# AZ AFT-HUNGARY KORLÁTOLT FELELŐSSÉGŰ TÁRSASÁG

# ADATVÉDELMI ÉS ADATBIZTONSÁGI SZABÁLYZATA

## 2020. november 2.

# TARTALOM

# BEVEZETÉS

Jelen Adatvédelmi és Adatbiztonsági Szabályzat (**Szabályzat**) az **AFT-Hungary Korlátolt Felelősségű Társaság** (székhely: 2651 Rétság, Ipari park 5.; cégjegyzékszám: 12-09-008027; adószám: 23954773-2-12; e-mail: contact@arcw.com a továbbiakban: **Adatkezelő**) által a tevékenységei körében végzett adatkezelések rendjét határozza meg. Az Adatkezelő, a vele munkaviszonyban vagy munkavégzésre irányuló egyéb jogviszonyban álló személyek, illetve az általa megbízott adatfeldolgozók kötelesek a Szabályzatban foglaltakat magukra nézve kötelezőnek elismerni és az Adatkezelő tevékenységei körében végzett adatkezelések vonatkozásában a Szabályzatban foglaltak szerint eljárni.

Az Adatkezelő a Szabályzatot a GDPR, az Infotv., valamint az általa tevékenységei körében végzett adatkezelések tekintetében irányadó egyéb jogszabályok előírásai alapján készítette el.

A Szabályzat 2020.november 2. napjától kezdve visszavonásig hatályos az Adatkezelő által a tevékenységei körében végzett adatkezelések vonatkozásában. A Szabályzat nyomtatott formában hozzáférhető a Adatkezelő székhelyén, valamint elérhető elektronikusan a helyben szokásos módon. Az Adatkezelő gondoskodik arról, hogy a Szabályzatot a vele munkaviszonyban vagy munkavégzésre irányuló egyéb jogviszonyban álló személyek, illetve az általa megbízott adatfeldolgozók megismerjék.

Az Adatkezelő fenntartja magának a jogot, hogy a jelen Szabályzatot bármikor, egyoldalúan megváltoztassa. Amennyiben a Szabályzat módosulna, akkor erről az Adatkezelő értesíti a vele munkaviszonyban vagy munkavégzésre irányuló egyéb jogviszonyban álló személyeket, illetve az általa megbízott adatfeldolgozókat.

Rétság, 2020.11.02.

AFT-Hungary Kft.

# I. ÁLTALÁNOS RENDELKEZÉSEK

## I.1. A Szabályzat célja és hatálya

1. § A Szabályzat célja, hogy meghatározza az Adatkezelő által a tevékenységei körében végzett adatkezelések törvényes rendjét, valamint biztosítsa az adatvédelem, az információs önrendelkezési jog és az adatbiztonság követelményeinek érvényesülését, megakadályozza a jogosulatlan hozzáférést, az adatok jogosulatlan megváltoztatását és nyilvánosságra hozatalát.

2. § A Szabályzat tárgyi hatálya a személyes adatoknak minden, az Adatkezelő által a tevékenységei körében végzett kezelésére kiterjed.

3. § A Szabályzat személyi hatálya az Adatkezelővel munkaviszonyban, munkavégzésre irányuló egyéb jogviszonyban álló személyekre, az Adatkezelővel kötött szerződés alapján eljáró adatfeldolgozókra, valamint az Adatkezelő szolgáltatásait igénybe vevő személyekre terjed ki.

## I.2. Fogalmak

4. § A Szabályzat alkalmazásában:

a) *érintett/adatalany*: a személyes adat alapján azonosított vagy – közvetve vagy közvetlenül – azonosítható természetes személy;[1]
b) *személyes adat*: érintettre vonatkozó bármely információ;[2]
c) *különleges adat*: a személyes adatok különleges kategóriáiba tartozó minden adat, azaz a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a genetikai adatok, a természetes személyek egyedi azonosítását célzó biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok;[3]
d) *adatkezelés*: a személyes adatokon 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;[4]
e) *adattovábbítás*: a személyes adat egy meghatározott harmadik személy számára történő hozzáférhetővé tétele;
f) *nyilvánosságra hozatal*: a személyes adat bárki számára történő hozzáférhetővé tétele;
g) *adattörlés*: a személyes adat felismerhetetlenné tétele oly módon, hogy a helyreállítása többé nem lehetséges;

[1] L. Általános adatvédelmi rendelet (GDPR) 4. cikk 1. pont.
[2] Uo.
[3] GDPR 9. cikk (1) bekezdés és Infotv. 3. § 3. pont.
[4] GDPR 4. cikk 2. pont.

h) *adatkezelő*: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza;[5]
i) *adatfeldolgozó*: az a természetes vagy jogi személy, illetve bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel;[6]
j) *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;[7]
k) *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;[8]
l) *harmadik ország*: minden, az Európai Gazdasági Térségen kívüli ország;
m) *hozzájárulás*: az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez;[9]
n) *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;[10]
o) *titoksértési incidens*: olyan incidens, amelynek eredményeként a személyes adatok jogosulatlan vagy véletlen közlése vagy az ilyen adatokhoz való jogosulatlan vagy véletlen hozzáférés következett be;[11]
p) *sértetlenségi incidens*: olyan incidens, amelynek eredményeként a személyes adatok jogosulatlan vagy véletlen módosítása következett be;[12]
q) *hozzáférhetőségi incidens*: olyan incidens, amelynek eredményeként a személyes adatokhoz való hozzáférhetőség jogosulatlan vagy véletlen elvesztés, vagy jogosulatlan vagy véletlen megsemmisítés miatt következett be;[13]
r) *adatbiztonság*: minden olyan technikai vagy szervezési intézkedés, amelynek célja a kezelt személyes adatok – fizikai, optikai vagy szervezeti – biztonságának biztosítása, így különösen azok az intézkedések, amelyek a személyes adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet szolgálják;[14]

[5] GDPR 4. cikk 7. pont.
[6] GDPR 4. cikk 8. pont.
[7] GDPR 4. cikk 9. pont.
[8] GDPR 4. cikk 8. pont.
[9] GDPR 4. cikk 11. pont.
[10] GDPR 4. cikk 12. pont.
[11] L. a 29. cikk alapján létrehozott Adatvédelmi Munkacsoport iránymutatása az adatvédelmi incidensek (EU) 2016/679 rendelet szerinti bejelentéséről (http://naih.hu/files/wp250rev01_hu.pdf).
[12] Uo.
[13] Uo.
[14] GDPR 5. cikk (1) bekezdés f) pont és 32. cikk.

s) *álnevesítés*: a személyes adatok olyan módon történő kezelése, amelynek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik, feltéve, hogy az ilyen további információt külön tárolják, és technikai és szervezési intézkedések megtételével biztosított, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni;[15]
t) *személyes adat megsemmisítése*: a személyes adat egyáltalán nem, vagy az Adatkezelő számára nem használható formában létezik;[16]
u) *személyes adat elvesztése*: az Adatkezelő már nem rendelkezik a személyes adat felett, nem fér hozzá, vagy az nincsen a birtokában;[17]
v) *személyes adat megváltoztatása*: a személyes adat módosult, sérült, vagy már nem hiánytalan;[18]
w) *személyes adat közlése vagy az ahhoz való hozzáférés*: a személyes adat arra nem jogosult címzett részére történő hozzáférhetővé tétele;[19]
x) *nemvárt esemény*: minden olyan esemény, amely az Adatkezelő kezelésében lévő információk megsemmisítésével, elvesztésével, megváltoztatásával, illetve jogosulatlan közlésével vagy az azokhoz való hozzáféréssel jár, ideértve különösen a t)-w) pontokban foglalt eseteket is;
y) *NAIH*: Nemzeti Adatvédelmi és Információszabadság Hatóság.

# II. AZ ADATKEZELŐ ADATVÉDLEMI RENSZERE

## II.1. Az Adatkezelő megnevezése és elérhetőségei

5. § A Szabályzat hatálya alá tartozó adatkezelések tekintetében az AFT-Hungary Korlátolt Felelősségű Társaság minősül adatkezelőnek.[20]

6. § Az Adatkezelőre vonatkozó adatok:
a) *megnevezés*: AFT-Hungary Korlátolt Felelősségű Társaság
b) *rövidített elnevezés*: AFT-Hungary Kft.
c) *cégjegyzékszám*: 12-09-008027
d) *adószám*: 23954773-2-12
e) *székhely*: 2651 Rétság, Ipari park 5.
f) *postacím*: 2651 Rétság, Ipari park 5.
g) *e-mail*: contact@arcw.com
h) *telefonszám*: +36/ 35 551 000

## II.2. Az adatvédelmi felelős

[15] GDPR 4. cikk 5. pont.
[16] L. a 29. cikk alapján létrehozott Adatvédelmi Munkacsoport iránymutatása az adatvédelmi incidensek (EU) 2016/679 rendelet szerinti bejelentéséről (http://naih.hu/files/wp250rev01_hu.pdf).
[17] Uo.
[18] Uo.
[19] Uo.
[20] L. GDPR 4. cikk 7. pont.

7. § Az Adatkezelő nem köteles adatvédelmi tisztviselőt (DPO) kijelölni.[21] Ugyanakkor, az adatvédelem megfelelő szintje érvényesülésének fenntartása, valamint az adatvédelmi teendők koordinálása érdekében adatvédelmi felelőst jelöl ki.
Az Adatkezelő adatvédelmi felelősét az Adatkezelő vezető tisztségviselője bízza meg.

8. § Az adatvédelmi felelős legalább a következő feladatokat látja el:

a) gondoskodik az Adatkezelő által a tevékenységei körében végzett adatkezelésekkel kapcsolatos adatkezelési tájékoztatók és a Szabályzat naprakészségéről, elérhetőségéről;
b) figyelemmel kíséri az Adatkezelő által a tevékenységei körében végzett adatkezeléseket;
c) együttműködik a Nemzeti Adatvédelmi és Információszabadság Hatósággal (NAIH);
d) az adatkezeléssel összefüggő ügyekben kapcsolattartó pontként szolgál a NAIH felé, valamint adott esetben bármely egyéb kérdésben konzultációt folytat vele;
e) vezeti az adatvédelmi tevékenységek nyilvántartását (belső adatvédelmi nyilvántartás);
vezeti az adatvédelmi incidensek nyilvántartását
f) az adatvédelmi kérdésekkel összefüggésben az contact@arcw.com e-mail címen fogadja az Adatkezelő munkavállalóinak, illetve egyéb érintett megkeresését, konzultációs kérdéseit és azzal érdemben foglalkozik.

9. § Az adatvédelmi felelős a fentieken túlmenően ellátja a Szabályzatban részére meghatározott feladatokat, illetve minden olyan feladatot, amellyel az Adatkezelő megbízza.

# III. AZ ADATKEZELÉS ELVEI

10. § Az Adatkezelő számára kiemelten fontos érték, egyben cél is a személyes adatok védelme. Az Adatkezelő ezért az általa folytatott tevékenységekkel összefüggésben végzett adatkezelések vonatkozásban betartja a releváns adatkezelési elveket.

11. § (1) Az Adatkezelő számára kiemelten fontos érték a tisztességesség követelménye.[22]
(2) Ennek megfelelően az Adatkezelő mindenkor tiszteletben tartja az érintettek emberi méltóságát és magánéletét.
(3) Tilos minden olyan tevékenység, amely az adatalanyok magánéletének szükségtelen megzavarásával jár.
(4) Tilos minden olyan tevékenység, amely az érintettek személyes adatainak rejtett vagy titkos kezelésével jár, vagy az érintettek titkos megfigyelését eredményezi.

12. § (1) Az Adatkezelő mindenkor eleget tesz a jogszerűség követelmények.[23]

[21] L. GDPR 37. cikk (1) bekezdés.
[22] GDPR 5. cikk (1) bekezdés a) pont.

(2) Az Adatkezelő az általa folytatott tevékenységekkel összefüggésben végzett adatkezelések során a mindenkor hatályos adatvédelmi előírások betartásával jár el.
(3) Az Adatkezelő továbbá eleget tesz a személyes adatok kezelésének jogalapjával kapcsolatos követelményeknek.

13. § (1) Az Adatkezelő törekszik arra, hogy az általa folytatott tevékenységekkel összefüggésben végzett adatkezelések átláthatóak legyenek az adatalanyok számára.[24]
(2) Az Adatkezelő e követelményt különösen a tájékoztatáshoz és hozzáféréshez való jog gyakorlásával összefüggésben, valamint az érintettel folytatott minden kommunikáció során érvényesíti.

14. § (1) Az Adatkezelő az általa folytatott tevékenységekkel összefüggésben végzett adatkezelések során mindenkor a célhoz kötöttség követelményére tekintettel jár el.[25]
(2) Az Adatkezelő a személyes adatok kizárólag előre meghatározott, egyértelmű jogszerű cél – jog gyakorlása vagy kötelezettség teljesítése – érdekében kezeli. Az adatkezelésnek mindvégig meg kell felelnie e célnak.
(3) Tilos a személyes adatokat a céllal össze nem egyeztethető módon kezelni.
(4) Tilos a személyes adatokat előre meghatározott, egyértelmű és jogszerű cél hiányában kezelni.

15. § Az Adatkezelő az általa folytatott tevékenységekkel összefüggésben végzett adatkezelések során csak olyan személyes adatot kezel, amely az adatkezelés célja szempontjából megfelelő és releváns, illetve az adatkezelés célja eléréséhez szükséges.[26]

16. § (1) Az Adatkezelő az általa folytatott tevékenységekkel összefüggésben végzett adatkezelések során csak olyan személyes adatot kezel, amely pontos és naprakész.[27]
(2) Az Adatkezelő köteles minden észszerű intézkedést meghozni az adatkezelés céljai szempontjából pontatlan személyes adatok haladéktalan törlése vagy helyesbítése érdekében.

17. § Az Adatkezelő az általa folytatott tevékenységekkel összefüggésben végzett adatkezelések során biztosítja, hogy a kezelt személyes adatok az érintettek azonosítását csak az adatkezelés céljának eléréséhez szükséges ideig teszik lehetővé.[28]

18. § Az Adatkezelő megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítja a személyes adatok megfelelő biztonságát, az adatok

---

[23] Uo.
[24] Uo.
[25] GDPR 5. cikk (1) bekezdés b) pont.
[26] GDPR 5. cikk (1) bekezdés c) pont
[27] GDPR 5. cikk (1) bekezdés d) pont
[28] GDPR 5. cikk (1) bekezdés e) pont.

jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmét is ideértve.[29]

19. § (1) Az Adatkezelő biztosítja az általa folytatott tevékenységekkel összefüggésben végzett adatkezelések megfelelőségének igazolásához szükséges dokumentumok rendelkezésre állását és naprakészségét.[30]
(2) Az Adatkezelő köteles bizonyítani azt, hogy az általa folytatott tevékenységekkel összefüggésben végzett adatkezelések megfelelnek a vonatkozó adatvédelmi előírásoknak.

# IV. AZ ADATKEZELÉS JOGALAPJAI

20. § A személyes adatok kezelése kizárólag akkor és annyiban jogszerű, amennyiben legalább az alábbiak egyike teljesül:

a) az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez;
b) az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél, vagy az a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges;
c) az adatkezelés az Adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges;
d) az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges;
e) az adatkezelés közérdekű vagy az Adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges;
f) az adatkezelés az Adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé, különösen, ha az érintett gyermek;
g) különleges adatok[31] esetében különösen akkor, ha az adatkezelés jelentős közérdek miatt szükséges, uniós jog vagy tagállami jog alapján, amely arányos az elérni kívánt céllal, tiszteletben tartja a személyes adatok védelméhez való jog lényeges tartalmát, és az érintett alapvető jogainak és érdekeinek biztosítására megfelelő és konkrét intézkedéseket ír elő;

21. § Kétség esetén a jogalap alkalmazhatóságáról az adatvédelmi felelős az Adatkezelő ügyvezetőjével egyetértésben dönt.

## IV.1. Az érintett hozzájárulása

22. § Az érintett hozzájárulása akkor tekinthető az adatkezelés érvényes jogalapjának, amennyiben az az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson

[29] GDPR 5. cikk (1) bekezdés f) pont.
[30] GDPR 5. cikk (2) bekezdés.
[31] GDPR 9. cikk

alapuló és egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez.

23. § (1) Az érintett hozzájárulása során biztosítani kell azt, hogy valódi választási lehetőség álljon az érintett rendelkezésére, a beleegyezés „tudatossága" felől nem lehet kétség.
(2) Nem minősül önkéntesnek a hozzájárulás akkor, ha annak következményei aláássák az egyén választási szabadságát.

24. § Az érintett hozzájárulása esetén továbbá:

a) az Adatkezelőnek képesnek kell lennie annak igazolására, hogy az érintett személyes adatainak kezeléséhez hozzájárult;[32]
b) az Adatkezelőnek biztosítania kell azt, hogy az érintett a hozzájárulását bármikor visszavonhassa, és a hozzájárulás visszavonását ugyanolyan egyszerű módon kell lehetővé tennie, mint annak megadását;[33]
c) a hallgatás, az előre bejelölt négyzet vagy a nem cselekvés nem minősül hozzájárulásnak;[34]
d) a hozzájárulás megadása nem tekinthető önkéntesnek, ha az érintett nem rendelkezik valós vagy szabad választási lehetőséggel, és nem áll módjában a hozzájárulás anélküli megtagadása vagy visszavonása, hogy ez kárára válna;[35]
e) nem tekinthető önkéntesnek a beleegyezés, ha nem tesz lehetővé külön-külön hozzájárulást a különböző személyes adatkezelési műveletekhez;[36]
f) nem tekinthető önkéntesnek a hozzájárulás, ha a szerződés teljesítését (például a szolgáltatás nyújtását) olyan adatkezeléshez való hozzájárulásához kötik, amely adatkezelés nem szükséges a szerződés teljesítéséhez;[37]
g) a hozzájárulás nem szolgálhat érvényes jogalapként akkor, ha az érintett és az Adatkezelő között egyértelműen egyenlőtlen viszony áll fenn;[38]
h) ha az Adatkezelő írásbeli nyilatkozaton keresztül szerzi be az érintett hozzájárulását, akkor a nyomtatványon a hozzájárulás iránti kérelmet egyértelműen és világosan el kell választani a szerződés többi részétől, valamint ezen kérelmet érthető és egyszerű nyelvezettel kell az adatkezelőnek megfogalmaznia.[39]

25. § (1) A hozzájárulás beszerzése előtt az Adatkezelő, az Adatkezelővel munkaviszonyban vagy munkavégzésre irányuló egyéb jogviszonyban álló személy, vagy az Adatkezelővel kötött szerződés alapján eljáró adatfeldolgozó köteles megfelelő tájékoztatásban részesíteni az érintettet. A tájékoztatás megtörténhet az erre rendszeresített hozzájáruló nyilatkozaton feltüntetett információk megismerése

[32] GDPR 7. cikk (1) bekezdés.
[33] GDPR 7. cikk (3) bekezdés.
[34] GDPR (32) preambulumbekezdés
[35] GDPR (42) preambulumbekezdés.
[36] GDPR (43) preambulumbekezdés.
[37] GDPR (43) preambulumbekezdés és 7. cikk (4) bekezdés.
[38] GDPR (43) preambulumbekezdés.
[39] GDPR 7. cikk (2) bekezdés.

révén. Ebben az esetben elegendő időt kell biztosítani az érintett számára arra, hogy megismerje a tájékoztatást és megértse a benne foglaltakat.
(2) Az érintett jogosult további információkat és felvilágosítást kérni az Adatkezelőtől, az Adatkezelővel munkaviszonyban vagy munkavégzésre irányuló egyéb jogviszonyban álló személytől, vagy az Adatkezelővel kötött szerződés alapaján eljáró adatfeldolgozótól. A tájékoztatás vagy felvilágosítás megadása kötelező.

### IV.2. A szerződéses jogalap

26. § Az Adatkezelő és az érintett közötti szerződés létrehozása és teljesítése jogalapot teremthet a személyes adatok kezelésére.[40]

27. § A szerződés megkötése érdekében akkor kezelhetők személyes adatok, ha:
a) a szerződést az Adatkezelő köti az érintettel;
b) az érintett bocsátja az adatokat az Adatkezelő rendelkezésére;
c) az adatok az Adatkezelő és az érintett közötti szerződés megkötéséhez szükségesek.

28. § A szerződés teljesítése érdekében akkor kezelhetők a személyes adatok, ha:
a) létezik a szerződés, amelynél az érintett az egyik fél;
b) a szerződés érvényes;
c) az adatkezelés ténylegesen szükséges a szerződés általános célkitűzésének eléréséhez.

29. § A szükségesség követelménye a szerződéses jogalap alkalmazásának előfeltétele.[41] E követelmény nem redukálható pusztán a szerződéses kitételek vizsgálatára, hanem feltételezi az adatvédelmi garanciák, illetve a GDPR-ban meghatározott alapelvek mérlegelését is, különös tekintettel a tisztességes eljárás, a célhoz kötöttség és az adattakarékosság elvére. Amennyiben tehát az adatkezelés hasznos, de nem objektíve szükséges a szerződés teljesítéséhez, nem alkalmazható a szerződéses jogalap.

### IV.3. A jogos érdek

30. § Az Adatkezelő – ideértve azt az adatkezelőt is, akivel a személyes adatokat közölhetik – vagy valamely harmadik fél jogos érdeke jogalapot teremthet az adatkezelésre, feltéve, hogy az érintett érdekei, alapvető jogai és szabadságai nem élveznek elsőbbséget, figyelembe véve az adatkezelővel való kapcsolata alapján az érintett észszerű elvárásait.[42]

31. § Az Adatkezelő – ideértve azt az adatkezelőt is, akivel a személyes adatokat közölhetik – vagy valamely harmadik fél jogos érdeke nem teremthet jogalapot az

[40] GDPR 6. cikk (1) bekezdés b) pont.
[41] L. az Európai Adatvédelmi Testület 2/2019. számú iránymutatása a személyes adatok GDPR 6. cikk (1) bekezdés b) pontja szerinti kezeléséről az adatalanyoknak nyújtott online szolgáltatások keretében (https://edpb.europa.eu/sites/edpb/files/consultation/edpb_draft_guidelines-art_6-1-b-final_public_consultation_version_en.pdf)
[42] GDPR 6. cikk (1) bekezdés f) pont.

adatkezelésre, amennyiben az adatkezelést az Adatkezelő – ideértve azt az adatkezelőt is, akivel a személyes adatokat közölhetik – vagy valamely harmadik fél közfeladat ellátásával összefüggésben végzi.[43]

32. § (1) A jogos érdek fennállásának megállapításához megvizsgálandó többek között az, hogy az érintett a személyes adatok gyűjtésének időpontjában és azzal összefüggésben számíthat-e észszerűen arra, hogy adatkezelésre az adott célból kerülhet sor.[44]
(2) Az érintett érdekei és alapvető jogai elsőbbséget élvezhetnek az Adatkezelő érdekével szemben, ha a személyes adatokat olyan körülmények között kezelik, amelyek közepette az érintettek nem számítanak további adatkezelésre.

33. § A jogos érdek jogalapként történő kezeléséhez az szükséges, hogy az Adatkezelő elvégezze az ún. érdekmérlegelési tesztet. Az érdekmérlegelési teszt a következő lépésekből áll:

a) meg kell határozni az adatkezelő jogszerű, egyértelmű és valós érdekét;
b) azonosítani kell az érintett alapvető jogait és szabadságait, valamint figyelembe kell venni az érintett elvárásait;
c) elemezni kell az adatkezelés szükségességét és arányosságát;
d) további olyan intézkedéseket kell meghatározni, amelyek az adatkezelés hatásait csökkentik.[45]

34. § A munkavállók ellenőrzésével kapcsolatos adatkezelésekre vonatkozó érdekmérlegelési tesztet a Szabályzat 3. számú melléklete tartalmazza.

### IV.4. Kötelező adatkezelés

35. § Az Adatkezelőre vonatkozó jogi kötelezettség teljesítése is jelentheti az adatkezelés jogalapját.[46]

36. § A jogi kötelezettség teljesítése abban az esetben szolgáltathat jogalapot a személyes adatok kezeléséhez, amennyiben:

a) azt uniós vagy hazai jogszabály rendeli el;
b) a rendelkezés közvetlenül az Adatkezelőre vonatkozó kötelezettséget tartalmaz;
c) a rendelkezés közérdekű célt szolgál;
d) a rendelkezés arányos az elérni kívánt jogszerű céllal.[47]

# V. AZ ÉRINTETTI JOGOK

### V.1. Előzetes tájékoztatási kötelezettség

[43] GDPR 6. cikk (1) bekezdés
[44] GDPR (47) preambulumbekezdés.
[45] L. a 29. cikk alapján létrehozott Adatvédelmi Munkacsoport 06/2014. számú vélemény az adatkezelő 95/46/EK irányelv 7. cikke szerinti jogszerű érdekeinek fogalmáról (https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_hu.pdf).
[46] GDPR 6. cikk (1) bekezdés c) pont.
[47] GDPR 6. cikk (3) bekezdés.

37. § (1) 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, a felügyeleti hatósághoz címzett panasz benyújtásának jogáról.[48]
(2) Az (1) bekezdés szerinti tájékoztatás mellett 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.
(3) Az (1)-(2) bekezdés szerinti tájékoztatást:
a) az álláspályázatot benyújtók számára az álláspályázati felhívás közzétételét szolgáló oldalon a vonatkozó adatkezelési tájékoztató szerinti tartalommal kell nyújtani;
b) az Adatkezelővel munkaviszonyt, munkavégzésre irányuló egyéb jogviszonyt létesítő személyek részére a jogviszony létrejöttekor a vonatkozó adatkezelési tájékoztatók szerinti tartalommal kell nyújtani;
c) az Adatkezelő által szervezett képzéseken, vizsgákon résztvevők számára a vonatkozó adatkezelési tájékoztató szerinti tartalommal kell nyújtani;
(4) A (3) bekezdés a) és c) pontja szerinti tájékoztatásokat az Adatkezelő honlapján, tömör, átlátható, és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva kell elhelyezni.
(5) A (3) bekezdés b) pont szerinti tájékoztatást a jogviszony létesítésekor elektronikus formában kell megadni, melynek megtörténtét az érintett papír alapú nyilatkozatával írásban igazolni köteles.

### V.2. A hozzáféréshez való jog

38. § (1) Az érintett kérelmére az adatkezelést végző illetékes ügyintéző vagy az adatvédelmi felelős a kérelem beérkezésétől számított 30 napon belül tájékoztatást ad az érintett vonatkozásában folyamatban lévő adatkezelésről.
(2) 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.[49]

[48] Vö. GDPR 13-14. cikk.
[49] GDPR 15. cikk.

(3) A személyes adatokhoz való hozzáférést úgy kell biztosítani, hogy ez alatt az érintett más személy személyes adatait lehetőleg ne ismerhesse meg. Ez alól kivételt képezhetnek azok a személyes adatok, amelyek mind az érintettre, mind pedig egy másik személyre vonatkoznak.[50]
(4) Az érintett hozzáféréshez való jogát az Adatkezelő az elérni kívánt céllal arányosan korlátozhatja vagy megtagadhatja, ha ezen intézkedés elengedhetetlenül szükséges:

a) az Adatkezelő részvételével végzett vizsgálatok vagy eljárások – így különösen büntetőeljárás – hatékony és eredményes lefolytatásának;
b) bűncselekmények hatékony és eredményes megelőzésének és felderítésének;
c) bűncselekmények elkövetőivel szemben alkalmazott büntetések és intézkedések végrehajtásának;
d) a közbiztonság hatékony és eredményes védelmének;
e) az állam külső és belső biztonsága hatékony és eredményes védelmének, így különösen honvédelem és nemzetbiztonság; vagy
f) harmadik személyek alapvető jogai védelmének biztosításához.

(5) Amennyiben az Adatkezelő a (4) bekezdésben foglaltak szerint megtagadja vagy korlátozza az érintett hozzáférési jogát, erről haladéktalanul írásban tájékoztatja érintettet – amennyiben a korlátozás, megtagadás célját ez nem veszélyezteti – az intézkedés indokát is megjelölve. A tájékoztatásban az Adatkezelő külön felhívja érintett figyelmét, hogy hozzáférési jogát a felügyeleti hatóság közreműködésével is gyakorolhatja.

39. § Az Adatkezelő a Szabályzat 1. számú függelékében foglalt nyilvántartásban tartja nyilván a hozzáféréshez való jog gyakorlásával kapcsolatos intézkedéseit. Amennyiben az Adatkezelő 38. § (4) bekezdésben foglalt intézkedést alkalmaz, az intézkedés jogi és ténybeli indokait is megjelöli.

### V.3. A helyesbítéshez való jog gyakorlása

40. § Az érintett kérelmére az adatkezelést végző illetékes ügyintéző vagy az adatvédelmi felelős indokolatlan késedelem nélkül helyesbíti az érintettre vonatkozó pontatlan személyes adatokat.[51] Figyelembe véve az adatkezelés célját, az érintett jogosult arra, hogy kérje a hiányos személyes adatok – egyebek mellett kiegészítő nyilatkozat útján történő – kiegészítését is.

### V.4. A törléshez való jog

41. § (1) Az érintett kérelmére az adatkezelést végző illetékes ügyintéző vagy az adatvédelmi felelős 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;

[50] GDPR 15. cikk (3)-(4) bekezdés.
[51] GDPR 16. cikk.

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 az Adatkezelő által alkalmazandó uniós vagy tagállami jogban előírt jogi kötelezettség teljesítéséhez törölni kell.[52]

(2) Ha az Adatkezelő nyilvánosságra hozta a személyes adatot, és az (1) bekezdés értelmében azt törölni köteles, az elérhető technológia és a megvalósítás költségeinek figyelembevételével megteszi az észszerűen elvárható lépéseket – ideértve technikai intézkedéseket – a szóban forgó személyes adatokra mutató linkek vagy e személyes adatok másolatának, illetve másodpéldányának törlése érdekében.[53]

42. § Az Adatkezelő 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, az adatkezelő által 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.[54]

### V.5. Az adatkezelés korlátozásához való jog

43. § (1) Az érintett kérelmére az adatkezelést végző illetékes ügyintéző korlátozza az adatkezelést, 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 az adatkezelést végző illetékes ügyintéző vagy az adatvédelmi felelős ellenőrizze a személyes adatok pontosságát;
b) az adatkezelés jogellenes, és az érintett ellenzi az adatok törlését, és ehelyett kéri azok felhasználásának korlátozását;
c) az Adatkezelőnek 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.[55]

(2) Ha az adatkezelés az (1) bekezdés alapján korlátozás alá esik, az ilyen személyes adatokat a tárolás kivételével csak az érintett hozzájárulásával, vagy jogi igények

[52] GDPR 17. cikk (1) bekezdés.
[53] GDPR 17. cikk (2) bekezdés.
[54] GDPR 17. cikk (3) bekezdés.
[55] GDPR 18. cikk (1) bekezdés.

előterjesztéséhez, érvényesítéséhez vagy védelméhez, vagy más természetes vagy jogi személy jogainak védelme érdekében, vagy az Unió, illetve valamely tagállam fontos közérdekéből lehet kezelni.
(3) Az adatkezelést végző illetékes ügyintéző vagy az adatvédelmi felelős az érintettet, akinek a kérésére az (1) bekezdés alapján korlátozták az adatkezelést, az adatkezelés korlátozásának feloldásáról előzetesen tájékoztatja.[56]

### V.6. A címzettek tájékoztatásának kötelezettsége

44. § Az Adatkezelő 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.

### V.7. Az adathordozhatósághoz való jog

45. § (1) Az érintett kérelmére az adatkezelést végző illetékes ügyintéző biztosítja a személyes adatok hordozhatóságát az alábbi feltételek teljesülése esetén:
a) a személyes adatokat az érintett bocsátotta az Adatkezelő rendelkezésére;
b) az adatkezelés jogalapja hozzájárulás vagy az érintett és az Adatkezelő között kötött szerződés;[57]
c) adatkezelés automatizált módon történik;[58]
d) a személyes adatok hordozása nem érinti hátrányosan mások jogait vagy szabadságait.

(2) Az adathordozhatósághoz való jog gyakorlása során az Adatkezelő köteles a személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban az érintett rendelkezésére bocsátani (PDF/XML).
(3) Az érintett kérheti, hogy az Adatkezelő a személyes adatokat közvetlenül egy másik adatkezelő részére továbbítsa. E lehetőséggel az érintett abban az esetben élhet csak, ha az technikailag megvalósítható.
(4) Az Adatkezelő emellett – a hozzáféréshez való jog érvényesülésének elősegítése érdekében – papír alapon is köteles rendelkezésre bocsátani a személyes adatokat.

### V.8. A tiltakozáshoz való jog

46. § (1) Amennyiben az adatkezelés az Adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, az érintett tiltakozhat a személyes adatok kezelése ellen.
(2) Tiltakozás esetén az Adatkezelő 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.[59]

---

[56] GDPR 18. cikk (3) bekezdés.
[57] GDPR 6. cikk (1) bekezdés a)-b) pontja.
[58] A papír alapú adatkezelések esetében e jog nem gyakorolható.
[59] GDPR 21. cikk (1) bekezdés.

47. § (1) 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.
(2) Amennyiben az érintett tiltakozik a személyes adatok közvetlen üzletszerzés céljából történő kezelése ellen, akkor a személyes adatok a továbbiakban e célból nem kezelhetők.[60]

### V.9. A jogorvoslathoz való jog

48. § (1) Adatkezeléssel kapcsolatos jogainak megsértése esetén az érintett – az adatkezelést végző ügyintéző útján vagy közvetlenül – az adatvédelmi felelőshöz fordulhat, aki a panaszt megvizsgálja, és ha alapos, az Adatkezelő vezető tisztségviselőjénél intézkedést kezdeményez, ellenkező esetben a panaszt elutasítja.
(2) Az elutasításról az Adatkezelő a panaszost a kérelem kézhezvételét követő 30 napon belül írásban tájékoztatja, a kérelem elutasításának ténybeli és jogi indokait is közölve. A kérelem elutasítása esetén a panaszost tájékoztatni kell a bírósági jogorvoslat, továbbá a felügyeleti szervhez fordulás lehetőségéről is. Az elutasított kérelmekről az adatvédelmi felelős jegyzőkönyvet köteles felvenni.

49.§ Ha az érintett továbbra is sérelmezi azt, ahogy a Adatkezelő kezeli az adatait, vagy közvetlenül hatósághoz szeretne fordulni, akkor bejelentéssel élhet a Nemzeti Adatvédelmi és Információszabadság Hatóságnál (cím: 1055 Budapest, Falk Miksa utca 9-11., levelezési cím: 1374 Budapest, Pf. 603. E-mail: ugyfelszolgalat@naih.hu, honlap: www.naih.hu).

50. § (1) Az érintettnek lehetősége van továbbá személyes adatainak védelme érdekében bírósághoz fordulni, amely az ügyben soron kívül jár el. Ebben az esetben az érintett szabadon választhat, hogy a lakóhelye (állandó lakcím) vagy a tartózkodási helye (ideiglenes lakcím) szerinti törvényszéknél (http://birosag.hu/torvenyszekek) nyújtja-e be keresetét.
(2) Az érintett a lakóhelye vagy tartózkodási helye szerinti törvényszéket megkeresheti a http://birosag.hu/ugyfelkapcsolati-portal/birosag-kereso oldalon.

## VI. ADATBIZTONSÁG

51. § (1) Az Adatkezelő 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 GDPR-ral összhangban történik. Ideértve többek között, adott esetben:

a) a személyes adatok álnevesítését és titkosítását;[61]
b) a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítását, integritását, rendelkezésre állását és ellenálló képességét;

[60] GDPR 21. cikk (3) bekezdés.
[61] GDPR 4. cikk 5. pont.

c) fizikai vagy műszaki incidens esetén az arra való képességet, hogy a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását kellő időben vissza lehet állítani;
d) az adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedések hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárást.[62]

(2) A 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.

52. § (1) Az Adatkezelő megfelelő technikai és szervezési intézkedéseket hajt végre, amelyek célja egyrészt a Szabályzat 10-19. §-aiban foglalt elvek hatékony megvalósítása, másrészt a további adatvédelmi garanciák beépítése az adatkezelés folyamatába.[63]

(2) Az Adatkezelő 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. Ez a kötelezettség vonatkozik a gyűjtött személyes adatok mennyiségére, kezelésük mértékére, tárolásuk időtartamára és hozzáférhetőségükre. Ezek az intézkedések különösen azt kell, hogy biztosítsák, hogy a személyes adatok alapértelmezés szerint a természetes személy beavatkozása nélkül ne válhassanak hozzáférhetővé meghatározatlan számú személy számára.[64]

53. § (1) 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.

(2) Az adathordozó képek és dokumentációk elhelyezésének-, fizikai védelmének biztonságáról az adatkezelő szervezeti egység vezetője az adatvédelmi felelőssel egyetértésben dönt.

(3) A szervezeti egységeknél kialakítandó adatkezelési rendszer környezetének védelméről a helyi adottságok figyelembevételével az illetékes vezetőknek kell gondoskodni, beleértve az adatsértések megelőzését is.

(4) A manuálisan kezelt személyes adatok elvesztésének megelőzése érdekében eredeti iratokat csak hivatalos ügyintézés, különösen bírósági eljárás vagy nyomozati eljárás során lehet kiadni. Kiadást megelőzően az eredeti iratokról az illetékes szervezeti egységnél történő megőrzés céljára hiánytalan másolatot kell készíteni.

(5) Személyes adatokat ért sérülés vagy megsemmisülés esetén a rendelkezésre álló egyéb adatforrásokból meg kell kísérelni a lehetséges mértékig a károsodott adatok pótlását. A sérült adat pótlására annak a szervezeti egységnek a vezetője felelős, ahol a sérülés bekövetkezett. Az adatpótlásba be kell vonni azon illetékes adatkezelő személyt, aki az adatok rögzítésében közreműködött. A pótolt adatokon a pótlás tényét fel kell tüntetni.

[62] GDPR 32. cikk (1) bekezdés.
[63] GDPR 25. cikk (1) bekezdés.
[64] GDPR 25. cikk (2) bekezdés.

# VII. AZ ADATVÉDELMI INCIDENSEK KEZELÉSE

## VII.1. Az adatvédelmi incidens észlelése

54. § Az Adatkezelő akár belső, akár külső jelzés alapján értesülhet a nemvárt eseményről.

55. § (1) Belső jelzésnek minősül, ha az Adatkezelővel munkaviszonyban, munkavégzésre irányuló egyéb jogviszonyban álló személy, vagy az Adatkezelővel kötött szerződés alapján eljáró adatfeldolgozó észleli a nemvárt eseményt.
(2) Amennyiben az Adatkezelővel munkaviszonyban, munkavégzésre irányuló egyéb jogviszonyban álló személy észleli a nemvárt eseményt, köteles haladéktalanul, legfeljebb azonban az (1) bekezdés szerinti észleléstől számított 2 órán belül tájékoztatni közvetlen felettesét, illetve az Adatkezelő vezetőjét.
(3) Amennyiben az Adatkezelővel munkaviszonyban, munkavégzésre irányuló egyéb jogviszonyban álló olyan személy észleli a nemvárt eseményt, akinek nincs közvetlen felettese, köteles haladéktalanul, legfeljebb azonban az (1) bekezdés szerinti észleléstől számított 2 órán belül tájékoztatni az Adatkezelő vezetőjét.
(4) Amennyiben az Adatkezelővel kötött szerződés alapján eljáró adatfeldolgozó észleli a nemvárt eseményt, köteles az említett szerződésben meghatározott kapcsolattartó útján haladéktalanul, legfeljebb azonban az (1) bekezdés szerinti észleléstől számított 2 órán belül tájékoztatni az Adatkezelő vezetőjét.

56. § (1) Külső jelzésnek minősül, ha az 55. § (1) bekezdésében meghatározott személyek körén kívül eső bármely személy észleli a nemvárt eseményt, és erről – szóban, írásban vagy elektronikus úton – tájékoztatja az Adatkezelőt.
(2) Amennyiben a külső jelzés az Adatkezelővel munkaviszonyban, munkavégzésre irányuló egyéb jogviszonyban álló személyhez érkezik, e személy köteles haladéktalanul, legfeljebb azonban az (1) bekezdés szerinti észleléstől számított 2 órán belül tájékoztatni közvetlen felettesét, illetve az Adatkezelő vezetőjét.
(3) Amennyiben az Adatkezelővel munkaviszonyban, munkavégzésre irányuló egyéb jogviszonyban álló olyan személyhez érkezik a tájékoztatás, akinek nincs közvetlen felettese, köteles haladéktalanul, legfeljebb azonban az (1) bekezdés szerinti észleléstől számított 2 órán belül tájékoztatni az Adatkezelő vezetőjét.
(4) Amennyiben az Adatkezelővel kötött szerződés alapján eljáró adatfeldolgozóhoz érkezik a tájékoztatás, köteles az említett szerződésben meghatározott kapcsolattartó útján haladéktalanul, legfeljebb azonban az (1) bekezdés szerinti észleléstől számított 2 órán belül tájékoztatni az Adatkezelő vezetőjét.
(5) A NAIH Adatkezelő részére küldött megkeresése minden esetben külső jelzésnek minősül.

57. § Az Adatkezelő vezetője köteles haladéktalanul, legfeljebb azonban a beérkezéstől számított 2 órán belül továbbítani a nemvárt eseményről szóló tájékoztatás az Adatkezelő adatvédelmi felelőse részére.

58. § (1) Az adatvédelmi felelős köteles a hozzá beérkezett a nemvárt eseményről szóló tájékoztatást haladéktalanul megvizsgálni.

(2) Az adatvédelmi felelős eljárása során az alábbi tényezőket veszi figyelembe:
a) a nemvárt esemény személyes adatokat érint-e;[65]
b) a nemvárt esemény a biztonság sérüléséből következett-e be;[66]
c) a biztonság sérülése milyen eredménnyel járt a személyes adatokra nézve.
(3) Az adatvédelmi felelős jogosult a nemvárt esemény vizsgálatával összefüggésben az Adatkezelővel munkaviszonyban, munkavégzésre irányuló egyéb jogviszonyban álló személytől, valamint az Adatkezelővel kötött szerződés alapján eljáró adatfeldolgozótól információt, tájékoztatást kérni.

59. § (1) Amennyiben az adatvédelmi felelős – az 58. § (2) bekezdés a)-b) pontja esetében végzett vizsgálat eredményeként – megállapítja, hogy a személyes adatokat érintő nemvárt esemény a biztonság sérüléséből következett be, az a GDPR 33. cikk (1) bekezdése szerinti tudomásra jutásnak minősül.[67]
(2) Amennyiben az adatvédelmi felelős a vizsgálat következtében megállapítja, hogy a nemvárt esemény adatvédelmi incidensnek minősül, köteles elvégezni az incidens 4. § o)-q) pontjaiban foglaltak szerinti kategorizálását is.

### VII.2. Az adatvédelmi incidens kivizsgálása

60. § Az adatvédelmi felelős haladéktalanul, legfeljebb azonban az 59. § (1) bekezdése szerinti tudomásra jutásáról számított 2 órán belül értesíti az Adatkezelő vezetőjét az adatvédelmi incidensről, és összehívja az incidenskezelő csoportot.

61. § (1) Az incidenskezelő csoport feladata az adatvédelmi incidens körülményeinek feltárása, az adatvédelmi incidens kockázatainak felmérése, elemzése és kezelése, valamint az adatvédelmi incidenssel kapcsolatos további intézkedések megtételére vonatkozó döntéshozatal.
(2) Az incidenskezelő csoport vezetését és irányítását az adatvédelmi felelős látja el.
(3) Az incidenskezelő csoport az adatvédelmi incidens kezelésének lezárásáig folyamatosan ülésezik az adatvédelmi felelős által meghatározott rendszerességgel.
(4) Az incidenskezelő csoport az adatvédelmi incidens kezelésének lezárásával szűnik meg, ideértve a NAIH esetleges eljárása keretében hozott döntéseket is.
(5) Az incidenskezelő csoport a tevékenységének lezárásaként jelen Szabályzat 5. számú függelékben foglaltak szerinti formában és tartalommal jelentést készít az Adatkezelő felső vezetésének az incidens kezelésével kapcsolatban.

62. § (1) Az incidenskezelő csoport tagjai:
a) az adatvédelmi felelős;
b) IT szakértő;
c) jogi tanácsadással megbízott partner;
d) az érintett munkatársa;
e) az Adatkezelő ügyvezetője vagy az általa megbízott személy.
(2) Az incidenskezelő csoport tagja lehet egyéb személy is szükség esetén.

[65] L. a Szabályzat 4. § a) pontját.
[66] L. a Szabályzat 4. § r) pontját.
[67] Következésképpen az incidenssel kapcsolatos kötelezettségek teljesítésére nyitva álló határidőt innen kell számolni.

63. § (1) Az incidenskezelő csoport első ülését az adatvédelmi felelős nyitja meg.
(2) Az adatvédelmi felelős az incidenskezelő csoport első ülésén ismerteti az adatvédelmi incidenssel kapcsolatban rendelkezésre álló információkat, tényeket, különös tekintettel az adatvédelmi incidens bekövetkezésének körülményeire és az incidens kategorizálására.
(3) Az incidenskezelő csoport ezt követően megkezdi az adatvédelmi incidens kockázatainak felmérését és elemzését, azok valószínűségének és súlyosságainak figyelembevételével. A kockázatok tekintetében azok forrását, a kiszolgáló környezetet, a személyes adatokat, illetve az incidens lehetséges hatásait kell vizsgálni.
(4) A kockázatok forrása tekintetében figyelembe vehető tényezők:
a) az incidens véletlen belső magatartás vagy tevékenység eredménye;
b) az incidens szándékos belső magatartás vagy tevékenység eredménye;
c) az incidens véletlen külső magatartás vagy tevékenység eredménye;
d) az incidens szándékos belső magatartás vagy tevékenység eredménye.
(5) A kiszolgáló környezet szempontjából figyelembe vehető tényezők:
a) az adatkezelés eszközei (papír alapú vagy automatizált módszerekkel történő adatkezelés);
b) az incidenssel érintett rendszer (levelező rendszer, adathordozó stb.);
c) a kiszolgáló környezet biztonságát védő intézkedések (pl. titkosítás, elnevesítés, tűzfal);[68]
d) a kiszolgáló környezet ellenállóképessége;
e) az incidens elhárítása érdekében előzetes tett intézkedések hatékonysága;
f) az incidens bekövetkeztét lehetővé tevő tényezők;
g) az incidens bekövetkeztét befolyásoló egyéb tényezők;
h) a rendszerszerű működés helyreállításának valószínűsége.
(6) A személyes adatok szempontjából figyelembe vehető tényezők:
a) a személyes adatok kategóriái, különös tekintettel a különleges adatokra;[69]
b) személyes adatok száma;
c) érintettek kategóriái, különös tekintettel az érintettek kiszolgáltatott helyzetéra (gyermek, munkavállaló);
d) az érintettek azonosíthatósága;
e) az érintettek száma.
(7) Az incidens hatásai szempontjából figyelembe vehető tényezők:
a) fizikai kár vagy veszély;
b) vagyoni kár;
c) nem vagyoni kár.[70]
(8) Az incidenskezelő csoport köteles az adatvédelmi incidenst egyedileg, kockázati szint szerint besorolni a következők szerint: alacsony, közepes vagy magas kockázatú incidens.
(9) A (4) bekezdés b)-d) pontjaiban foglalt esetek, az (6) bekezdés a) pontjában foglalt különleges adatok és c) pontjában foglalt kiszolgáltatott helyzetben lévő érintettek, a (7) bekezdés b) pontja szerinti személyes adatok, illetve e) pontja szerinti érintettek magas száma közepes vagy magasabb kockázatot jelent.
(10) Szintén valószínűsíthetően magasabb kockázattal jár az adatvédelmi incidens a természetes személyek jogaira és szabadságaira nézve, ha annak eredménye:

[68] GDPR 24. cikk (1)-(2) bekezdés és 32. cikk.
[69] GDPR 4. cikk 1., 13-15. pontok, 9. cikk (1) bekezdés és 10. cikk.
[70] GDPR (75) preambulumbekezdés.

a) az érintett hátrányos megkülönböztetése;
b) személyazonosság-lopás;
c) személyazonossággal való visszaélés;
d) pénzügyi veszteség;
e) az érintett jó hírnevének sérelme;
f) a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülése;
g) álnevesítés engedély nélkül történő feloldása;
h) bármilyen egyéb jelentős gazdasági vagy szociális hátrány;
i) alapvető jogai vagy szabadságai gyakorlásának ellehetetlenülése;
j) az érintettek saját személyes adatai feletti önrendelkezései jogának megszűnése;
k) személyes jellemzők értékelésére személyes profil létrehozása vagy felhasználása céljából.

64. § Amennyiben az adatvédelmi incidens alacsony kockázatú, úgy kell tekinteni, hogy az valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve.

65. § Amennyiben az adatvédelmi incidens közepes kockázatú, úgy kell tekinteni, hogy az – a GDPR 33. cikk (1) bekezdése szerint – valószínűsíthetően kockázattal jár a természetes személyek jogaira és szabadságaira nézve.

66. § Amennyiben az adatvédelmi incidens magas kockázatú, úgy kell tekinteni, hogy az – a GDPR 34. cikk (1) bekezdése szerint – valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve.

67. § Az incidenskezelő csoport köteles továbbá meghozni mindazon intézkedéseket, amelyek az adatvédelmi incidens következményeinek mérséklése vagy elhárítása érdekében szükséges, ideértve az érintett rendszerek működésének helyreállítását, az érintettek esetleges tájékoztatását, valamint – szabálysértés vagy bűncselekmény esetén – a szabálysértések vagy bűncselekmények felderítésére hatáskörrel és illetékességgel rendelkező szervek értesítését.

### VII.3 Az adatvédelmi incidens bejelentése

68. § (1) Amennyiben az adatvédelmi incidens valószínűsíthetően kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az Adatkezelő köteles indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, bejelentést tenni a NAIH-hoz.
(2) Amennyiben az adatvédelmi incidens körülményeinek feltárása, kockázatainak felmérése indokolttá teszi, a bejelentés részletekben is történhet.
(3) Az Adatkezelő nevében a bejelentési kötelezettséget az adatvédelmi felelős teljesíti.
(4) Az adatvédelmi felelős a bejelentési kötelezettséget papír alapon, vagy a NAIH honlapján elérhető elektronikus bejelentési rendszer útján telesíti.[71]

[71] http://naih.hu/adatvedelmi-incidensbejelent--rendszer.html.

69. § A NAIH részére tett bejelentésnek tartalmaznia kell:[72]

a) az Adatkezelő adatait;
b) az adatvédelmi incidens időpontját;
c) az adatvédelmi incidensről való tudomásszerzés időpontját;
d) az adatvédelmi incidens észlelésének módját;
e) esetleges késedelmes tájékoztatás indokait;
f) az adatvédelmi incidens jellegét;
g) az adatvédelmi incidenssel érintett személyes adatokat;
h) az adatvédelmi incidenssel érintett személyes adatok becsült számát;
i) az érintettek kategóriáit;
j) az adatvédelmi incidens előtt alkalmazott intézkedéseket;
k) az adatvédelmi incidens következményeinek a megjelölését;
l) az érintetteket ért fizikai, anyagi vagy nem vagyoni károkat, vagy egyéb jelentős következményeket, valamint a valószínűsíthető következmények súlyosságát;
m) a megtett intézkedéseket;
n) az adatvédelmi incidens orvoslására tett intézkedéseket;
o) egyéb bejelentéseket;
p) az adatvédelmi felelős nevét és elérhetőségeit.

70. § (1) Az adatvédelmi felelős köteles együttműködni a NAIH-hal az adatvédelmi incidensek kezelésével összefüggésben indult eljárások során.
(2) Az adatvédelmi felelős köteles a NAIH rendelkezésére bocsátani az adatvédelmi incidensek kezelésével összefüggésben indult eljárások lefolytatásához szükséges további információkat.
(3) Annak érdekében, hogy az adatvédelmi felelős teljesíteni tudja a fenti kötelezettségét, jogosult az Adatkezelővel munkaviszonyban, munkavégzésre irányuló egyéb jogviszonyban álló személytől, valamint az Adatkezelővel kötött szerződés alapján eljáró adatfeldolgozótól információt, tájékoztatást kérni.
(4) Az incidenskezelő csoport tagjai kötelesek közreműködni az adatvédelmi felelősvel a fenti kötelezettség teljesítése során.

71. § (1) Amennyiben az 68. § szerinti bejelentés mellőzésére kerül sor, annak okait az adatvédelmi felelős dokumentálni köteles.
(2) A bejelentés megtörténtével vagy mellőzésével kapcsolatos információk az incidenskezelő csoport 61. § (5) bekezdése szerinti jelentésének részét képezik.

### VII.4. Az érintettek tájékoztatása

72. § (1) Amennyiben az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az Adatkezelő köteles indokolatlan késedelem nélkül tájékoztatni az érintettet az adatvédelmi incidensről.
(2) Az Adatkezelő nevében az (1) bekezdés szerinti kötelezettségét az adatvédelmi felelős teljesíti.
(3) Amennyiben az adatvédelmi incidens az Adatkezelővel munkaviszonyban, munkavégzésre irányuló egyéb jogviszonyban álló személyek érint, a tájékoztatást az

[72] GDPR 33. cikk (3) bekezdés.

érintetteket foglalkoztató szervezeti egységek bevonásával, a munkavállalókkal történő kapcsolattartás céljára használt rendszerek segítségével kell megadni.
(4) Amennyiben az adatvédelmi incidens a (3) bekezdés hatálya alá nem tartozó személyeket érint, a tájékoztatást az érintettekkel történő kapcsolattartás céljára használt rendszerek segítségével kell megadni. Ebben az esetben a tájékoztatás tartalmának kialakításában az Adatkezelő sajtókapcsolatokért felelős munkatársa közreműködik.
(5) Amennyiben – az érintettek nagy számára tekintettel – a személyes tájékoztatás lehetetlen lenne vagy aránytalan költséggel járna az Adatkezelőre nézve, a tájékoztatás helyi vagy országos sajtótermékekben megjelentetett figyelemfelhívó jelzés útján is megadható.
(6) A (4) és (5) bekezdésekben foglalt esetekben az Adatkezelő honlapján figyelemfelhívó jelzést kell elhelyezni, amely általános tájékoztatást nyújt az incidens jellegéről, az érintett személyes adatok, illetve az érintettek kategóriáról.

73. § Az érintett vagy érintettek részére nyújtott tájékoztatásnak tartalmaznia kell legalább:[73]

a) az adatvédelmi incidens jellegének leírását;
b) az adatvédelmi felelős nevét és elérhetőségeit;
c) az adatvédelmi incidens valószínűsíthető következményeinek ismertetését;
d) az adatvédelmi incidens orvoslására tett vagy tervezett intézkedések ismertetését, beleértve adott esetben az incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket is;
e) az érintettek által az adatvédelmi incidens orvoslására tehető intézkedések ismertetését, beleértve adott esetben az incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket is.

74. § (1) Annak érdekében, hogy az adatvédelmi felelős teljesíteni tudja a 72. § (2) bekezdésben foglalt kötelezettségét, jogosult az Adatkezelővel munkaviszonyban, munkavégzésre irányuló egyéb jogviszonyban álló személytől, valamint az Adatkezelővel kötött szerződés alapján eljáró adatfeldolgozótól információt, tájékoztatást kérni.
(4) Az incidenskezelő csoport tagjai kötelesek közreműködni az adatvédelmi felelősvel a 72. § (2) bekezdésben foglalt kötelezettség teljesítése során.

75. § (1) Amennyiben az 72. § szerinti tájékoztatás mellőzésére kerül sor, annak okait az adatvédelmi felelős dokumentálni köteles.
(2) A tájékoztatás megtörténtével vagy mellőzésével kapcsolatos információk az incidenskezelő csoport 61. § (5) bekezdése szerinti jelentésének részét képezik.

### VII.5. Az adatvédelmi incidensek nyilvántartása

76. § (1) Az Adatkezelő köteles nyilvántartani az adatvédelmi incidenseket, tekintet nélkül azok kockázati besorolására.
(2) Az Adatkezelő az (1) bekezdés szerinti kötelezettségének a 2. számú függelékben foglaltak szerinti formában és tartalommal tesz eleget.

[73] 34. cikk (1)-(2) bekezdés.

(3) Az adatvédelmi incidensek nyilvántartása tartalmazza:[74]

a) az Adatkezelő megnevezését és elérhetőségeit;
b) az adatvédelmi incidens azonosítóját;
c) az érintett személyes adatok körét;
d) az adatvédelmi incidenssel érintettek körét;
e) az adatvédelmi incidenssel érintettek számát;
f) az adatvédelmi incidens megtörténtének időpontját;
g) az adatvédelmi incidens tudomásra jutásának időpontját;
h) az adatvédelmi incidens jellegét;
i) az adatvédelmi incidens körülményeit;
j) az adatvédelmi incidens hatásait;
k) az adatvédelmi incidens elhárítására megtett intézkedéseket;
l) az adatkezelést előíró jogszabályban meghatározott egyéb adatokat;
m) a bejelentési kötelezettség tényét;
n) a hatósági bejelentés időpontját;
o) a bejelentő személy nevét;
p) a tájékoztatási kötelezettség tényét;
q) az érintettek tájékoztatásának időpontját;
r) a bejegyzés dátumát.

(4) Az Adatkezelő nevében az (1) bekezdés szerinti kötelezettségét az adatvédelmi felelős teljesíti.
(5) Az adatvédelmi felelős gondoskodik az adatvédelmi incidensek nyilvántartásának naprakészen tartásáról, frissítéséről.
(6) Az adatvédelmi felelős köteles a nyilvántartást a NAIH ez irányú kérésére rendelkezésre bocsátani.[75]

# VIII. ELSZÁMOLTATHATÓSÁG

## VIII.1. Az adatkezelésre és adatfeldolgozásra vonatkozó általános követelmények

77. § (1) Az Adatkezelővel a jelen Szabályzat 3. § (1) bekezdése szerint jogviszonyban álló 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 azoknak megfelelő védelmét biztosítsa.
(2) 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.
(3) Az Adatkezelővel jogviszonyban állók, illetve az Adatkezelő képviseletében eljáró személyek kötelesek bizalmasan kezelni minden olyan személyes adatot, amely számukra a jogviszonyukkal összefüggésben vált ismertté.

[74] GDPR 33. cikk (5) bekezdés.
[75] Uo.

78. § Az Adatkezelővel jogviszonyban álló, adatkezelést vagy adatfeldolgozást végző személyek felelősséggel tartoznak minden olyan kárért, amely adatkezelési, adatvédelmi kötelezettségük megszegéséből származik.

79. § (1) Ha az adatkezelést az Adatkezelő nevében más végzi, az Adatkezelő kizárólag olyan adatfeldolgozókat vehet igénybe, akik vagy amelyek megfelelő garanciákat nyújtanak az adatkezelés követelményeinek való megfelelést és az érintettek jogainak védelmét biztosító, megfelelő technikai és szervezési intézkedések végrehajtására.
(2) Az adatfeldolgozó által végzett adatkezelést olyan szerződésnek kell szabályoznia, amely köti az adatfeldolgozót az Adatkezelővel szemben. A szerződés kizárólag írásban köthető meg.
(3) A szerződésben rögzíteni kell különösen az alábbiakat:

a) az Adatkezelő és az adatfeldolgozó megnevezése;
b) az adatkezelés tárgya;
c) a kezelendő személyes adatok típusa;[76]
d) a kezelendő személyes adatok mennyisége (ha lehetséges);
e) az érintettek kategóriái;[77]
f) az adatkezelés jellege és célja;
g) az adatkezelés jogalapja;[78]
h) az adatkezelés időtartama;
i) teendők az adatkezelési szolgáltatás nyújtásának befejezés esetén;[79]
j) az Adatkezelő kötelezettségeit és jogai;
k) az adatfeldolgozó 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;
l) az Adatkezelő és az adatfeldolgozó közötti utasításadás, illetve kapcsolattartás módja;
m) a további adatfeldolgozó igénybevételére vonatkozó döntés;
n) az adatfeldolgozó a további adatfeldolgozó igénybevételére vonatkozóan tiszteletben tartja a jogszabályi előírásokat;[80]
o) titoktartási kötelezettség;
p) adatbiztonsági előírások;[81]
q) közreműködés az adatbiztonsági előírások érvényesítésében, az incidensek kezelésében és a hatásvizsgálatok elvégzésénél;[82]
r) közreműködés az érintetti jogok gyakorlásában;[83]

[76] A kezelendő adatkörök megnevezése.
[77] Pl. munkavállaló, ügyfél, kapcsolattartó, stb.
[78] L. a Szabályzat 20-36. §-ai.
[79] Személyes adatot törlése, vagy visszajuttatása az Adatkezelőnek és törlése.
[80] GDPR 28. cikk (2) és (4) bekezdés.
[81] L. GDPR 32. cikk.
[82] L. GDPR 32-36. cikk.
[83] L. a Szabályzat 37-50. §-ai.

s) információk nyújtása az Adatkezelőnek és az Adatkezelő ellenőrzési jogosultsága;[84]
t) az Adatkezelő ellenőrzésének kivitelezési módja;
u) a felelősség egyes kérdései;
v) a jogérvényesítési lehetőségek.

(4) Amennyiben szükséges, az adatkezelő és az adatfeldolgozó további 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.

### VIII.2. Az adattovábbításra vonatkozó követelmények

80. § Az Adatkezelő szervezeti rendszerén belül a személyes adatok – a feladat elvégzéséhez szükséges mértékben és ideig – olyan szervezeti egységhez, személyhez továbbíthatók, amelynek az Adatkezelőnél végzett feladatának ellátásához a személyes adatok megismerése és kezelése szükséges.

81. § Az Adatkezelőnél különböző célra irányuló adatkezelések csak törvényes céloknak megfelelően, indokolt esetben kapcsolhatók össze.

82. § (1) Olyan megkeresés, amely az Adatkezelő által kezelt személyes adat továbbítására irányul csak jogszabályi előírás alapján, vagy csak a (2) bekezdésben foglalt feltételek fennállása esetén teljesíthető. Minden más esetben az adattovábbítás teljesítését meg kell tagadni.
(2) Olyan esetben, amikor az adattovábbítás nem jogszabályi kötelezettségen alapul, a megkeresés csak akkor teljesíthető, ha az érintett ehhez – részletes tájékoztatást követően – igazolható módon hozzájárul, vagy ha az az Adatkezelő vagy harmadik személy jogos érdekének érvényesítéséhez szükséges.[85]

83. § (1) Külföldre 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.[86]
(2) Olyan személyes adatok továbbítására – ideértve a személyes adatok harmadik országból vagy nemzetközi szervezettől egy további harmadik országba vagy további nemzetközi szervezet részére történő újbóli továbbítását is –, amelyeket harmadik országba vagy nemzetközi szervezet részére történő továbbításukat követően adatkezelésnek vetnek alá vagy szándékoznak alávetni, csak abban az esetben

[84] Az Adatkezelő vagy az általa megbízott más ellenőr jogosult az adatkezelés megkezdése előtt, illetve annak folyamatában auditokat végezni, beleértve a helyszíni vizsgálatokat is, amelyek célja az adatfeldolgozó tevékenysége jogszerűségének biztosítása.
[85] L. a Szabályzat 20-36. §-ai.
[86] L. GDPR 44-50. cikkek.

kerülhet sor, ha az adatkezelő és az adatfeldolgozó egyaránt teljesíti a GDPR-ban rögzített feltételeket.
(3) Személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására sor kerülhet, ha az Európai Bizottság megállapította, illetve az Európai Unió Hivatalos Lapjában és annak honlapján közzétette, hogy a harmadik ország, a harmadik ország valamely területe, vagy egy vagy több meghatározott ágazata, vagy a szóban forgó nemzetközi szervezet megfelelő védelmi szintet biztosít (megfelelőségi határozat). Az ilyen adattovábbításhoz nem szükséges külön engedély.

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

85. § Az Adatkezelő vállalja, hogy a személyes adatokat statisztikai célra kizárólag úgy adja át, hogy gondoskodik arról, hogy azt az érintettel ne lehessen kapcsolatba hozni.

86. § Az Adatkezelő az általa végzett adattovábbításokat a Szabályzat 3. számú függelékét képező nyilvántartás szerinti tartalommal tartja nyilván.

### VIII.3. Az adatkezelési tevékenységek nyilvántartása

87. § (1) Az Adatkezelő köteles nyilvántartani minden olyan adatkezelési tevékenységét, amely:
a) az érintettek jogaira és szabadságaira nézve valószínűsíthetően kockázattal jár;
b) nem alkalmi jellegű;
c) különleges adatok vagy bűnügyi személyes adatok kezelésével jár.[87]
(2) Az Adatkezelő az (1) bekezdés szerinti kötelezettségének az 4. számú függelékben foglaltak szerinti tartalommal tesz eleget.
(3) Az Adatkezelő nevében az (1) bekezdés szerinti kötelezettségét az adatvédelmi felelős teljesíti.
(4) Az adatvédelmi felelős gondoskodik az adatvédelmi tevékenységek nyilvántartásának naprakészen tartásának felügyeletéről.
(5) Az adatvédelmi felelős köteles a nyilvántartást a NAIH ez irányú kérésére rendelkezésre bocsátani.

88. § Az adatvédelmi tevékenységek nyilvántartása tartalmazza:[88]
a) az Adatkezelő megnevezését és elérhetőségeit;
b) az adatkezelés megnevezését;
c) a tényleges adatkezelés helyét;
d) az adatkezelés célját;
e) az adatkezelés jogalapját;
f) az adatkezelés jogalapjának megnevezését;
g) közös adatkezelés esetén a közös adatkezelő megnevezését és elérhetőségeit;
h) az adatkezelés helyét;
i) az adatfeldolgozónak az adatkezeléssel összefüggő tevékenységét;

[87] L. GDPR 9. cikk (1) bekezdés és 10. cikk.
[88] GDPR 30. cikk (1) bekezdés.

j) az adatkezelés technológiáját;
k) az informatikai alkalmazás megnevezését;
l) az adatkezelő által kezelt személyes adatok körét;
m) az adatkezelés időtartamát;
n) az adatok forrását;
o) adattovábbítás esetén az adatok fajtáját;
p) a címzett megnevezését és elérhetőségét;
q) a személyes adatok harmadik országba vagy nemzetközi szervezet részére történő adattovábbítása esetén a megfelelő garanciára vonatkozó információkat;
r) az adattovábbítás jogalapját;
s) az érintettek körét;
t) az adatbiztonság garantálása érdekében alkalmazott technikai és szervezési intézkedések leírását.

### VIII.4. Az adatvédelmi hatásvizsgálat és az előzetes konzultáció

89. § Amennyiben 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 az Adatkezelő az adatkezelést megelőzően hatásvizsgálatot végez arra vonatkozóan, hogy a tervezett adatkezelési műveletek a személyes adatok védelmét hogyan érintik.

90. § Amennyiben 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 az Adatkezelő konzultál a felügyeleti hatósággal (előzetes konzultáció). Az Adatkezelő előzetes konzultáció szükségessége esetén a felügyeleti hatóság álláspontját az érintett adatkezeléssel összefüggő döntések meghozatala során köteles figyelembe venni.

## IX. AZ ADATKEZELÉS SPECIÁLIS ESETEI

### IX.1. A munkatársak adatainak kezelése

91. § Az Adatkezelő valamennyi munkaviszonyt vagy munkavégzésre irányuló egyéb jogviszonyt létesítőt köteles tájékoztatni a munkavégzéssel kapcsolatos adatkezelésekről. A tájékoztatás megismeréséről az érintett írásban nyilatkozik.

92. § A bér- és munkaügyi nyilvántartás adatai a foglalkoztatott jogviszonyával kapcsolatos tények megállapítására, a besorolási követelmények igazolására, bérszámfejtésre, társadalombiztosítási ügyintézésre és statisztikai adatszolgáltatásra használhatók fel.

93. § A bér- és munkaügyi nyilvántartás kezelését – a feladatkörük ellátásához szükséges mértékben – az Adatkezelő személyzeti ügyekért felelős munkavállalója, illetve szerződéses partnere végzi.

### IX.2. Manuálisan kezelt személyes adatok

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

95. § (1) A manuálisan kezelt személyes adatok biztonsága érdekében az alábbi intézkedéseket kell foganatosítani:

a) az irattári kezelésbe vett iratokat jól zárható, száraz, tűzvédelmi és vagyonvédelmi berendezéssel ellátott helyiségben kell elhelyezni;
b) a folyamatos aktív kezelésben lévő iratokhoz csak az illetékes ügyintézők férhetnek hozzá, a személyzeti, a bér- és munkaügyi iratokat biztonságosan elzárva kell tartani,
c) az adatkezelések iratainak archiválását rendszeresen el kell végezni, az archivált iratokat a vonatkozó előírásoknak megfelelően kell szétválogatni és irattári kezelésbe venni.

(2) Az (1) bekezdés b) pontja szerinti helyiségek, illetve szekrények kulcsához való hozzáférés rendjét az Adatkezelő ügyvezetője állapítja meg, melyet az adatvédelmi felelős részére tájékoztatásul megküld.

### IX.3. Elektronikusan kezelt személyes adatok

96. § (1) Amennyiben az Adatkezelő olyan elektronikus rendszerben kezel személyes adatot, amelybe csak a hozzáférési listára felvett, nyilvántartott, illetékes munkavállaló léphet be, úgy az illetékes munkatársnak egyéni, titkos jelszóval kell bejelentkeznie a rendszerbe. Az adatkezelés befejeztével a rendszerből ki kell lépni. A rendszerben történt, jelszóval védett adatkezelésért az Adatkezelő felel.
(2) Az adatvédelmi incidensek elkerülése érdekében a munkavállaló kötelessége az egyéni jelszavának védelme. Az egyéni jelszó a munkavállalón kívül kizárólag az adatkezelési szoftver fejlesztését, üzemeltetését ellátó informatikai munkatársak, valamint az adatvédelmi felelős által ismerhető meg, ha az az Adatkezelőnél elvégzendő feladatuk ellátásához szükségessé válik.
(3) Az adatkezelésre használt számítógépek adatbevitelre, lekérdezésre alkalmas állapotban történő, felügyelet nélkül hagyása tilos.
(4) Az Adatkezelő kizárólag olyan adatkezelési rendszert alkalmazhat, amely a rendszerbe történt belépést regisztrálja, illetve a rögzített adatokról megállapítható, hogy az adatrögzítés ki által és milyen időpontban történt.

### IX.4. A munkavállalókat érintő ellenőrzések szabályai

#### IX.4.1. Postai küldemények

97.§ A munkahelyre érkezett postai küldemény, amennyiben feltételezhető, hogy az személyre szóló – például „s.k.” jelzéssel lett ellátva, vagy a címzett pontos nevét feltüntették – először a munkavállalónak kell átadni. Amennyiben ilyen tartalmú levél

mégis felbontásra kerül, akkor azt vissza kell zárni, és a felbontás dátumát, valamint a levél tartalmának megismerő személy nevét fel kell rajta tüntetni.

### IX.4.2.Telefonok használatának ellenőrzése

98.§ Az Adatkezelő által a munkavállalók rendelkezésére bocsátott mobil és vezetékes telefonokat kizárólag hivatalos célból lehet használni, a magáncélú használat nem engedélyezett.

99.§ Amennyiben az Adatkezelő, mint munkáltató a jogos érdekére hivatkozva ellenőrizni kívánja a munkavállalók telefonhasználatát, akkor ez kizárólag a hivatalos használatra terjedhet ki, az esetleges magáncélú használat ellenőrzése tilos. Az ellenőrzés során főszabály szerint az Adatkezelő biztosítja a munkavállaló jelenlétét és ellenőrzés során a fokozatosság elvének betartásával jár el. Az ellenőrzés lefolytatása előtt a munkáltatói jogkörgyakorló köteles a munkavállalót az adatkezelés körülményeiről tájékoztatni. Amennyiben a munkáltatói ellenőrzés a munkavállalóhoz köthető híváslista ellenőrzéséhez kapcsolódik, akkor a távközlési szolgáltatótól meg kell kérni az adott telefonszámhoz tartozó részletes híváslistát olyan módon, hogy a híváslistában szereplő telefonszámok utolsó három számjegye nem felismerhető formában (anonimizáltan) szerepeljen, amely alapján a munkavállaló az esetleges magáncélú hívásait kiválogathatja. Ezt az anonimizált híváslistát kizárólag az érintett munkavállaló és a munkáltatói jogkörgyakorló ismerheti meg.

100. § Abban az esetben, ha a munkavállaló visszaadja az általa használt mobiltelefont akár a munkaviszony fennállása alatt, akár a munkaviszony megszűnésekor, gondoskodni kell arról, hogy az eszközön tárolt esetleges magánjellegű adatokat – így telefonszámokat, üzeneteket, képeket, filmeket, egyéb formájú és tartalmú adatokat – az érintett lementhesse, majd azokat visszaállíthatatlan módon törölni kell. A munkavállaló köteles a magánjellegű tartalmak eltávolításáról jelen Szabályzat 6. számú függelékben foglaltak szerinti formában és tartalommal írásbeli nyilatkozatot tenni. A készüléket csak azt követően lehet átadni harmadik személy részére, ha az eszközkiadásért felelős személy meggyőződött arról, hogy azon magánjellegű adat már nincs, vagy nem fellelhető. Az eljárást lefolytató személyt a megismert magánjellegű adatok tekintetében titoktartási kötelezettség terheli, azt harmadik személy részére nem adhatja át, rá vonatkozó információt nem közölhet.

### IX.4.3. E-mail postafiók használatának és ellenőrzésének adatvédelmi szabályai

101. § Az Adatkezelő a munkavégzés céljára rendelkezésre bocsátott e-mail postafiókot hivatalos célból adja át a munkavállalónak, mely fiók magáncélra nem használható.

102. § Az Adatkezelő informatikai rendszereinek üzembiztos működéséért felelős szervezeti egysége (ICT) jogosult az e-mail postafiók tárolókapacitását meghatározni, az e-mailhez csatolt fájlok méretét és formátumát korlátozni, és köteles az ezzel kapcsolatos információkról a munkavállalókat szükség szerint, de legalább fél évente e-mailben tájékoztatni. E beállításokat, és a szervezeti egység által meghatározott további felhasználói szabályokat a munkavállalók kötelesek betartani.

103. § A munkavállaló további nem üzleti e-mail postafiókokat a munkahelyi számítógépen megnyithat, és használhat azzal, hogy az ilyen magáncélú használat során az Adatkezelő üzleti érdekeit és jó hírnevét nem sértheti.

104. § Az Adatkezelő, mint munkáltató jogos érdekére hivatkozva ellenőrizheti a munkavállaló által folytatott hivatalos levelezést a jelen Szabályzatban foglaltak betartásával. Az ellenőrzés során az Adatkezelő fő szabály szerint biztosítja a munkavállaló személyes jelenlétét, továbbá az ellenőrzés során a fokozatosság elvének betartásával jár el. Az ellenőrzés alapját az Adatkezelő által elkészített érdekmérlegelési teszt eredménye adja. Az ellenőrzésre jogosult munkáltatói jogkör gyakorló köteles a munkavállalót dokumentált módon, a tényleges ellenőrzés megkezdése előtt tájékoztatni, hogy mely, pontosan meghatározott érdek miatt kerül sor az ellenőrzésre. A munkavállaló az ellenőrzés során az e-mail tartalmának megtekintése előtt köteles jelezni a munkáltatónak, illetve a munkáltató képviseletében eljáró személynek, ha az adott e-mail személyes adatot tartalmaz. A munkaköri feladatokkal kapcsolatos e-mailek tartalmát az Adatkezelő korlátozás nélkül vizsgálhatja.

105. § Amikor a hivatalos e-mail postafiók tartalmát a munkáltató ellenőrizni kívánja – a lépcsőzetes ellenőrzési rendszer alapján –, elsősorban a levelek fejlécének listáját jogosult az informatikai szakértőtől megkérni. A lista tartalmazhatja a postafiókba érkezett és onnan küldött levelek címzettjét, tárgyát, valamint, amennyiben további adat ismerete szükséges a küldés vagy fogadás időtartamát, és az esetlegesen csatolt fájl nevét, méretét. A lista megismerését követően a munkáltatói jogkörgyakorló kijelölheti azokat a leveleket, amelyeket a munkavállalónak át kell adnia, aki a kérést csak abban az esetben jogosult megtagadni, ha a levél magánjellegű. A magánjellegű levelek tartalmát a munkáltató nem ismerheti meg. A tilalom ellenére folytatott magánjellegű levelezés esetében ugyanis a levél tartalmának megismerése nem szükséges a munkavállalóval szemben esetlegesen alkalmazandó munkajogi jogkövetkezményekhez. Ilyen levelek törlésére a munkáltatói jogkörgyakorló jogosult felszólítani a munkavállalót, a munkavállaló pedig köteles eleget tenni a felszólításnak

106. § Amennyiben olyan időpontban kellene az e-mail postafiókban tárolt levelek közül a szükséges hivatalos tárgyú leveleket kiválogatni, amikor az érintett munkavállaló tartósan nem tartózkodik a számítógép mellett, az érintett kijelölhet olyan munkavállalót, aki helyette a postafiókba belépve ezt megteheti. Ennek hiányában a közvetlen vezető jelölhet ki két személyt, akik együttes jelenlétük mellett csak a meghatározott, hivatalos tárgyú leveleket menthetik le a postafiókból, a nem hivatalos tárgyú levelek tekintetében azonban titoktartási kötelezettsége áll fenn, annak tartalmát nem adhatják át, arról információt nem közölhetnek a vezetővel, vagy más személlyel.

107. § Amennyiben a munkavállalót felmentik a munkavégzés alól, a felmentés időtartamára, illetve a munkavégzésre irányuló jogviszonya megszűnésétől számított legfeljebb három hónapos időtartamban a munkavállaló e-mail címét a munkavállaló és más munkavállalók számára hozzáférhetetlenné kell tenni (zárolni), valamint olyan

informatikai beállítást kell életbe léptetni, amely a postafiók címre küldött levél feladóját automatikus válaszban arról tájékoztatja, hogy:

- a postafiók használata megszűnt, és
- amennyiben hivatalos tárgyú levelet kíván az Adatkezelő részére megküldeni, azt mely e-mail vagy postacímre teheti meg.

108. § A 107. §-ban deklarált határidő leteltét követően az e-mail postafiók címet inaktívvá kell tenni, vagyis olyan informatikai beállítást kell életbe léptetni, amely megakadályozza, hogy a postafiók további levelet fogadhasson.

109. § A 107. § szerinti tájékoztatásban nem lehet adatot, információt szolgáltatni arról, hogy az e-mail postafiók használata mely okból szűnt meg, illetőleg, hogy az érintett munkavállaló jogviszonya megszűnt-e, ha igen, a megszűnés mely okból történt.

110. § A postafiók hozzáférhetetlenné, illetve inaktívvá tétele mellett tilos olyan beállítás alkalmazása, mely a postafiókba érkező leveleket más e-mail címre továbbítaná.

111. § A munkavállaló számára az utolsó munkában töltött napján – de legkésőbb az attól számított öt munkanapon belül – biztosítani kell, hogy az esetlegesen postafiókjába érkezett esetleges magán jellegű leveleit a postafiókjából lementhesse. E mentést csak akkor kontrolálhatja egy erre kijelölt munkavállaló, ha a jogviszony megszűnésének oka azt indokolja. Ebben az esetben a kijelölt munkavállalót titoktartási kötelezettség terheli a tudomására jutott magánjellegű adatok tekintetében.

112. § Ha a postafiók olyan jellegű hivatalos levelezést tartalmaz, amely a későbbi feladatok ellátása tekintetében szükséges lehet, és a dokumentumok lementése az Adatkezelő részére aránytalan nehézséget okoz, akkor a magánjellegű adatok lementését és végleges eltávolítását követően a postafiók tovább működtethető, melyről az érintett munkavállalót is tájékoztatni kell. A postafiókban a továbbiakban csak hivatalos tárgyú levelek kezelhetők.

### IX.4.4. A munkavállalók rendelkezésére bocsátott internethasználatnak és ellenőrzésének adatvédelmi szabályai

113. § A munkavállalók rendelkezésére bocsátott internet kapcsolat célja elsődlegesen a hatékony munkavégzés elősegítése, emellett a szolgáltatás magán célú használata – az Adatkezelő üzleti érdekeinek, jó hírnevének sérelme, valamint az informatikai rendszer kapacitásainak aránytalan korlátozása nélkül – megengedett.

114. Az Adatkezelő informatikai rendszereinek üzembiztos működéséért felelős szakértője jogosult az internet felhasználást korlátozni, és meghatározni azokat a kulcsszavakat, amelyeket tartalmazó weboldalak megnyitását az informatikai rendszer automatikusan elutasít. Ezen szabályokat a vonatkozó belső szabályzat tartalmazza.

115. § Amennyiben megalapozottan vélelmezhető, hogy a munkavállaló az internet kapcsolatot a fenti szabályok megsértésével használja, a munkáltatói jogkörgyakorló a

szabályszegés körülményeit fő szabály szerint személyes elbeszélgetés útján köteles tisztázni.

116. § Amennyiben a 115. §-ban foglalt eljárás nem vezetne eredményre, a munkáltató kérheti az informatikáért felelős szakértők bevonását azzal, hogy az érintett munkavállaló számítógépén megnyitott weboldalak listáját a munkáltató részére adják át. Ebben az esetben az adatkezelés jogalapját a munkáltató jogos érdeke képezi, amely a munkáltató által elvégzett érdekmérlegelési teszten alapul. A munkáltató listát fő szabály szerint az érintett munkavállaló jelenlétében jogosult ellenőrizni, és a nem hivatalos jellegű adatokat csak a szükséges mértékben és ideig kezelheti, azzal, hogy azokat részleteiben nem ismerheti meg, nem kezelheti, pusztán az esetleges munkajogi következmények megállapításához szükséges mértékben jogosult az adatokat észrevételezni.

### IX.4.5. A munkavállaló munkaállomásának ellenőrzése

117. § Azt a területet, ahol a munkavállaló dolgozik – így például az íróasztalának fiókját – munkaügyi célból nem lehet ellenőrizni. Amennyiben egyéb célból az ellenőrzés szükségessége felmerül, úgy azt csak abban az esetben lehet megtenni, ha a vonatkozó jogszabályi rendelkezések azt lehetővé teszik, és ezt az adatvédelmi felelős előzőleg jóváhagyta. A munkavállalót minden esetben teljeskörűn tájékoztatni kell előzetesen az ellenőrzéssel kapcsolatban megvalósuló adatkezelésről.

### IX.4.6. Elektronikus megfigyelőrendszer alkalmazása

118. § Amennyiben az Adatkezelő a munkáltatói ellenőrzés körében elektronikus megfigyelőrendszert kíván alkalmazni, az erre vonatkozó rendelkezéseket külön dokumentumban kell megfogalmaznia. Az ellenőrzéshez fűződő legitim érdek mérlegelése során tekintettel kell lenni az alábbi adatkezelési korlátokra:

a) a munkáltatói ellenőrzés akkor tekinthető jogszerűnek, amennyiben a munkaviszony rendeltetésével közvetlenül összefüggő okból feltétlenül szükséges,
b) a munkáltatói ellenőrzés és az annak során alkalmazott eszközök, módszerek nem járhatnak az emberi méltóság megsértésével, illetőleg a munkavállalók magánélete nem ellenőrizhető,
c) a munkavállalókat előzetesen tájékoztatni kell az adatkezelés lényeges körülményeiről,
d) az Adatkezelő köteles a jogszerűség, a tisztességes eljárás és átláthatóság, valamint a célhoz kötöttség elveit az adatkezelés során betartani.

## X. ZÁRÓ RENDELKEZÉSEK

119. § Jelen Szabályzat 2020.11.02. napjától kezdve visszavonásig hatályos.

*1. számú melléklet*

# A vonatkozó jogszabályok

A Tájékoztató kialakítása során az Adatkezelő figyelembe vette a vonatkozó hatályos jogszabályokat, illetve a fontosabb nemzetközi ajánlásokat, különös tekintettel az alábbiakra:

- 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 szóló, 2016. április 27-i 2016/679/EU európai parlamenti és tanácsi rendelet (GDPR);

- az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény 2011. évi CXII. törvény (Infotv.);

- a Munka Törvénykönyvéről szóló 2012. évi I. törvény;

- a Polgári Törvénykönyvről szóló 2013. évi V. törvény;

- a polgári perrendtartásról szóló 2016. évi CXXX. törvény.