



Magyar Agrár-, Élelmiszergazdasági és Vidékfejlesztési Kamara

Adatvédelmi és adatkezelési szabályzata

Dokumentum felelősenek aláírása:

Dokumentum felelőse és beosztása: dr. Dubalar Alekszej Valerjevics
adatvédelmi tisztségviselő

A szabályzat első kiadásának
időpontja: 2014. február 19.

Jóváhagyás időpontja: 2018. május 25.

Jóváhagyó aláírása:

Jóváhagyó neve és beosztása: Darabos Tamás főigazgató

Hatálybalépés dátuma: 2018. május 25.

Tartalomjegyzék

1. A szabályzat célja	3
2. A szabályzat hatálya	3
3. Fogalomtár	3
4. Adatvédelmi alapelvek	6
5. Adatkezelési jogszerűsége, adatkezelési jogalapok	6
6. Az érintett tájékoztatására vonatkozó kötelezettség	8
7. Az érintett kérelmének kezelése és az érintett hozzáférési joga	10
8. Az érintett egyes jogai	12
9. Az adatkezelő kötelességei, beépített és alapértelmezett adatvédelem	14
10. Az adatfeldolgozó igénybevételeire vonatkozó szabályok	16
11. Az adatkezelések nyilvántartása	17
12. Adatbiztonság és az adatvédelmi incidensek kezelése	18
13. Adatvédelmi hatásvizsgálat	21
14. Adatvédelmi tisztségviselő kijelölése, jogállása és feladatai	22
15. Személyes adatok harmadik országokba vagy nemzetközi szervezetek részére történő továbbítása	23
16. Személyes adatokkal, adatvédelmi jogviszonnyal kapcsolatos jogorvoslatok	23

Verziószám	Hatálybalépés dátuma	Módosítás
1.0	2014.02.19.	Első kiadás
2.0	2018. 05.	Második (GDPR kompatibilis) kiadás

1. A szabályzat célja

(1) Jelen szabályzat célja Magyarország Alaptörvényének VI. cikk (2) bekezdésében foglalt, személyes adatok védelméhez fűződő alapjog (a továbbiakban: információs önrendelkezési jog) érvényesülése.

(2) Jelen szabályzat célja a személyes adatok védelmét biztosító hazai és uniós jogi normáknak, így mindenekelőtt az információs önrendelkezési jogról és információszabadságról szóló 2011. évi CXII. törvénynek (a továbbiakban: Infotv.), és az EURÓPAI PARLAMENT ÉS A TANÁCS 2016. április 27-i (EU) 2016/679 RENDELETÉNEK (a továbbiakban: GDPR) való megfelelés.

(3) Jelen szabályzat célja az, hogy a szabályzat publikálásával az érintettek a személyes adataik kezelésével kapcsolatosan a legalapvetőbb tájékoztatást megkapják.

(4) Jelen szabályzat célja az, hogy a Nemzeti Agrárgazdasági Kamara (a továbbiakban: NAK) és az általa ellenőrzött gazdasági társaságok az (1)-(3) bekezdésekben foglalt célokat, az információs önrendelkezési jog megfelelő szintű védelmét (a továbbiakban: adatvédelem), szabályozási környezetükkel, munkatársaik és egyéb közreműködőjük normakövető magatartásaival biztosítsák.

2. A szabályzat hatálya

(1) Jelen szabályzat jóváhagyásának időpontjában lép hatályba, azzal egyidejűleg hatályon kívül helyi a Magyar Agrár-, Élelmiszergazdasági és Vidékfejlesztési Kamara adatvédelmi és adatkezelési szabályzatáról rendelkező 4/2014. (II.19.) Főigazgatói utasítást.

(2) Jelen szabályzat személyi hatálya kiterjed a NAK és az általa ellenőrzött gazdasági társaságok munkavállalóira, választott tisztségviselőire és a személyes adatok kezelésében vagy feldolgozásában részt vevő szerződéses partnerekre.

(3) Jelen szabályzat tárgyi hatálya szerint, jelen szabályzat alkalmazandó NAK és a többségi tulajdonában álló gazdasági társaságok valamennyi személyes adatot érintő adatkezelésére. Ahol jelen szabályzat általánosságban adatkezelői kötelezettséget ír elő, ott az adatkezelői kötelezettség címzettje a NAK és a többségi tulajdonában álló gazdasági társaságok, valamint a velük kapcsolatban álló más adatkezelők (szerződéses partnerek).

3. Fogalomtár

E szabályzat alkalmazásában:

1. „személyes adat”: azonosított vagy azonosítható természetes személyre („érintett”) vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható;

2. „különleges személyes adat”: a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a természetes személyek egyedi azonosítását célzó genetikai és biometrikus adatok,

az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok;

3. „adatkezelés”: a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés;

4. „az adatkezelés korlátozása”: a tárolt személyes adatok megjelölése jövőbeli kezelésük korlátozása céljából;

5. „profilalkotás”: személyes adatok automatizált kezelésének bármely olyan formája, amelynek során a személyes adatokat valamely természetes személyhez fűződő bizonyos személyes jellemzők értékelésére, különösen a munkahelyi teljesítményhez, gazdasági helyzetéhez, egészségi állapothoz, személyes preferenciákhoz, érdeklődéshez, megbízhatósághoz, viselkedéshez, tartózkodási helyhez vagy mozgáshoz kapcsolódó jellemzők elemzésére vagy előrejelzésére használják;

6. „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;

7. „nyilvántartási rendszer”: a személyes adatok bármely módon - centralizált, decentralizált vagy funkcionális vagy földrajzi szempontok szerint - tagolt állománya, amely meghatározott ismérvek alapján hozzáférhető;

8. „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; ha az adatkezelés céljait és eszközeit az uniós vagy a tagállami jog határozza meg, az adatkezelőt vagy az adatkezelő kijelölésére vonatkozó különös szempontokat az uniós vagy a tagállami jog is meghatározhatja;

9. „adatfeldolgozó”: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel;

10. „címezett”: 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 címezettnek; az említett adatok e közhatalmi szervek általi kezelése meg kell, hogy feleljen az adatkezelés céljainak megfelelően az alkalmazandó adatvédelmi szabályoknak;

11. „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;

12. „az érintett hozzájárulása”: az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel az érintett nyilatkozik vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez;

13. „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;

14. „genetikai adat”: egy természetes személy örökölt vagy szerzett genetikai jellemzőire vonatkozó minden olyan személyes adat, amely az adott személy fiziológiájára vagy egészségi állapotára vonatkozó egyedi információt hordoz, és amely elsősorban az említett természetes személyből vett biológiai minta elemzéséből ered;

15. „biometrikus adat”: egy természetes személy testi, fiziológiai vagy viselkedési jellemzőire vonatkozó minden olyan sajátos technikai eljárásokkal nyert személyes adat, amely

lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását, ^{Verzió: 2.0} ilyen például az arckép vagy a daktiloszkópiai adat;

16. „egészségügyi adat”: egy természetes személy testi vagy pszichikai egészségi állapotára vonatkozó személyes adat, ideértve a természetes személy számára nyújtott egészségügyi szolgáltatásokra vonatkozó olyan adatot is, amely információt hordoz a természetes személy egészségi állapotáról;

17. „tevékenységi központ”:

a) az egynél több tagállamban tevékenységi hellyel rendelkező adatkezelő esetében az Unión belüli központi ügyvitelének helye, ha azonban a személyes adatok kezelésének céljaira és eszközeire vonatkozó döntéseket az adatkezelő egy Unión belüli másik tevékenységi helyén hozzák, és az utóbbi tevékenységi hely rendelkezik hatáskörrel az említett döntések végrehajtására, az említett döntéseket meghozó tevékenységi helyet kell tevékenységi központnak tekinteni;

b) az egynél több tagállamban tevékenységi hellyel rendelkező adatfeldolgozó esetében az Unión belüli központi ügyvitelének helye, vagy ha az adatfeldolgozó az Unióban nem rendelkezik központi ügyviteli hellyel, akkor az adatfeldolgozónak az az Unión belüli tevékenységi helye, ahol az adatfeldolgozó tevékenységi helyén folytatott tevékenységekkel összefüggésben végzett fő adatkezelési tevékenységek zajlanak, amennyiben az adatfeldolgozóra e rendelet szerint meghatározott kötelezettségek vonatkoznak;

18. „képviselő”: az az Unióban tevékenységi hellyel, illetve lakóhellyel rendelkező és az adatkezelő vagy adatfeldolgozó által a 27. cikk alapján írásban megjelölt természetes vagy jogi személy, aki, illetve amely az adatkezelőt vagy adatfeldolgozót képviseli az adatkezelőre vagy adatfeldolgozóra az e rendelet értelmében háruló kötelezettségek vonatkozásában;

19. „vállalkozás”: gazdasági tevékenységet folytató természetes vagy jogi személy, függetlenül a jogi formájától, ideértve a rendszeres gazdasági tevékenységet folytató személyegyesítő társaságokat és egyesületeket is;

20. „vállalkozáscsoport”: az ellenőrző vállalkozás és az általa ellenőrzött vállalkozások;

21. „kötelező erejű vállalati szabályok”: a személyes adatok védelmére vonatkozó szabályzat, amelyet az Unió valamely tagállamának területén tevékenységi hellyel rendelkező adatkezelő vagy adatfeldolgozó egy vagy több harmadik országban a személyes adatoknak az ugyanazon vállalkozáscsoporton vagy közös gazdasági tevékenységet folytató vállalkozások ugyanazon csoportján belüli adatkezelő vagy adatfeldolgozó részéről történő továbbítása vagy ilyen továbbítások sorozata tekintetében követ;

22. „felügyeleti hatóság”: egy tagállam által az 51. cikknek megfelelően létrehozott független közhatalmi szerv;

23. „érintett felügyeleti hatóság”: az a felügyeleti hatóság, amelyet a személyes adatok kezelése a következő okok valamelyike alapján érint:

a) az adatkezelő vagy az adatfeldolgozó az említett felügyeleti hatóság tagállamának területén rendelkezik tevékenységi hellyel;

b) az adatkezelés jelentős mértékben érinti vagy valószínűsíthetően jelentős mértékben érinti a felügyeleti hatóság tagállamában lakóhellyel rendelkező érintetteket; vagy

c) panaszt nyújtottak be az említett felügyeleti hatósághoz;

24. „személyes adatok határokon átnyúló adatkezelése”:

a) személyes adatoknak az Unióban megvalósuló olyan kezelése, amelyre az egynél több tagállamban tevékenységi hellyel rendelkező adatkezelő vagy adatfeldolgozó több tagállamban található tevékenységi helyein folytatott tevékenységekkel összefüggésben kerül sor; vagy

b) személyes adatoknak az Unióban megvalósuló olyan kezelése, amelyre az adatkezelő vagy az adatfeldolgozó egyetlen tevékenységi helyén folytatott tevékenységekkel összefüggésben kerül sor úgy, hogy egynél több tagállamban jelentős mértékben érint vagy valószínűsíthetően jelentős mértékben érint érintetteket;

25. „releváns és megalapozott kifogás”: a döntéstervezettel szemben benyújtott, azzal kapcsolatos kifogás, hogy ezt a rendeletet megsértették-e, illetve hogy az adatkezelőre vagy az adatfeldolgozóra vonatkozó tervezett intézkedés összhangban van-e a rendelettel; a kifogásban egyértelműen be kell mutatni a döntéstervezet által az érintettek alapvető jogaira és szabadságaira, valamint adott esetben a személyes adatok Unión belüli szabad áramlására jelentett kockázatok jelentőségét;

26. „Közvetlen üzletszerzés” (direkt marketing): azoknak a közvetlen megkeresés módszerével végzett, tájékoztató tevékenységeknek és kiegészítő szolgáltatásoknak az összessége, amelyeknek célja termékek vagy szolgáltatások értékesítésével, szolgáltatásával vagy eladásösztönzésével közvetlen kapcsolatban álló, a gazdasági reklámtevékenység alapvető feltételeiről és egyes korlátairól szóló 2008. évi XLVIII. törvény (a továbbiakban: Grt.) 3. §-ának d) pontja szerinti reklám továbbítása a fogyasztók vagy kereskedelmi partnerek (a továbbiakban együtt: ügyfelek) részére.

4. Adatvédelmi alapelvek

(1) A **Jogszerűség elve** szerint; személyes adat kizárólag az arra vonatkozó jogi felhatalmazás, azaz jogalap mellett kezelhető.

(2) A **Tisztességes eljárás és átláthatóság elve szerint**; személyes adat kezelése kizárólag tisztességes és átlátható eljárás keretében valósulhat meg.

(3) A **Célhoz kötöttség elve** szerint; személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból valósulhat meg. Az adatkezelési célokkal össze nem egyeztethető módon adatkezelés nem megengedett.

(4) A **Pontosság kötöttség elve** szerint; a személyes adatoknak pontosnak és szükség esetén naprakésznek kell lenniük; az adatkezelőnek minden észszerű intézkedést meg kell tennie annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul töröljék vagy helyesbítsék.

(5) A **Korlátozott tárolhatóság elve** szerint; a személyes adatok tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé.

(6) Az **Integritás és bizalmas jelleg elve** szerint; a személyes adatok kezelését oly módon kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve.

(7) Az **Elszámoltathatóság elve** szerint; az adatkezelő felelős az (1)-(6) bekezdésekben foglalt elveknek való megfelelésért, továbbá képesnek kell lennie e megfelelés igazolására.

5. Adatkezelési jogszerűsége, adatkezelési jogalapok

(1) 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 (*hozzájáruláson alapuló adatkezelés*);
- 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 (*szerződéses adatkezelés*);
- c. az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges (*jogi kötelezettségen alapuló adatkezelés*);
- d. az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges (*létfontosságú érdeken alapuló adatkezelés*);

- e. az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges (közérdekű adatkezelés);
 - 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 (*jogos érdeken alapuló adatkezelés*).
- (2) Ha az adatkezelés hozzájáruláson alapul, az adatkezelőnek képesnek kell lennie annak igazolására, hogy az érintett személyes adatainak kezeléséhez hozzájárult.
- (3) Ha az érintett hozzájárulását olyan írásbeli nyilatkozat keretében adja meg, amely más ügyekre is vonatkozik, a hozzájárulás iránti kérelmet ezektől a más ügyektől egyértelműen megkülönböztethető módon kell előadni, érthető és könnyen hozzáférhető formában, világos és egyszerű nyelvezettel.
- (4) Az érintett jogosult arra, hogy hozzájárulását bármikor visszavonja. A hozzájárulás visszavonása nem érinti a hozzájáruláson alapuló, a visszavonás előtti adatkezelés jogszerűségét. A hozzájárulás megadása előtt az érintettet erről tájékoztatni kell. A hozzájárulás visszavonását ugyanolyan egyszerű módon kell lehetővé tenni, mint annak megadását. Hozzájáruláson alapuló adatkezelés esetén a hozzájárulás visszavonása nem zárja ki azt, hogy a személyes adatot az adatkezelő más jogalapon tovább kezelje, feltéve, hogy a más jogalapon történő adatkezelést megfelel az adatvédelmi elveknek, arról az érintett megfelelő tájékoztatást kapott.
- (5) Annak megállapítása során, hogy a hozzájárulás önkéntes-e, a lehető legnagyobb mértékben figyelembe kell venni azt a tényt, egyebek mellett, hogy a szerződés teljesítésének - beleértve a szolgáltatások nyújtását is - feltételül szabták-e az olyan személyes adatok kezeléséhez való hozzájárulást, amelyek nem szükségesek a szerződés teljesítéséhez.
- (6) Különleges személyes adatok kezelése tilos, leszámítva, ha:
- a. az érintett kifejezett hozzájárulását adta az adatok egy vagy több konkrét célból történő kezeléséhez;
 - b. az adatkezelés az adatkezelőnek vagy az érintettnek a foglalkoztatást, valamint a szociális biztonságot és szociális védelmet szabályozó jogszabályból fakadó kötelezettségei teljesítése és konkrét jogai gyakorlása érdekében szükséges;
 - c. az adatkezelés az érintett vagy más természetes személy létfontosságú érdekeinek védelméhez szükséges, ha az érintett fizikai vagy jogi cselekvőképtelensége folytán nem képes a hozzájárulását megadni;
 - d. az adatkezelés valamely politikai, világnézeti, vallási vagy szakszervezeti célú alapítvány, egyesület vagy bármely más nonprofit szervezet megfelelő garanciák mellett végzett jogszerű tevékenysége keretében történik, azzal a feltétellel, hogy az adatkezelés kizárólag az ilyen szerv jelenlegi vagy volt tagjaira, vagy olyan személyekre vonatkozik, akik a szervezettel rendszeres kapcsolatban állnak a szervezet céljaihoz kapcsolódóan, és hogy a személyes adatokat az érintettek hozzájárulása nélkül nem teszik hozzáférhetővé a szervezeten kívüli személyek számára;
 - e. az adatkezelés olyan személyes adatokra vonatkozik, amelyeket az érintett kifejezetten nyilvánosságra hozott;
 - f. az adatkezelés jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez szükséges, vagy amikor a bíróságok igazságszolgáltatási feladatkörükben járnak el;
 - g. az adatkezelés jogszabály alapján jelentős közérdek miatt szükséges;

- h. az adatkezelés megelőző egészségügyi vagy munkahelyi egészségügyi célokból, a munkavállaló munkavégzési képességének felmérése, orvosi diagnózis felállítása, egészségügyi vagy szociális ellátás vagy kezelés nyújtása, illetve egészségügyi vagy szociális rendszerek és szolgáltatások irányítása érdekében szükséges, uniós vagy tagállami jog alapján vagy egészségügyi szakemberrel kötött szerződés értelmében, továbbá a (7) bekezdésben említett feltételekre és garanciákra figyelemmel;
- i. az adatkezelés a népegészségügy területét érintő olyan közérdekből szükséges, mint a határokon át terjedő súlyos egészségügyi veszélyekkel szembeni védelem vagy az egészségügyi ellátás, a gyógyszerek és az orvostechikai eszközök magas színvonalának és biztonságának a biztosítása, és olyan uniós vagy tagállami jog alapján történik, amely megfelelő és konkrét intézkedésekről rendelkezik az érintett jogait és szabadságait védő garanciákra, és különösen a szakmai titoktartásra vonatkozóan;
- j. az adatkezelés a GDPR 89. cikk (1) bekezdésével összhangban a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból szükséges olyan uniós 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.

(7) Különleges személyes adatokat abban az esetben lehet a (6) bekezdés h) pontjában említett célokból kezelni, ha ezen adatok kezelése olyan szakember által vagy olyan szakember felelőssége mellett történik, aki jogszabályban vagy hatósági határozatban meghatározott szakmai titoktartási kötelezettség hatálya alatt áll.

(8) Ha azok a célok, amelyekből az adatkezelő a személyes adatokat kezeli, nem vagy már nem teszik szükségessé az érintettnek az adatkezelő általi azonosítását, az adatkezelő nem köteles kiegészítő információkat megőrizni, beszerezni vagy kezelni annak érdekében, hogy pusztán azért azonosítsa az érintettet, hogy megfeleljen a GDPR-nak.

(9) Ha a (8) bekezdésében említett esetekben az adatkezelő bizonyítani tudja, hogy nincs abban a helyzetben, hogy azonosítsa az érintettet, erről lehetőség szerint őt megfelelő módon tájékoztatja. Ilyen esetekben a hozzáférési jog, helyesbítés és törlés, korlátozás-zárolás, adathordozhatósághoz kapcsolódó jog nem alkalmazandó, kivéve, ha az érintett abból a célból, hogy az említett jogait gyakorolja, az azonosítását lehetővé tevő kiegészítő információkat nyújt.

6. Az érintett tájékoztatására vonatkozó kötelezettség

(1) Az adatkezelő megfelelő intézkedéseket hoz annak érdekében, hogy az érintett részére a személyes adatok kezelésére vonatkozó minden lényeges információt, tájékoztatást tömör, átlátható, érthető és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva nyújtsa. Az érintett személyes adatai kezelését érintő proaktív, GDPR 13. és 14. cikke alapján nyújtandó tájékoztatás módjáról jelen fejezet, a kérelemre és különleges esetekben (pl.: adatvédelmi incidens) biztosítandó tájékoztatásról a következő fejezetek rendelkeznek.

(2) A tájékoztatást olyan módon kell megtenni, hogy az adatkezelő bármikor bizonyítani tudja ezen kötelezettségének teljesítését. A tájékoztatási kötelezettség bizonyítását elsősorban az érintett részéről a tájékoztatás megismerését igazoló írásbeli nyilatkozat, vagy a nyilatkozat igazolását biztosító megfelelő informatikai megoldás biztosítja.

(3) A tájékoztatást a személyes adat kezelésével összefüggő írásbeli dokumentumon - valamint a kapcsolattartást illetve nyilatkozattételt szolgáló informatikai felületen - illetve az ezen dokumentumon vagy felületen hivatkozott, az érintett számára elérhető forráson kell biztosítani (pl. weblap, webes alkalmazás). A tájékoztatásnak valamennyi alkalommal kötelezően hivatkoznia kell a <http://www.nak.hu/adatvedelem> címre, ahol a jelen szabályzat,

valamint a személyes adatok védelmével összefüggő egyéb lényeges információk elérhetőek. A <http://www.nak.hu/adatvedelem> címen közzétett jelen szabályzat nem pótolja a konkrét adatkezeléssel összefüggő információk biztosítására vonatkozó kötelező tájékoztatást [lásd 9. fejr. (5) bekezdés].

(4) A tájékoztatást, ha a személyes adatokat az érintettől gyűjtik az adatok megszerzésének időpontjában, ha a személyes adatokat nem az érintettől szerezték meg úgy az alábbiak szerint kell biztosítani:

- a. a személyes adatok kezelésének konkrét körülményeit tekintetbe véve, a személyes adatok megszerzésétől számított észszerű határidőn, de legkésőbb egy hónapon belül;
- b. ha a személyes adatokat az érintettel való kapcsolattartás céljára használják, legalább az érintettel való első kapcsolatfelvétel alkalmával; vagy
- c. ha várhatóan más címzettel is közlik az adatokat, legkésőbb a személyes adatok első alkalommal való közlésekor.

(5) A tájékoztatás keretében a tájékoztatás tartalmazza:

- a. az adatkezelőnek és - ha van ilyen - az adatkezelő képviselőjének a kiléte és elérhetőségei;
- b. az adatvédelmi tisztviselő elérhetőségei,
- c. a személyes adatok tervezett kezelésének célja, valamint az adatkezelés jogalapja;
- d. jogos érdeken alapuló adatkezelés esetén, az adatkezelő vagy harmadik fél jogos érdekei;
- e. adott esetben a személyes adatok címzettjei, illetve a címzettek kategóriái, ha van ilyen;
- f. adott esetben annak ténye, hogy az adatkezelő harmadik országba vagy nemzetközi szervezet részére kívánja továbbítani a személyes adatokat, továbbá a Bizottság megfelelőségi határozatának léte vagy annak hiánya, vagy a GDPR 46. cikkben, a 47. cikkben vagy a 49. cikk (1) bekezdésének második albekezdésében említett adattovábbítás esetén a megfelelő és alkalmas garanciák megjelölése, valamint az azok másolatának megszerzésére szolgáló módokra vagy az azok elérhetőségére való hivatkozás,
- g. a személyes adatok tárolásának időtartama, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjai;
- h. az érintett azon jogáról való kioktatást, hogy az érintett kérelmezheti az adatkezelőtől a rá vonatkozó személyes adatokhoz való hozzáférést, azok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen, valamint az érintett adathordozhatósághoz való jogáról;
- i. hozzájáruláson alapuló adatkezelés esetén a hozzájárulás bármely időpontban történő visszavonásához való jog, amely nem érinti a visszavonás előtt a hozzájárulás alapján végrehajtott adatkezelés jogszerűségét;
- j. a felügyeleti hatósághoz vagy felügyeleti hatóságokhoz címzett panasz benyújtásának jogáról;
- k. a GDPR 22. cikk (1) és (4) bekezdésében említett automatizált döntéshozatal ténye, ideértve a profilalkotást is, valamint legalább ezekben az esetekben az alkalmazott logikára és arra vonatkozóan érthető információk, hogy az ilyen adatkezelés milyen jelentőséggel, és az érintettre nézve milyen várható következményekkel bír;

- l. ha az adatkezelő a személyes adatokon a gyűjtésük céljától eltérő célból további adatkezelést kíván végezni, a további adatkezelést megelőzően tájékoztatnia kell az érintettet erről az eltérő célról és minden releváns kiegészítő információról.
 - m. a személyes adatoknak érintettől történő gyűjtése esetén arról, hogy a személyes adat szolgáltatása jogszabályn vagy szerződéses kötelezettségen alapul vagy szerződés kötésének előfeltétele-e, valamint hogy az érintett köteles-e a személyes adatokat megadni, továbbá hogy milyen lehetséges következményeikkel járhat az adatszolgáltatás elmaradása;
 - n. ha a személyes adatokat nem az érintettől szerezték meg úgy, a személyes adatok forrása és adott esetben az, hogy az adatok nyilvánosan hozzáférhető forrásból származnak-e.
- (6) A személyes adatoknak érintettől történő gyűjtése esetén a fenti tájékoztatásra vonatkozó rendelkezések nem alkalmazandó, ha és amilyen mértékben az érintett már rendelkezik az információkkal.
- (7) Ha a személyes adatokat nem az érintettől szerezték meg, úgy a fenti tájékoztatásra vonatkozó nem kell alkalmazni, ha és amilyen mértékben:
- a. az érintett már rendelkezik az információkkal;
 - b. a szóban forgó információk rendelkezésre bocsátása lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényelne, különösen a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból, vagy amennyiben az e tájékoztatási kötelezettség valószínűsíthetően lehetetlenné tenné vagy komolyan veszélyeztetné ezen adatkezelés céljainak elérését. Ilyen esetekben az adatkezelőnek megfelelő intézkedéseket kell hoznia - az információk nyilvánosan elérhetővé tételét is ideértve - az érintett jogainak, szabadságainak és jogos érdekeinek védelme érdekében;
 - c. az adat megszerzését vagy közlését kifejezetten előírja az adatkezelőre alkalmazandó uniós vagy tagállami jogszabály, amely az érintett jogos érdekeinek védelmét szolgáló megfelelő intézkedésekről rendelkezik; vagy
 - d. a személyes adatoknak valamely uniós vagy tagállami jogszabályban előírt szakmai titoktartási kötelezettség alapján, ideértve a jogszabályon alapuló titoktartási kötelezettséget is, bizalmasnak kell maradnia.

7. Az érintett kérelmének kezelése és az érintett hozzáférési joga

- (1) Az adatkezelő elősegíti az érintett jogainak gyakorlását és ennek érdekében az érintett által kért tájékoztatást írásban vagy más módon - ideértve adott esetben az elektronikus utat is - megadja. Az érintett kérésére szóbeli tájékoztatás is megadható, feltéve, hogy más módon igazolták az érintett személyazonosságát.
- (2) Az adatkezelő kizárólag abban az esetben tagadhatja meg az érintett tájékoztatását, amennyiben bizonyítja, hogy az érintett azonosítása nem állt módjában.
- (3) Az adatkezelő az érintett kérelmével összefüggő intézkedésektől indokolatlan késedelem nélkül, legfeljebb azonban a kérelem beérkezésétől számított egy hónapon belül tájékoztatja az érintettet. Szükség esetén, figyelembe véve a kérelem összetettségét és a kérelmek számát, ez a határidő további két hónappal meghosszabbítható. A határidő meghosszabbításáról az adatkezelő a késedelem okainak megjelölésével a kérelem kézhezvételétől számított egy hónapon belül tájékoztatja az érintettet. Ha az érintett elektronikus úton nyújtotta be a kérelmet, a tájékoztatást lehetőség szerint elektronikus úton kell megadni, kivéve, ha az érintett azt másként kéri.

(4) Ha az adatkezelő nem tesz intézkedéseket az érintett kérelme nyomán, késedelem nélkül, de legkésőbb a kérelem beérkezésétől számított egy hónapon belül tájékoztatja az érintettet az intézkedés elmaradásának okairól, valamint arról, hogy az érintett panaszt nyújthat be valamely felügyeleti hatóságnál, és élhet bírósági jogorvoslati jogával.

(5) A kérelem ügyintézését a (6) bekezdésben foglalt esetet leszámítva díjmentesen kell biztosítani.

(6) Ha az érintett kérelme egyértelműen megalapozatlan vagy - különösen ismétlődő jellege miatt - túlzó, az adatkezelő, figyelemmel a kért információ vagy tájékoztatás nyújtásával vagy a kért intézkedés meghozatalával járó adminisztratív költségekre:

- a. észszerű összegű díjat számíthat fel, vagy
- b. megtagadhatja a kérelem alapján történő intézkedést.

(7) A kérelem egyértelműen megalapozatlan vagy túlzó jellegének bizonyítása az adatkezelőt terheli.

(8) A jelen szabályzat 5. fejezet (8)-(9) bekezdésében foglaltak sérelme nélkül, ha az adatkezelőnek megalapozott kétségei vannak a kérelmet benyújtó természetes személy kilétével kapcsolatban, további, az érintett személyazonosságának megerősítéséhez szükséges információk nyújtását kérheti.

(9) Az érintett jogosult arra, hogy az adatkezelőtől visszajelzést kapjon arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e, és ha ilyen adatkezelés folyamatban van, 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. az 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.
- i. Ha személyes adatoknak harmadik országba vagy nemzetközi szervezet részére történő továbbítására kerül sor, az érintett jogosult arra, hogy tájékoztatást kapjon a továbbításra vonatkozóan a GDPR 46. cikk szerinti megfelelő garanciákról.

(10) Az adatkezelő az adatkezelés tárgyát képező személyes adatok másolatát az érintett rendelkezésére bocsátja. Az érintett által kért további másolatokért az adatkezelő az

adminisztratív költségeken alapuló, észszerű mértékű díjat számíthat fel. Ha az érintett elektronikus úton nyújtotta be a kérelmet, az információkat széles körben használt elektronikus formátumban kell rendelkezésre bocsátani, kivéve, ha az érintett másként kéri. A másolat igénylésére vonatkozó jog nem érintheti hátrányosan mások jogait és szabadságait.

8. Az érintett egyes jogai

(1) Az érintett - *a helyesítéshez való jog alapján* - jogosult arra, hogy kérésére az adatkezelő indokolatlan késedelem nélkül helyesbítse a rá vonatkozó pontatlan személyes adatokat. Figyelembe véve az adatkezelés célját, az érintett jogosult arra, hogy kérje a hiányos személyes adatok - egyebek mellett kiegészítő nyilatkozat útján történő - kiegészítését.

(2) Az érintett - *a törléshez való jog alapján* - jogosult arra, hogy kérésére az adatkezelő indokolatlan késedelem nélkül törölje a rá vonatkozó személyes adatokat, az adatkezelő pedig köteles arra, hogy az érintettre vonatkozó személyes adatokat indokolatlan késedelem nélkül törölje, ha az alábbi indokok 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 jelen fejezet (13) bekezdése alapján tiltakozik az adatkezelése ellen, és nincs elsőbbséget élvező jogszerű ok az adatkezelésre, vagy az érintett jelen fejezet (14) bekezdése alapján tiltakozik az adatkezelés ellen;
- d. a személyes adatokat jogellenesen kezelték;
- e. a személyes adatokat az adatkezelőre alkalmazandó uniós vagy tagállami jogszabályban előírt jogi kötelezettség teljesítéséhez törölni kell;
- f. a személyes adatok gyűjtésére a GDPR 8. cikk (1) bekezdésében említett, gyermekek számára információs társadalommal összefüggő szolgáltatások kínálásával kapcsolatosan került sor.

(3) Ha az adatkezelő nyilvánosságra hozta a személyes adatot, és az (2) bekezdés értelmében azt törölni köteles, az elérhető technológia és a megvalósítás költségeinek figyelembevételével megteszi az észszerűen elvárható lépéseket - ideértve technikai intézkedéseket - annak érdekében, hogy tájékoztassa az adatokat kezelő adatkezelőket, hogy az érintett kérelmezte tőlük a szóban forgó személyes adatokra mutató linkek vagy e személyes adatok másolatának, illetve másodpéldányának törlését.

(4) Az (2) és (3) bekezdés nem alkalmazandó, amennyiben az adatkezelés szükséges:

- a. a véleménynyilvánítás szabadságához és a tájékozódáshoz való jog gyakorlása céljából;
- b. a személyes adatok kezelését előíró, az adatkezelőre alkalmazandó uniós vagy tagállami jogszabály szerinti kötelezettség teljesítése, illetve közérdekből vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlása keretében végzett feladat végrehajtása céljából;
- c. a GDPR 9. cikk (2) bekezdése h) és i) pontjának, valamint a GDPR 9. cikk (3) bekezdésének megfelelően a népegészségügy területét érintő közérdek alapján;
- d. a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból, amennyiben a törléshez való jog valószínűsíthetően lehetetlenné tenné vagy komolyan veszélyeztetné ezt az adatkezelést; vagy

e. jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez.

(5) Az érintett - *az adatkezelés korlátozásához való jog alapján* - jogosult arra, hogy kérésére az adatkezelő korlátozza az adatkezelést, ha az alábbiak valamelyike teljesül:

- a. az érintett vitatja a személyes adatok pontosságát, ez esetben a korlátozás arra az időtartamra vonatkozik, amely lehetővé teszi, hogy az adatkezelő 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 a 21. cikk (1) bekezdése szerint tiltakozott 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.

(6) Ha az adatkezelés az (5) bekezdés alapján 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.

(7) Az adatkezelő az adatkezelés korlátozását kérő érintettet az adatkezelés korlátozásának feloldásáról előzetesen tájékoztatja.

(8) Az adatkezelő minden olyan címzettet tájékoztat a (1), (2), illetve az (5) bekezdés szerinti valamennyi helyesbítésről, törlésről vagy adatkezelés-korlátozásról, akivel, illetve amellyel a személyes adatot közölték, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel. Az érintettet kérésére az adatkezelő tájékoztatja e címzettekről.

(9) Az érintett - *az adatok hordozhatóságához való jog alapján* - jogosult arra, hogy a rá vonatkozó, általa egy adatkezelő rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja, továbbá jogosult arra, hogy ezeket az adatokat egy másik adatkezelőnek továbbítsa anélkül, hogy ezt akadályozná az az adatkezelő, amelynek a személyes adatokat a rendelkezésére bocsátotta, ha:

- a. az adatkezelés hozzájáruláson alapuló adatkezelésnek vagy szerződéses adatkezelésnek minősül; és
- b. az adatkezelés automatizált módon történik.

(10) Az adatok hordozhatóságához való jog (9) bekezdés szerinti gyakorlása során az érintett jogosult arra, hogy - ha ez technikailag megvalósítható - kérje a személyes adatok adatkezelők közötti közvetlen továbbítását.

(11) Az e cikk (9) bekezdésében említett jog gyakorlása nem sértheti a (2)-(4) bekezdésben foglaltakat. Az említett jog nem alkalmazandó abban az esetben, ha az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítványai gyakorlásának keretében végzett feladat végrehajtásához szükséges.

(12) Az (9) bekezdésben említett jog nem érintheti hátrányosan mások jogait és szabadságait.

(13) Az érintett - *a tiltakozáshoz való jog alapján* - jogosult arra, hogy a saját helyzetével kapcsolatos okokból bármikor tiltakozzon személyes adatainak közérdekű adatkezelésén vagy jogos érdeken alapuló kezelése ellen, ideértve az említett rendelkezéseken alapuló

profilalkotást is. Ebben az esetben az adatkezelő a személyes adatokat nem kezelheti tovább, kivéve, ha az adatkezelő 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.

(14) 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.

(15) Ha az érintett tiltakozik a személyes adatok közvetlen üzletszerzés érdekében történő kezelése ellen, akkor a személyes adatok a továbbiakban e célból nem kezelhetők.

(16) Az (13) és (14) bekezdésben említett jogra legkésőbb az érintettel való első kapcsolatfelvétel során kifejezetten fel kell hívni annak figyelmét, és az erre vonatkozó tájékoztatást egyértelműen és minden más információtól elkülönítve kell megjeleníteni.

(17) Az információk társadalommal összefüggő szolgáltatások igénybevételéhez kapcsolódóan és a 2002/58/EK irányelvtől eltérve az érintett a tiltakozáshoz való jogot műszaki előírásokon alapuló automatizált eszközökkel is gyakorolhatja.

(18) Ha a személyes adatok kezelésére a GDPR 89. cikk (1) bekezdésének megfelelően tudományos és történelmi kutatási célból vagy statisztikai célból kerül sor, az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból tiltakozhasson a rá vonatkozó személyes adatok kezelése ellen, kivéve, ha az adatkezelésre közérdekű okból végzett feladat végrehajtása érdekében van szükség.

(19) Az érintett jogosult arra, hogy ne terjedjen ki rá az olyan, kizárólag automatizált adatkezelésen - ideértve a profilalkotást is - alapuló döntés hatálya, amely rá nézve joghatással járna vagy őt hasonlóképpen jelentős mértékben érintené.

(20) Az (19) bekezdés nem alkalmazandó abban az esetben, ha a döntés:

- a. az érintett és az adatkezelő közötti szerződés megkötése vagy teljesítése érdekében szükséges;
- b. meghozatalát az adatkezelőre alkalmazandó olyan uniós vagy tagállami jog teszi lehetővé, amely az érintett jogainak és szabadságainak, valamint jogos érdekeinek védelmét szolgáló megfelelő intézkedéseket is megállapít; vagy
- c. az érintett kifejezett hozzájárulásán alapul.

(21) A (20) bekezdés a) és c) pontjában említett esetekben az adatkezelő köteles megfelelő intézkedéseket tenni az érintett jogainak, szabadságainak és jogos érdekeinek védelme érdekében, ideértve az érintettnek legalább azt a jogát, hogy az adatkezelő részéről emberi beavatkozást kérjen, álláspontját kifejezze, és a döntéssel szemben kifogást nyújtson be.

(22) A (20) bekezdésben említett döntések nem alapulhatnak a különleges személyes adatokon, kivéve, ha az 5. fejezet (2) bekezdésének a) vagy g) pontja alkalmazandó, és az érintett jogainak, szabadságainak és jogos érdekeinek védelme érdekében megfelelő intézkedések megtételére került sor.

9. Az adatkezelő kötelességei, beépített és alapértelmezett adatvédelem

(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 szabályzat

céljaival összhangban történjen. Ezeket az intézkedéseket az adatkezelő felülvizsgálja és szükség esetén naprakésszé teszi.

(2) Az adatkezelő - a *beépített és alapértelmezett adatvédelem* követelményének megfelelően - a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével mind az adatkezelés módjának meghatározásakor, mind pedig az adatkezelés során olyan megfelelő technikai és szervezési intézkedéseket - például álnevesítést - hajt végre, amelyek célja egyrészt az adatvédelmi elvek, például az adattakarékosság hatékony megvalósítása, másrészt az e rendeletben foglalt követelmények teljesítéséhez és az érintettek jogainak védelméhez szükséges garanciák beépítése az adatkezelés folyamatába.

(3) Az adatkezelő - a *beépített és alapértelmezett adatvédelem* követelményének szerint - 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.

(4) Az adatkezelő az adatkezelési tevékenység vonatkozásában arányos belső adatvédelmi szabályokat is alkalmaz. Az adatkezelés műveletek teljességére kiterjedő, általános szabályokat és alapelveket tartalmazó adatvédelmi és adatkezelési szabályzatot - ideértve annak módosítását - az adatvédelmi tisztviselő javaslatára a főigazgató hagyja jóvá.

(5) Az eltérő célú adatkezeléseket az adatvédelmi és adatkezelési szabályzat rendelkezéseit figyelembe vevő folyamatszabályozó eljárásrend szabályozza, továbbá az eltérő célú adatkezelésekhez a 6. fejezetnek megfelelő tájékoztatás kerül kiadmányozásra.

(6) Az eltérő célú adatkezelése vonatkozó eljárásrendnek és tájékoztatónak elkészítéséért felelős személy annak a szervezeti egységnek a vezetője, akinek a munkafolyamata során az adatkezelési művelet meghatározó hányada történik, vagy akinek a munkafolyamata a személyes adatok kezelésére épül. Amennyiben az adott eljárásrend esetében több szervezeti egység illetékessége is fennáll, akkor az eljárásrend előkészítéséért felelős személyt a szervezeti egységeket közvetlenül illetve közvetetten irányító vezető jelöli ki. Az eljárásrend előkészítéséért felelős személy az eljárásrend előkészítése során köteles kikérni az adatvédelmi tisztviselő véleményét.

(7) Az adatkezelő a *beépített és alapértelmezett adatvédelem* követelményének való megfeleléséért részleges bizonyítást szolgálhatja, ha az adatkezelő a GDPR 42. cikk szerinti jóváhagyott tanúsítási mechanizmus.

(8) Ha az adatkezelés céljait és eszközeit két vagy több adatkezelő közösen határozza meg, azok közös adatkezelőknek minősülnek. A közös adatkezelők átlátható módon, a közöttük létrejött megállapodásban határozzák az adatvédelemmel kapcsolatos kötelezettségeikből fakadó feladataikat és az összefüggő felelősségük megoszlását, kivéve azt az esetet és annyiban, ha és amennyiben az adatkezelőkre vonatkozó felelősség megoszlását uniós vagy tagállami jogszabály határozza meg. A megállapodásban az érintettek számára kapcsolattartót jelölhetnek ki.

(9) (8) bekezdésben említett megállapodásnak megfelelően tükröznie kell a közös adatkezelők érintettekkel szembeni szerepét és a velük való kapcsolatukat. A megállapodás lényegét az érintett rendelkezésére kell bocsátani. Az érintett az (8) bekezdésben említett megállapodás feltételeitől függetlenül mindegyik adatkezelő vonatkozásában és mindegyik adatkezelővel szemben gyakorolhatja az e rendelet szerinti jogait.

10. Az adatfeldolgozó igénybevételére vonatkozó szabályok

(1) Ha az adatkezelést az adatkezelő nevében más végzi, az adatkezelő kizárólag olyan adatfeldolgozókat vehet igénybe, akik vagy amelyek megfelelő garanciákat nyújtanak az adatkezelés e rendelet követelményeinek való megfelelését és az érintettek jogainak védelmét biztosító, megfelelő technikai és szervezési intézkedések végrehajtására.

(2) Az adatfeldolgozó az adatkezelő előzetesen írásban tett eseti vagy általános felhatalmazása nélkül további adatfeldolgozót nem vehet igénybe. Az általános írásbeli felhatalmazás esetén az adatfeldolgozó tájékoztatja az adatkezelőt minden olyan tervezett változásról, amely további adatfeldolgozók igénybevételét vagy azok cseréjét érinti, ezzel biztosítva lehetőséget az adatkezelőnek arra, hogy ezekkel a változtatásokkal szemben kifogást emeljen.

(3) Az adatfeldolgozó által végzett adatkezelést az adatkezelés tárgyát, időtartamát, jellegét és célját, a személyes adatok típusát, az érintettek kategóriáit, valamint az adatkezelő kötelezettségeit és jogait meghatározó szerződésben kell szabályoznia. A szerződés vagy szerződést kiegészítő nyilatkozat különösen köteles 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 jogszabály 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 állnak;
- c. meghozza az adatbiztonságra vonatkozó jelen szabályzat 12. fejezetében, valamint a GDPR 32. cikkében előírt intézkedéseket;
- d. tiszteletben tartja a további adatfeldolgozó igénybevételére vonatkozóan a (2) és (6) bekezdésben említett feltételeket;
- e. az adatkezelés jellegének figyelembevételével megfelelő technikai és szervezési intézkedésekkel a lehetséges mértékben segíti az adatkezelőt abban, hogy az adatkezelő teljesíteni tudja az érintett jogainak gyakorlásához kapcsolódó kötelezettségeit (pl. tájékoztatás, kérelmek intézése, hozzáférési jog biztosítása);
- f. segíti az adatkezelőt az adatbiztonsággal, és adatvédelmi incidenssel és hatásvizsgálattal kapcsolatos kötelezettségek 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 az e bekezdésben meghatározott kötelezettségek teljesítésének igazolásához szükséges, továbbá amely lehetővé teszi és elősegíti az adatkezelő által vagy az általa megbízott más ellenőr által végzett ellenőrzéseket, auditokat, beleértve a helyszíni vizsgálatokat is.

(4) A (3) albekezdés h.) pontjával kapcsolatban az adatfeldolgozó haladéktalanul tájékoztatja az adatkezelőt, ha úgy véli, hogy annak valamely utasítása sérti ezt a rendeletet vagy a tagállami vagy uniós adatvédelmi rendelkezéseket.

(5) A (3) bekezdésben foglalt szerződéses nyilatkozatnak megfelel az is, ha a szerződéses nyilatkozatban az adatfeldolgozó a jelen szabályzat, az adatkezelő utasításainak és különösen a jelen szabályzat adatfeldolgozóra vonatkozó rendelkezéseit magára nézve kötelezőnek ismeri el.

(6) Ha az adatfeldolgozó bizonyos, az adatkezelő nevében végzett konkrét adatkezelési tevékenységekhez további adatfeldolgozó szolgáltatásait is igénybe veszi, uniós vagy tagállami jog alapján létrejött szerződés vagy más jogi aktus útján erre a további adatfeldolgozóra is ugyanazok az adatvédelmi kötelezettségeket kell telepíteni, mint amelyek az adatkezelő és az adatfeldolgozó között létrejött, a (3) bekezdésben említett szerződésben vagy szerződéses nyilatkozatban szerepelnek, különösen úgy, hogy a további adatfeldolgozónak megfelelő garanciákat kell nyújtania a megfelelő technikai és szervezési intézkedések végrehajtására, és ezáltal biztosítania kell, hogy az adatkezelés megfeleljen e rendelet követelményeinek. Ha a további adatfeldolgozó nem teljesíti adatvédelmi kötelezettségeit, az őt megbízó adatfeldolgozó teljes felelősséggel tartozik az adatkezelő felé a további adatfeldolgozó kötelezettségeinek a teljesítéséért.

(7) A GDPR 40. cikk szerinti jóváhagyott magatartási kódexekhez vagy a GDPR 42. cikk szerinti jóváhagyott tanúsítási mechanizmushoz való csatlakozás felhasználható annak bizonyítása részeként, hogy az adatfeldolgozó biztosítja az (1) és (6) bekezdésben említett megfelelő garanciákat.

(8) Ha egy adatfeldolgozó e rendeletet sértve maga határozza meg az adatkezelés céljait és eszközeit, akkor őt az adott adatkezelés tekintetében adatkezelőnek kell tekinteni, leszámítva ha a cél bíróság vagy hatóság előtti igényérvényesítés.

(9) Az adatfeldolgozó és bármely, az adatkezelő vagy az adatfeldolgozó irányítása alatt eljáró, a személyes adatokhoz hozzáféréssel rendelkező személy ezeket az adatokat kizárólag az adatkezelő utasításának megfelelően kezelheti, kivéve, ha az ettől való eltérésre őt uniós vagy tagállami jogszabály kötelezi.

11. Az adatkezelések nyilvántartása

(1) Az adatkezelő adatkezelési tevékenységekről nyilvántartást vezet. E nyilvántartás a következő információkat tartalmazza:

- a. az adatkezelő neve és elérhetősége, valamint - ha van ilyen - a közös adatkezelőnek, az adatkezelő képviselőjének és az adatvédelmi tisztviselőnek a neve és elérhetősége;
- b. az adatkezelés céljai;
- c. az érintettek kategóriáinak, valamint a személyes adatok kategóriáinak ismertetése;
- d. olyan címzettek kategóriái, akikkel a személyes adatokat közlik vagy közölni fogják, ideértve a harmadik országbeli címzetteket vagy nemzetközi szervezeteket;
- e. adott esetben a személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk, beleértve a harmadik ország vagy a nemzetközi szervezet azonosítását, valamint a GDPR 49. cikk (1) bekezdésének második albekezdés szerinti továbbítás esetében a megfelelő garanciák leírása;
- f. ha lehetséges, a különböző adatkategóriák törlésére előírányzott határidők;
- g. ha lehetséges, az adatbiztonsági intézkedések általános leírása.

(2) Az adatfeldolgozó nyilvántartást vezet az adatkezelő nevében végzett adatkezelési tevékenységek minden kategóriájáról; a nyilvántartás a következő információkat tartalmazza:

- a. az adatfeldolgozó vagy adatfeldolgozók neve és elérhetőségei, és minden olyan adatkezelő neve és elérhetőségei, amelynek vagy akinek a nevében az adatfeldolgozó eljár, továbbá - ha van ilyen - az adatkezelő vagy az adatfeldolgozó képviselőjének, valamint az adatvédelmi tisztviselőnek a neve és elérhetőségei;
- b. az egyes adatkezelők nevében végzett adatkezelési tevékenységek kategóriái;
- c. adott esetben a személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítása, beleértve a harmadik ország vagy a nemzetközi szervezet azonosítását, valamint a GDPR 49. cikk (1) bekezdésének második albekezdés szerinti továbbítás esetében a megfelelő garanciák leírása;
- d. ha lehetséges, az adatbiztonsági intézkedések általános leírása.

(3) Az (1) és (2) bekezdésben említett nyilvántartást írásban kell vezetni, ideértve az elektronikus formátumot is.

(4) Az adatkezelő vagy az adatfeldolgozó megkeresés alapján a felügyeleti hatóság részére rendelkezésére bocsátja a nyilvántartást.

(5) Az (1) és (2) bekezdésben foglalt kötelezettségek nem vonatkoznak a 250 főnél kevesebb személyt foglalkoztató vállalkozásra vagy szervezetre, kivéve, ha az általa végzett adatkezelés az érintettek jogaira és szabadságaira nézve valószínűsíthetően kockázattal jár, ha az adatkezelés nem alkalmi jellegű, vagy ha az adatkezelés kiterjed a különleges személyes adatok kezelésére. Amennyiben a NAK többségi tulajdonában álló gazdasági társaság a NAK tagjegyzékében szereplő vagy hatósági ügyintézővel összefüggő személyes adatokat kezel vagy ilyen adatok tekintetében adatfeldolgozóként eljár, úgy az (1) és a (2) bekezdésben foglalt kötelezettségek alóli mentesség esetében nem alkalmazandó.

(6) Az adatkezelő adatkezelési nyilvántartását a NAK Szervezeti és Működési Szabályzata szerint az Informatikai Igazgatóság vezeti (a továbbiakban: az adatkezelési nyilvántartás vezetéséért felelős szervezeti egység). Az adatkezelési nyilvántartáshoz az adatvédelmi tisztviselő számára folyamatos hozzáférést kell biztosítani.

(7) Az adatkezelési nyilvántartáshoz a 9. fejezet (6) bekezdése szerinti, eltérő célú adatkezelése vonatkozó eljárásrend elkészítéséért felelős személy megfelelő információkat biztosít. A megfelelő információátadás és együttműködés kialakítása érdekében az adatkezelési nyilvántartás vezetéséért felelős szervezeti egység vezetője folyamatszabályozó eljárásrendet készít elő.

(8) Az Informatikai Igazgatóság az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény (a továbbiakban: Eütv.) 54. §-a szerint olyan adattovábbítási nyilvántartást köteles vezetni, amely biztosítja, hogy az ügyfél elektronikus úton, legfeljebb 3 napon belül tájékoztatást tudjon szerezni arról, hogy mely adatait mely Eütv. szerinti együttműködő szerv, milyen célból és milyen időpontban vette át.

12. Adatbiztonság és az adatvédelmi incidensek kezelése

(1) Az adatkezelő és az adatfeldolgozó a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja, ideértve, többek között, adott esetben:

- a. a személyes adatok álnevesítését és titkosítását;

- b. a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítását, integritását, rendelkezésre állását és ellenálló képességét;
- 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.

(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 hozzáférésekből erednek.

(3) Az adatkezelő, illetve az adatfeldolgozó GDPR 40. cikk szerinti jóváhagyott magatartási kódexekhez vagy a GDPR 42. cikk szerinti jóváhagyott tanúsítási mechanizmushoz való csatlakozását felhasználhatja annak bizonyítása részeként, hogy az e bekezdés (1) bekezdésében meghatározott követelményeket teljesíti.

(4) 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 jogszabály kötelezi őket.

(5) Az adatkezelő informatikai rendszereinek adatbiztonságát az Informatikai Igazgatóság az Informatikai Biztonsági Szabályzatában (a továbbiakban: IBSZ) foglaltaknak megfelelően biztosítja. Az IBSZ publikus szabályainak, valamint az Informatikai Igazgatóság információbiztonsággal kapcsolatos egyéb útmutatóját minden a 2. fejezet (2) bekezdésében említett valamennyi személy köteles betartani. Az informatikai rendszereinek adatbiztonsága során biztosítani kell az Eütv., az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.), valamint végrehajtási rendeleteinek szükség szerinti betartását. Az Eütv. és az Ibtv. tekintetében, kétség esetén, konzultáció kezdeményezendő az illetékes hatóságokkal.

(6) A nyomtatott dokumentumokon fellelhető adatok biztonságát a 2. fejezet (2) bekezdésében említett valamennyi személy a jelen szabályzat, az iratkezelési szabályzat alapján különösen gondossággal köteles biztosítani.

(7) Az adatvédelmi incidenst az adatkezelő indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, az adatvédelmi tisztviselő útján bejelenti az illetékes felügyeleti hatóságnak, kivéve, ha az adatvédelmi incidens az adatvédelmi tisztviselő szerint valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Ha a bejelentés nem történik meg 72 órán belül, mellékelni kell hozzá a késedelem igazolására szolgáló indokokat is.

(8) Az adatvédelmi incidenst 2. fejezet (2) bekezdésében említett valamennyi személy haladéktalanul köteles jelezni az adatvédelmi tisztviselő számára. A 2. fejezet (2) bekezdésében említett valamennyi személy soron kívül köteles az adatvédelmi incidenssel összefüggő valamennyi lényeges és által ismert információt adatvédelmi tisztviselő számára megadni.

(9) Az adatfeldolgozó az adatvédelmi incidenst, az arról való tudomásszerzést követően indokolatlan késedelem nélkül bejelenti az adatkezelőnek.

(10) Az (7) bekezdésben említett bejelentésben legalább:

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

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

(12) Az adatkezelő adatvédelmi tisztviselője nyilvántartja az adatvédelmi incidenseket, feltüntetve az adatvédelmi incidenshez kapcsolódó tényeket, annak hatásait és az orvoslására tett intézkedéseket. E nyilvántartás lehetővé teszi, hogy a felügyeleti hatóság ellenőrizze az e cikk követelményeinek való megfelelést.

(13) Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatkezelő adatvédelmi tisztviselője útján indokolatlan késedelem nélkül tájékoztatja az érintettet az adatvédelmi incidensről.

(14) Az (13) bekezdésben említett, az érintett részére adott tájékoztatásban világosan és közérthetően ismertetni kell az adatvédelmi incidens jellegét, és közölni kell legalább a (10) bekezdés b), c) és d) pontjában említett információkat és intézkedéseket.

(15) Az érintettet nem kell az (13) bekezdésben említettek szerint tájékoztatni, ha az adatvédelmi tisztviselő álláspontja szerint a következő feltételek bármelyike teljesül:

- a. az adatkezelő 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. az adatkezelő az adatvédelmi incidenst követően olyan további intézkedéseket tett, amelyek biztosítják, hogy az érintett jogaira és szabadságaira jelentett, az (13) bekezdésben említett 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.

(16) Ha az adatkezelő még nem értesítette az érintettet az adatvédelmi incidensről, a felügyeleti hatóság, miután mérlegelte, hogy az adatvédelmi incidens valószínűsíthetően magas kockázattal jár-e, elrendelheti az érintett tájékoztatását, vagy megállapíthatja a (15) bekezdésben említett feltételek valamelyikének teljesülését.

13. Adatvédelmi hatásvizsgálat

(1) 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 az adatkezelő 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 értékelhetők.

(2) Az adatkezelő az adatvédelmi hatásvizsgálat elvégzésekor az adatvédelmi tisztviselő szakmai tanácsát köteles kikérni.

(3) Az (1) bekezdésben említett 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. különleges személyes adatok kategóriái kezelése; vagy
- c. nyilvános helyek nagymértékű, módszeres megfigyelése.

(4) A felügyeleti hatóság meghatározhat olyan adatkezelési műveleteket, amelyekre vonatkozóan az (1) bekezdés értelmében adatvédelmi hatásvizsgálatot kell végezni.

(5) 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 (1) bekezdésben említett, az érintett jogait és szabadságait érintő kockázatok vizsgálatára; és
- d. a kockázatok kezelését célzó intézkedések bemutatására, ideértve a személyes adatok védelmét és az e rendelettel való összhang igazolását szolgáló, az érintettek és más személyek jogait és jogos érdekeit figyelembe vevő garanciákat, biztonsági intézkedéseket és mechanizmusokat.

(6) Az adatkezelők, illetve adatfeldolgozók által végzett adatkezelési műveletek hatásainak értékelése - különösen az adatvédelmi hatásvizsgálatok - során megfelelően figyelembe kell venni, hogy a szóban forgó adatkezelők, illetve adatfeldolgozók teljesítik-e a GDPR 40. cikkében említett jóváhagyott magatartási kódexek előírásait.

(7) Az adatkezelő szükség szerint, de legalább az adatkezelési műveletek által jelentett kockázat változása esetén ellenőrzést folytat le annak értékelése céljából, hogy a személyes adatok kezelése az adatvédelmi hatásvizsgálatnak megfelelően történik-e.

(8) Ha 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 a GDPR 36. cikke szerint konzultál a felügyeleti hatósággal.

14. Adatvédelmi tisztségviselő kijelölése, jogállása és feladatai

- (1) A NAK főigazgatója jelöli ki a NAK adatvédelmi tisztségviselőjét. A NAK alapítói döntése szerint a kijelölés kiterjedhet a NAK által ellenőrzött gazdasági társaságok tekintetében ellátandó adatvédelmi tisztségviselői feladatokra is, egyébként a NAK által ellenőrzött gazdasági társaságok adatvédelmi tisztségviselőjét az ellenőrzött gazdasági társaság ügyvezetése bízza meg.
- (2) Az adatvédelmi tisztségviselőt szakmai rátermettség és különösen az adatvédelmi jog és gyakorlat szakértői szintű ismerete, valamint a jelen fejezetben foglalt feladatok ellátására való alkalmasság alapján kell kijelölni.
- (3) Az adatvédelmi tisztségviselő az adatkezelő vagy az adatfeldolgozó alkalmazottja lehet, vagy szolgáltatási szerződés keretében láthatja el a feladatait.
- (4) Az adatkezelő vagy az adatfeldolgozó közzéteszi az adatvédelmi tisztségviselő elérhetőségeit, és azokat közli a felügyeleti hatósággal.
- (5) Az adatkezelő és az adatfeldolgozó biztosítja, hogy az adatvédelmi tisztségviselő a személyes adatok védelmével kapcsolatos összes ügybe megfelelő módon és időben bekapcsolódjon.
- (6) Az adatkezelő és az adatfeldolgozó támogatja az adatvédelmi tisztségviselőt a jelen szabályzatban foglalt feladatai ellátásában azáltal, hogy biztosítja számára azokat az forrásokat, amelyek e feladatok végrehajtásához, a személyes adatokhoz és az adatkezelési műveletekhez való hozzáféréshez, valamint az adatvédelmi tisztségviselő szakértői szintű ismereteinek fenntartásához szükségesek.
- (7) Az érintettek a személyes adataik kezeléséhez és az e rendelet szerinti jogaik gyakorlásához kapcsolódó valamennyi kérdésben az adatvédelmi tisztségviselőhöz fordulhatnak.
- (8) Az adatvédelmi tisztségviselőt feladatai teljesítésével kapcsolatban uniós vagy tagállami jogszabályban meghatározott titoktartási kötelezettség vagy az adatok bizalmas kezelésére vonatkozó kötelezettség köti.
- (9) Az adatkezelő és az adatfeldolgozó biztosítja, hogy az adatvédelmi tisztségviselő a feladatai ellátásával kapcsolatban utasításokat senkitől ne fogadjon el, és az általa ellenőrzött adatkezelési tevékenységgel összefüggésben az ellenőrzés függetlenségét sértő feladatot ne végezzen. Az adatkezelő vagy az adatfeldolgozó az adatvédelmi tisztségviselőt feladatai ellátásával összefüggésben nem bocsáthatja el és szankcióval nem sújthatja. Az adatvédelmi tisztségviselő közvetlenül az adatkezelő vagy az adatfeldolgozó legfelső vezetésének tartozik felelősséggel.
- (10) Az adatvédelmi tisztségviselő más feladatokat is elláthat. Az adatkezelő vagy az adatfeldolgozó biztosítja, hogy e feladatokból ne fakadjon összeférhetetlenség. Az adatvédelmi tisztségviselő tekintetében különösen összeférhetetlen az, ha a (11) bekezdés a.) pontjában foglalt tájékoztatás és szakmai tanács keretében olyan feladat, vagy munkafolyamat megvalósítását végzi, amelyiknek ellenőrzésére a (11) bekezdés b.) pontja alapján egyébként jogosult és köteles.
- (11) Az adatvédelmi tisztségviselő legalább a következő feladatokat ellátja:
 - a. tájékoztat és szakmai tanácsot ad az adatkezelő vagy az adatfeldolgozó, továbbá az adatkezelést végző alkalmazottak részére az e rendelet, valamint az egyéb uniós vagy

tagállami adatvédelmi rendelkezések szerinti kötelezettségeikkel kapcsolatban, véleményezi a 9. fejezet (6) bekezdése szerinti eljárásrendeket;

- b. ellenőrzi az e rendeletnek, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezéseknek, továbbá az adatkezelő vagy az adatfeldolgozó személyes adatok védelmével kapcsolatos belső szabályainak való megfelelést, ideértve a feladatkörök kijelölését, az adatkezelési műveletekben részt vevő személyzet tudatosság-növelését és képzését, valamint a kapcsolódó auditokat is;
- c. kérésre szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomon követi a hatásvizsgálat elvégzését;
- d. együttműködik a felügyeleti hatósággal; és
- e. az adatkezeléssel összefüggő ügyekben - ideértve a 13. fejezet (8) bekezdése szerinti előzetes konzultációt is - kapcsolattartó pontként szolgál a felügyeleti hatóság felé, valamint adott esetben bármely egyéb kérdésben konzultációt folytat vele.

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

15. Személyes adatok harmadik országokba vagy nemzetközi szervezetek részére történő továbbítása

(1) 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 kerülhet sor, e rendelet egyéb rendelkezéseinek betartása mellett, ha az adatkezelő és az adatfeldolgozó teljesíti a GDPR V. fejezetében foglalt feltételeket.

(2) Amennyiben az (1) bekezdésben foglalt adattovábbítás informatikai megoldással történik, úgy a GDPR V. fejezetében foglaltak mellett alkalmazandó különösen a jelen szabályzat 12. fejezetének (5) bekezdése.

16. Személyes adatokkal, adatvédelmi jogviszonnyal kapcsolatos jogorvoslatok

(1) Minden érintett jogosult arra, hogy panaszt tegyen egy felügyeleti hatóságnál - különösen a szokásos tartózkodási helye, a munkahelye vagy a feltételezett jogsértés helye szerinti tagállamban -, ha az érintett megítélése szerint a rá vonatkozó személyes adatok kezelése megsérti e rendeletet.

(2) Minden természetes és jogi személy jogosult a hatékony bírósági jogorvoslatra a felügyeleti hatóság rá vonatkozó, jogilag kötelező erejű döntésével szemben.

(3) Minden érintett jogosult a hatékony bírósági jogorvoslatra, ha az illetékes felügyeleti hatóság nem foglalkozik a panasszal, vagy három hónapon belül nem tájékoztatja az érintettet az (1) bekezdés alapján benyújtott panasszal kapcsolatos eljárási fejleményekről vagy annak eredményéről.

(4) A felügyeleti hatósággal szembeni eljárást a felügyeleti hatóság székhelye szerinti tagállam bírósága előtt kell megindítani.

(5) Minden érintett hatékony bírósági jogorvoslatra jogosult, ha megítélése szerint a személyes adatainak nem megfelelő kezelése következtében megsértették jogait.

(6) Az adatkezelővel vagy az adatfeldolgozóval szembeni eljárást az adatkezelő vagy az adatfeldolgozó tevékenységi helye szerinti tagállam bírósága előtt kell megindítani. Az ilyen eljárás megindítható az érintett szokásos tartózkodási helye szerinti tagállam bírósága előtt is, kivéve, ha az adatkezelő vagy az adatfeldolgozó valamely tagállamnak a közhatalmi jogkörében eljáró közhatalmi szerve.

(7) Az érintett jogosult arra, hogy panaszának, jogorvoslati kérelmének a nevében történő benyújtásával, adatvédelemmel összefüggő jogainak a nevében való gyakorlásával, valamint - ha a tagállam joga ezt lehetővé teszi - a 82. cikkben említett kártérítési jognak a nevében történő érvényesítésével olyan nonprofit jellegű szervet, szervezetet vagy egyesületet bízjon meg, amelyet valamely tagállam jogának megfelelően hoztak létre, és amelynek az alapszabályában rögzített céljai a közérdeket szolgálják, és amely az érintettek jogainak és szabadságainak a személyes adataik vonatkozásában biztosított védelme területén tevékenykedik.

(8) Minden olyan személy, aki személye adatainak vagy GDPR-ban foglalt jogai megsértésének eredményeként vagyoni vagy nem vagyoni kárt szenvedett, az elszenvedett kárért az adatkezelőtől vagy az adatfeldolgozótól kártérítésre jogosult.

(9) Az adatkezelésben érintett valamennyi adatkezelő felelősséggel tartozik minden olyan kárért, amelyet az e rendeletet sértő adatkezelés okozott. Az adatfeldolgozó csak abban az esetben tartozik felelősséggel az adatkezelés által okozott károkért, ha nem tartotta be az e GDPR-ben meghatározott, kifejezetten az adatfeldolgozókat terhelő kötelezettségeket, vagy ha az adatkezelő jogszerű utasításait figyelmen kívül hagyta vagy azokkal ellentétesen járt el.

(10) Az adatkezelő, illetve az adatfeldolgozó mentesül (9) bekezdése szerinti felelősség alól, ha bizonyítja, hogy a kárt előidéző eseményért őt semmilyen módon nem terheli felelősség.

(11) Ha több adatkezelő vagy több adatfeldolgozó vagy mind az adatkezelő mind az adatfeldolgozó érintett ugyanabban az adatkezelésben, és - a (9) és (10) bekezdés alapján - felelősséggel tartozik az adatkezelés által okozott károkért, minden egyes adatkezelő vagy adatfeldolgozó az érintett tényleges kártérítésének biztosítása érdekében egyetemleges felelősséggel tartozik a teljes kárért.

(12) Ha valamely adatkezelő vagy adatfeldolgozó a (4) bekezdéssel összhangban teljes kártérítést fizetett az elszenvedett kárért, jogosult arra, hogy az ugyanazon adatkezelésben érintett többi adatkezelőtől vagy adatfeldolgozótól visszaigényelje a kártérítésnek azt a részét, amely megfelel a (9) bekezdésben megállapított feltételek értelmében a károkozásért viselt felelősségük mértékének.

(13) A kártérítéshez való jog érvényesítését célzó bírósági eljárást az előtt a bíróság előtt kell megindítani, amely (6) bekezdésében említett tagállam joga szerint illetékes.

(14) A jogorvoslatokkal kapcsolatos egyéb szabályokat a GDPR VIII. fejezete tartalmazza.