést eredményezhet, a jó hírnév sérelmével jár, a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülését eredményezheti, az olyan adatsérülés és adatvesztés, amely esetében az adatok helyreállítása nem lehetséges, stb.

b) alacsony kockázatúnak minősül az az incidens, amely az érintettek jogaira és szabadságaira nézve reális kockázatot nem jelent, pl. a Társaság munkavállalói által használt belső rendszerekben bekövetkező adatsérüléssel vagy adatvesztéssel nem járó átmeneti szolgáltatáskiesés, amely rövid idő alatt helyreállítható, vagy a rendszer, adathordozó sérülése, megsemmisülése miatt bekövetkező adatsérülés vagy adatvesztés, amely különösebb nehézség nélkül, rövid időn belül helyreállítható, stb.

103. Az ügyvezető igazgató legkésőbb a bejelentésre rendelkezésre álló 72 órás határidő leteltét megelőzően dönt a GDPR 33. cikkében írt hatósági bejelentés szükségességéről.

104. Az adatvédelmi tisztviselő elektronikusan nyilvántartja az adatvédelmi incidenseket, feltüntetve különösen az alábbiakat:

a) az incidensben érintett személyes adatok körét és számát,
b) az adatvédelmi incidenssel érintettek körét és számát,
c) az adatvédelmi incidens időpontját,
d) az adatvédelmi incidens körülményeit, hatásait,
e) az adatvédelmi incidens elhárítására megtett intézkedéseket,
f) az adatvédelmi incidenssel kapcsolatban adott tájékoztatások adatait.

105. A Társaság az incidens kivizsgálásával kapcsolatos papíralapú és elektronikus dokumentumokat tíz évig köteles megőrizni, illetéktelenek számára hozzá nem férhető, zárt helyen.

106. Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, a Társaság indokolatlan késedelem nélkül tájékoztatja az érintettet az adatvédelmi incidensről. Az érintett részére adott tájékoztatásban világosan és közérthetően ismertetni kell az adatvédelmi incidens jellegét, és közölni kell legalább a következő információkat és intézkedéseket:

a) a kapcsolattartó nevét és elérhetőségeit,
b) az adatvédelmi incidensből eredő, valószínűsíthető következményeket,
c) a Társaság által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

107. Az érintettet nem kell tájékoztatni, amennyiben az incidens nem jár magas kockázattal, és egyidejűleg a következő feltételek bármelyike teljesül:

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

108. Abban az esetben, ha az érintettek elérhetősége nem áll rendelkezésre vagy az érintettek pontosan meg nem határozható körére tekintettel a közvetlen tájékoztatás nem lehetséges, az ügyvezető igazgató döntése alapján a Társaság az érintetteket a Társaság honlapján is értesítheti.

109. Az adatvédelmi incidensre tekintettel meghozott intézkedések végrehajtását követően a Társaság felméri az intézkedések hatékonyságát, szükség esetén az érintett adatkörben újabb kockázatelemzést végez.

27. Belső adatvédelmi ellenőrzési eljárás

110. A belső adatvédelmi ellenőrzési eljárás célja, hogy a Társaság meggyőződjön arról, hogy a Társaság munkavállalói az adatvédelemmel kapcsolatos jogszabályoknak és belső szabályzatoknak megfelelően kezelik-e az adatokat.

111. Az egyes területek vagy adatkezelési folyamatok belső ellenőrzésére az az adatvédelmi tisztviselő, az érintett felsővezető, a belső ellenőr, a megfelelési tanácsadó, illetve a felügyelőbizottság tehet javaslatot. Az ellenőrzést az ügyvezető igazgató jogosult elrendelni.

112. A belső ellenőrzést írásbeli ellenőrzési terv alapján, az abban meghatározott felelős köteles lefolytatni és az ellenőrzés eredményét, a megállapított eltérések orvoslására irányuló intézkedési tervet írásban rögzíteni.

VIII. fejezet

Adattovábbítás szabályai

113. A Társaság szervezeti rendszerén belül a személyes adatok – a feladat elvégzéséhez szükséges mértékben és ideig – olyan személyhez továbbíthatók, amelynek a Társaságnál végzett feladatának ellátásához a személyes adatok megismerése és kezelése szükséges.

114. A Társaságnál különböző célra irányuló adatkezelések csak törvényes céloknak megfelelően, indokolt esetben kapcsolhatók össze.

115. Olyan megkeresés, amely a Társaság által kezelt személyes adat továbbítására irányul, csak jogszabályi előírás alapján, az adattovábbításhoz megfelelő jogalap és

adatkezelési cél fennállása esetén, vagy a fenti feltételek fennállása esetén teljesíthető. Minden más esetben az adattovábbítás teljesítését meg kell tagadni.

116. Harmadik országba irányuló adattovábbítás esetén az adattovábbítást végzőnek külön meg kell győződnie arról, hogy a külföldre történő adattovábbítás GDPR-ban előírt feltételei fennállnak-e. Ennek kapcsán vizsgálandó, hogy az adattovábbítás a GDPR-ban meghatározott valamely jogalapnak megfelelően történik-e, és az adatok megfelelő védelmi szintje az adatokat átvevő adatkezelőnél biztosított-e. Ha az adattovábbítás az Európai Gazdasági Térség valamely tagállamába irányul, úgy a személyes adatok megfelelő szintű védelmét nem kell vizsgálni.

117. Személyes adatok továbbítása során, amennyiben az postai küldeményként történik, biztosítani kell, hogy a küldemény zártan kerüljön feladásra.

118. A Társaság vállalja, hogy a személyes adatokat statisztikai célra kizárólag olyan formában adja át, amely az érintett azonosítására nem alkalmas.

IX. fejezet
Záró rendelkezések

119. Jelen szabályzat a kiadmányozást követő naptól visszavonásig érvényes.

120. Jelen szabályzat érvénybe lépésével valamennyi, azonos tárgykörben kiadott korábbi szabályzat érvénytelen.

121. Jelen szabályzatot a Társaság https://campus21.uni-nke.hu/ elérési útvonalú internetes honlapján nyilvánosan elérhetővé kell tenni, továbbá gondoskodni kell arról, hogy a Társaság valamennyi munkavállalója megismerje, a megismerés tényét dokumentálni kell.

Budapest, 2021. december 14.

NKE Campus XXI. Szolgáltató Nonprofit Kft.
1089 Budapest, Orczy út 1.
Cégjegyzékszám: 01-09-350854
Adószám: 27125900-2-42
Bankszámlaszám: OTP Bank: 11705008-22533704
1.

Novákné Balogh Katalin

dr Mikola (12.14)

1. melléklet – Incidens nyilvántartás sablonja

#	Az adatvédelmi incidens időpontja, helye	Az adatvédelmi incidenssel érintettek köre, száma	Az érintett személyes adatok köre	Az adatvédelmi incidens körülményei, az adatkezelést előíró jogszabályban meghatározott egyéb adatok	Az adatvédelmi incidens hatásai	Az adatvédelmi incidens elhárítására megtett intézkedések	Bejegyzés dátuma, bejegyző neve, aláírása
1.							
2.							
3.							
4.							
5.							
6.							
7.							
8.							
...							

2. melléklet – Adattovábbítási nyilvántartás sablonja

#	Személyes adatok továbbításának időpontja	Az adatszolgáltatást teljesítő beosztása	Az adattovábbítás jogalapja és célja	A továbbított személyes adatok körének meghatározása	Az adattovábbítás címzettje	az adatkezelést előíró jogszabályban meghatározott egyéb adatok, további megjegyzés	Bejegyzés dátuma, bejegyző neve, aláírása
1.							
2.							
3.							
4.							
5.							
6.							
7.							
8.							
...							

3. melléklet – Adatvédelmi incidens bejelentőlap

Adatvédelmi incidens bejelentőlap

Kérjük, hogy a kitöltött dokumentumot a tudomásszerzést követően a Társaság ügyvezetése számára haladéktalanul szíveskedjen eljuttatni!

I. Adatvédelmi incidensről tudomást szerző személy

- neve:
- beosztása:
- munkahelyi elérhetősége:

II. Az adatvédelmi incidens

- jellege:
- feltételezett időpontja, helye:
- által érintett személyek kategóriái és hozzávetőleges száma:
- által érintett személyes adatok köre és hozzávetőleges száma:
- észlelt vagy lehetséges következményei:
- orvoslására tett vagy tervezett intézkedés és az intézkedés elrendelője, valamint végrehajtója (név és beosztás szerint):

III. Az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve: IGEN / NEM

IV. Egyéb észrevétel:

Budapest, 20.... (év) ..... (hó). .....(nap)