

## SZEMÉLYES ADATOKRA VONATKOZÓ ADATVÉDELMI SZABÁLYZAT

### GDPR Szabályzat

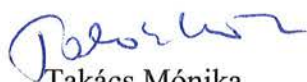
**Érvénybe lépett: 2022. 09. 01.**

**Verziószám: 2.0**

**Verziókövetés:**

**A szabályzat szövegének jogi átvizsgálása, átstrukturálása és pontosítása a jobb érthetőség miatt.**

**Összeállította:**



Takács Mónika  
minőségirányítási vezető

**Jóváhagyta:**



Simon Ferenc  
vizsgaközpont vezető

## Bevezetés

A Training360 Vizsgaközpont – mint a Training360 Kft. önálló szervezeti egysége, a továbbiakban: **Adatkezelő**) – szakmai és képesítő vizsgák lebonyolítása során számos személyes adatot kezel mind a vizsgára jelentkezők, mind a vizsgázók, és a vizsga lebonyolításában közreműködők vonatkozásában. Ennek során kiemelt figyelmet fordít a személyes adatok védelmére, melynek érdekében jelen Adatkezelési Szabályzatot (a továbbiakban: **Szabályzat**) alkotja.

## Jelen Adatkezelési Szabályzat jogszabályi háttere

- az Európai Parlament és a Tanács (EU) 2016. április 27. napján kiadott 2016/679 Rendelete (a továbbiakban: Rendelet vagy GDPR) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet),
- az információs önrendelkezési jogról és az információszabadságról szóló 2011. év CXII. törvény (továbbiakban: Infotv.),
- a Polgári Törvénykönyvről szóló 2013.évi V. törvény (Ptk.),
- a köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről szóló 1995. évi LXVI. törvény,
- a nemzeti köznevelésről szóló 2011.évi CXCV. törvény és annak végrehajtásáról szóló 229/2012.(VIII.28.) Kormányrendelet
- a szakképzésről szóló 2011.évi CLXXXVII. törvény
- a felnőttképzésről szóló 2013.évi LXXVII. törvény (Fktv.)
- a Munka törvénykönyvéről szóló 2012.évi I. törvény (Mt.)
- elektronikus ügyintézés és bizalmi szolgáltatások általános szabályairól szóló 2015.évi CCXXII. törvény
- 20/2012.(VIII.31.) EMMI rendelet a nevelési – oktatási intézmények működéséről és a köznevelési intézmények névhasználatáról
- 315/2013.(VII.28.) Kormányrendelet a komplex szakmai vizsgáztatás szabályairól
- 362/2011. (XII.30.) Kormányrendelet az oktatási igazolványokról
- a közfeladatot ellátó szervek iratkezelésének általános követelményeiről szóló 335/2005. (XII. 29.) Korm. rendelet
- IO/34-10/2017 iktatószám alatt kiadott 12/2018.(II.14.) OH elnöki utasítás, valamint a 22/2018 (VIII.29.) OH elnöki utasítás melléklete – Az Oktatási Hivatal adatvédelmi és adatbiztonsági szabályzata
- a szakképzésről szóló 2019. évi LXXX. törvény (Sztv.)
- a szakképzésről szóló törvény végrehajtásáról szóló 12/2020. (II. 7.) Korm. rendelet (Kr.)
- a társadalombiztosítási nyugellátásról szóló 1997. évi LXXXI. törvény
- a társadalombiztosítás ellátásaira jogosultakról, valamint ezen ellátások fedezetéről szóló 2019. évi CXXII. törvény

## Egyéb szabályozók:

MSZ EN ISO/IEC 17024: 2013

A Training360 Vizsgaközpont Vizsgaszabályzata (Vizsgaszabályzat)

## 1. A Szabályzat személyi hatálya

A Szabályzat személyi hatálya kiterjed az Adatkezelőre, az Adatkezelővel jogviszonyban álló, vagy jogviszonyt létesíteni kívánó **vizsgára jelentkezőkre, vizsgázókra**, valamint az Adatkezelő nevében adatkezelési tevékenységet ellátó személyekre, különösen a **vizsgáztatásban résztvevő valamennyi érintettre** (munkavégzésre irányuló jogviszonyban álló személyekre), továbbá az adatfeldolgozókra, a nem természetes személy adatfeldolgozó nevében adatkezelési tevékenységet ellátó személyekre (munkavállalók, megbízottak, vállalkozók, vagy egyéb, munkavégzésre irányuló jogviszonyban álló személyek).

## 2. A személyes adatok kezelésére vonatkozó Alapelvek

Az Adatkezelő az adatkezelés során mindenkor figyelemmel van az alábbi alapelvekre, és érvényesíti azokat az egyes adatkezelési folyamatokban és lépésekben:

- a) Az adatok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni („**jogszerűség, tisztességes eljárás és átláthatóság**”);
- b) Az adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történhet, és azok az adatkezelés jogalapjával össze nem egyeztethető módon nem kezelhetők; nem minősül az eredeti céllal össze nem egyeztethetőnek a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból történő további adatkezelés („**célhoz kötöttség**”);
- c) Az adatkezelés céljai szempontjából megfelelőek és relevánsak kell, hogy legyenek az adatok, és a szükségesre kell korlátozódniuk („**adattakarékosság**”);
- d) Az adatoknak pontosnak és szükség esetén naprakésznek kell lenniük; minden észszerű intézkedést meg kell tenni annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatok haladéktalanul törlésre vagy helyesbítésre kerüljenek („**pontosság**”);
- e) Az adattárolás olyan formában történhet, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé; a személyes adatok ennél hosszabb ideig történő tárolására csak akkor kerülhet sor, amennyiben a személyes adatok kezelésére a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból kerül majd sor, az érintettek jogainak és szabadságainak védelme érdekében előírt megfelelő technikai és szervezési intézkedések végrehajtására is figyelemmel („**korlátozott tárolhatóság**”);
- f) Az adatkezelés oly módon végezhető, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosított legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve („**integritás és bizalmas jelleg**”).
- g) Az Adatkezelő felelős az előző pontokban való megfelelésért, továbbá képesnek kell lennie e megfelelés igazolására („**elszámoltathatóság**”).

Az Adatkezelő alkalmazza továbbá az alábbi elveket:

- a) Az Adatkezelő 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 a Rendeletben foglalt követelmények teljesítéséhez és az Érintettek jogainak védelméhez szükséges garanciák beépítése az adatkezelés folyamatába („**beépített adatvédelem**”).
- b) 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 („**alapértelmezett adatvédelem**”).

### 3. Fogalom-meghatározások

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. „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;
3. „az adatkezelés korlátozása”: a tárolt személyes adatok megjelölése jövőbeli kezelésük korlátozása céljából;
4. „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;
5. „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;
6. „nyilvántartási rendszer”: a személyes adatok bármely módon – centralizált, decentralizált vagy funkcionális vagy földrajzi szempontok szerint – tagolt állománya, amely meghatározott ismérvek alapján hozzáférhető;
7. „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;
8. „adatfeldolgozó”: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel;
9. „címzett”: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, akivel vagy amellyel a személyes adatot közlik, függetlenül attól, hogy harmadik fél-e. Azon közhatalmi szervek, amelyek egy egyedi vizsgálat keretében az uniós vagy a tagállami joggal összhangban férhetnek hozzá személyes adatokhoz, nem minősülnek címzettnek; az említett adatok e közhatalmi szervek általi kezelése meg kell, hogy feleljen az adatkezelés céljainak megfelelően az alkalmazandó adatvédelmi szabályoknak;
10. „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;
11. „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;
12. „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;

13. „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;

14. „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, ilyen például az arckép vagy a daktiloszkópiai adat;

15. „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;

16. „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;

17. „NAIH”: Nemzeti Adatvédelmi és Információszabadság Hatóság, mint felügyeleti hatóság

## 8. Az adatkezelés jogszerűsége

Az adatkezelés jogszerűségének biztosításához megfelelő jogalap szükséges. Az adatkezelés során mindig meg kell állapítani, hogy az alábbi jogalapok közül valamelyik fennáll-e:

- a) az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez – a továbbiakban: **Az Érintett hozzájárulása, vagy Hozzájárulás;**
- 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 – a továbbiakban: **Szerződés teljesítése;**
- c) az adatkezelés az Adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges – a továbbiakban: **Jogszabályi kötelezettség teljesítése;**
- 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 – a továbbiakban: **Jogos érdek.**

## 9. A Hozzájáruláson alapuló adatkezelés

A Hozzájárulás az alábbi feltételek együttes fennállása esetén állapítható meg jogalapként:

- önkéntes és befolyásmentes – nem tekinthető annak, ha az adatszolgáltatás elmaradása olyan jellegű hátrányt okoz az érintettnek, amely befolyásolja az önkéntes akaratnyilvánítást, illetve ha az érintett alárendelt helyzetben van az Adatkezelővel szemben – *ilyen esetben a Jogszabályi kötelezettség teljesítése, Szerződés teljesítése vagy a Jogos érdek jogalap alkalmazási lehetőségét kell megvizsgálni.*
- megfelelő tájékoztatáson alapuló – *nem elegendő annak kinyilvánítása, hogy az érintett hozzájárulását adja valamely Adatkezeléshez, ezt az adott adatkezelésre vonatkozó tájékoztató(k) ismeretében kell megtennie, és az Adatkezelőnek tudnia kell bizonyítani, hogy a hozzájárulás tájékozott volt.*

- egyértelmű – a tájékoztatás nem rejthető el a szerződésben, más jogi szövegben; több adatkezelési cél esetén a hozzájárulást külön-külön célonként kell megkérni (és ezek nem tehetők egymástól függővé, nem lehet pl. a szerződés teljesítését a marketing hírlevélre történő feliratkozástól függővé tenni).
- kifejezett – nyilatkozat vagy egyéb félreérthetetlen cselekvés útján adja meg az érintett a hozzájárulást. Papír alapú dokumentum esetén aláírással, elektronikus dokumentum esetén pl. elektronikus levélben (vagy elektronikus aláírással, ha rendelkezik vele). A ráutaló magatartás nem fogadható el hozzájárulásként! Elektronikus felület esetén pl. ikonra kattintás, négyzet bejelölése is elfogadható, de tilos az előre bejelölt négyzetek alkalmazása. Minden esetben mellékelni kell a vonatkozó adatkezelési tájékoztatót, amelynek megismerését szintén egyértelműen és kifejezetten jeleznie kell az érintettnek (checkbox kipipálása, kifejezett nyilatkozat), ám a hozzájárulás kifejezettsége nem azonos a tájékoztató elfogadásával vagy megismerésével, tehát minden esetben tartalmaznia kell a nyilatkozatnak azt, hogy hozzájárul az Érintett az adatkezeléshez.

Amennyiben az adatkezelés kizárólag az érintett hozzájárulásán alapul, a hozzájárulás visszavonása esetén az adatkezelést meg kell szüntetni, és törölni kell a személyes adatot.

Különleges személyes adat Hozzájárulás alapján, vagy a Rendelet 9. cikk (2) bekezdésében tételesen meghatározott egyéb esetekben kezelhető, ám ilyen esetben is meg kell először állapítani az elsődleges jogalapot, és ezt követően megvizsgálni, hogy a 9. cikk (2) bekezdése szerinti feltételek közül megvalósul-e valamelyik. Amennyiben olyan, különleges személyes adatot tartalmazó adathordozó érkezik az Adatkezelőhöz, amellyel kapcsolatosan sem Hozzájárulás, sem egyéb, a Rendeletben meghatározott körülmény nem áll fenn, azt haladéktalanul, másolat készítése nélkül vissza kell juttatni a feladónak, vagy ha ez nem lehetséges, meg kell semmisíteni.

## 10. Szerződés teljesítése

A Szerződés teljesítése, mint jogalap csak a szerződés lényegéhez tartozó adatkezelések vonatkozásában alkalmazható. Így pl. a szerződéskötéshez feltétlenül szükséges azonosító adatok, aláírás, díjazás. Egyéb, jogszabály által előírt adatok esetében a Jogszabályi kötelezettség teljesítése jogalap alkalmazandó. Kifejezetten az érintettel (pl. vizsgán közreműködő személy) kötött szerződés esetén alkalmazható! Ha a szerződő fél az érintett munkáltatója, megbízója, cége stb., akkor Jogos érdek jogalap alkalmazható.

## 11. Jogszabályi kötelezettség teljesítése

Amennyiben jogszabály írja elő az Adatkezelést, csak azon adatok kérhetők az Érintettől, melyeket a jogszabály kifejezetten előír.

A vonatkozó jogszabálynak meg kell felelnie a Rendelet 6. cikk (3) bekezdésében foglalt előírásoknak. Amennyiben a jogszabály nem felel meg valamennyi kitételnek, az Adatkezelőnek az adott jogszabály betartására vonatkozó Jogos érdeke lehet a jogalap.

## 12. Jogos érdek

Jogos érdek jogalap esetén az érdekmérlegelési tesztet az adatkezelés megkezdése előtt el kell végezni.

Ennek keretében meg kell határozni, hogy mi alkotja az Adatkezelő vagy a harmadik fél jogszerű érdekét, meg kell vizsgálni, hogy mi alkotja az érintett olyan érdekeit vagy alapvető jogait és szabadságait, amelyek korlátozásra kerülnek, illetve melyek a személyes adatok védelmét teszik szükségessé. Ezen tényezők alapján előzetes mérlegelést kell végezni, amelynek eredményéhez képest – amennyiben nem egyértelmű – további garanciákat kell társítani az érintett jogainak védelmében. Az elszámoltathatóság alapelveire tekintettel Jogos érdek jogalap esetén személyes adat csak érdekmérlegelés elvégzését és írásbeli dokumentálását követően kezelhető. Az érdekmérlegelési tesztet az adatkezelés megkezdését megelőzően az adatvédelmi felelősnek kell elkészítenie (szükség esetén szakértői közreműködéssel) és megőriznie. Az érintettek tájékoztatásába bele kell foglalni az érdekmérlegelési teszt lényegét, és erre irányuló hozzáférési kérelem esetén meg kell küldeni az érintettnek a teszt másolatát.

### 13. Egyéb jogalapok

A Rendelet 6. cikk (1) bekezdés d) pontjában megjelölt jogalapon történő adatkezelés kivételes esetben fordulhat elő, pl. humanitárius veszélyhelyzetben, természeti vagy ember által okozott katasztrófa esetén.

Az e) pont szerinti adatkezelés közhatalmi jogosítványnak az Adatkezelőre ruházása esetén történhet, ekkor a jelen Szabályzatot is megfelelően módosítani kell.

### 14. Az érintett tájékoztatása

Az Adatkezelő az érintettek számára a személyes adatok kezelésére vonatkozó információkat tömör, átlátható, érthető és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva köteles nyújtani. A tájékoztatást írásban – ideértve az elektronikus utat is – kell megadni. Ennek elsődleges formája a weboldalon adatkezelési tájékoztatók közzététele.

A tájékoztatónak minden esetben tartalmaznia kell **legalább** az alábbi információkat:

- az **Adatkezelő neve, elérhetőségei**
- az adatkezelés tervezett **célja(i)**
- az adatkezelés **jogalapja**
- az adatok **tárolásának időtartama**
- az **érintett jogai** (jogos érdek Jogalap esetén külön kiemelve a tiltakozáshoz való jog, Hozzájárulás jogalap esetén a hozzájárulás bármikori visszavonhatóságára vonatkozó jog is)
- a NAIH-hoz címzett **panasz** benyújtásának joga

A fentiekén túlmenően, amennyiben releváns, a Rendelet 13-14. cikkében meghatározott további információkat (pl. jogos érdek megjelölés, harmadik félhez vagy harmadik országban történő adattovábbítás jogalapja stb.) is közölni kell.

*A tájékoztatókat az adatkezelési nyilvántartás alapján kell elkészíteni.*

*Amennyiben az adatokat nem közvetlenül az érintett-től szerzi az Adatkezelő, mindenképpen fel kell tüntetni az adatok forrását és a kezelt személyes adatok kategóriáit (azaz hogy milyen adatokat szerzett az Adatkezelő az érintettől).*

A tájékoztatást az érintett-től származó adatok esetében legkésőbb az adatok megszerzésének időpontjában, más forrásból származó adatok esetében 1 hónapon belül (ha pedig kapcsolattartásra kívánja az Adatkezelő használni az adatot, az első kapcsolatfelvételkor) kell megadni. A weboldalon a hatályos tájékoztatóknak könnyen elérhetőnek kell lenniük, legfeljebb két kattintásnyira a fő- illetve a vonatkozó aloldal címlapjától. A korábbi tájékoztatókat archív anyagként elérhetővé kell tenni. Ahol személyes adatok megadását kéri a weblap (pl. jelentkezés), a releváns tájékoztatót közvetlenül elérhetővé kell tenni.

### 15. Az érintetti joggyakorlásra vonatkozó kérelmek kezelése

#### 15.1. Általános szabályok

A Rendelet értelmében az érintett jogainak gyakorlása érdekében jogosult bármely formában (szóban, írásban elektronikus úton vagy papír alapon) kérelmet benyújtani az Adatkezelő részére. A kérelem teljesítése nem tagadható meg, kivéve, ha az érintettet az Adatkezelőnek nem áll módjában azonosítani (pl. anonim kérelmek) vagy ha erre egyébként a Rendelet lehetőséget biztosít. Ezt azonban bizonyítani kell.

Az Adatkezelő köteles elősegíteni az érintett Rendelet szerinti jogainak gyakorlását. A személyazonosság ellenőrzését első lépésben akként kell megtenni, hogy az Adatkezelő összeveti az érintett által a kérelemben megadott személyes adatokat a nyilvántartásában szereplő adatokkal. Egyezőség esetén a kérelem elbírálása

azonnal megkezdhető. Ha azonban az Adatkezelőnek megalapozott kétségei vannak a kérelmet benyújtó természetes személy kilétével kapcsolatban, azaz amennyiben a kezelt személyes adatok és az érintett által a kérelemben sajátjaként megjelölt személyes adatok az azonosítást nem teszik lehetővé (pl. másik e-mail címről küldte a kérelmet, mint amelyet korábban megadott), és az Adatkezelő bizonyítani tudja, hogy nincs abban a helyzetben, hogy azonosítsa az érintettet, további, az érintett személyazonosságának megerősítéséhez szükséges információk benyújtását kérheti. Ezek azonban csak olyan információk lehetnek, melyek ténylegesen lehetővé teszik az azonosítást, tehát az Adatkezelő rendelkezésére állnak (pl. nem kérhető személyi igazolvány másolat beküldése, mivel az igazolvány másolata egyébként nem áll rendelkezésre). A kért adat körét esetenként kell megállapítani, attól függően, hogy melyek azok a meglévő adatok, melyek az azonosítást lehetővé teszik.

A tájékoztatókban meg kell jelölni azokat az elérhetőségeket, amelyeken az érintett kérelmet terjeszthet elő. Az Adatkezelő központi postai és telefonos elérhetőségén felül a [vizsgakozpont@training360.com](mailto:vizsgakozpont@training360.com) e-mail címet kell feltüntetni.

*Ez azonban nem jelenti azt, hogy az Érintett más csatornán nem juttat el GDPR szerint érintetti kérelemnek minősülő nyilatkozatot az Adatkezelőhöz. Ezért a munkatársak oktatása során ki kell térni erre az eshetőségre is, fel kell tudniuk ismerni az ilyen kérelmeket, és jelezni az adatvédelmi felelősnek. Noha a visszajelzés elmaradása esetén egy esetleges NAIH vizsgálat során kimentési okként hivatkozhat az Adatkezelő arra, hogy az érintett nem a megfelelő címen terjesztette elő a kérelmét, ezeket célszerű megelőzni, és lehetőség szerint a más módon érkező kérelmeket is helyesen kezelni.*

*Szóbeli kérelemről feljegyzést kell készíteni, és a konkrét kérelemtől az érintett valamilyen (postai vagy elektronikus) elérhetőségét is fel kell tüntetni ezen.*

A kérelem benyújtását és dokumentált érkeztetését (iktatását) követően az adatvédelmi felelős (szükség esetén külső szakértő igénybe vételével) haladéktalanul megvizsgálja a kérelmet az alábbiak szerint:

- a) a kérelem benyújtója beazonosítható-e,
- b) a kérelem tárgya (melyik érintetti jog gyakorlására vonatkozik),
- c) a kérelemben foglaltak teljesítésére vonatkozó intézkedés (pl. helyesbítés, törlés) megtételére az Adatkezelő köteles-e.

A kérelmet tartalma szerint kell elbírálni, és ha a teljesítésnek nincs jogi akadálya, teljesíteni. Tájékoztatási jellegű kérelem esetén (tehát amikor nem szükséges pl. törlés, helyesbítés végrehajtása, hanem valamilyen információt kell az érintettnek megadni) a Rendeletben és jelen Szabályzatban előírt körben kell a visszajelzésben tájékoztatni az érintettet. Amennyiben csak bizonyos részinformációkat kér, azokat kell rendelkezésére bocsátani.

A hozzáférési jog keretében másolatot kell biztosítani az érintettnek (első alkalommal díjmentesen) az adathordozóról, amelyben adatait kezelik. Papíralapú dokumentum esetén fénymásolat vagy szkennelt formátum, kizárólag elektronikus dokumentum esetén excel táblába vagy xml formátumba történő kimásolás formájában történik a másolat kiadása. A másolatban nem szerepelhetnek más természetes személyek személyes adatai! Ha más módon nem lehetséges ezek eltávolítása, a másolaton ki kell takarni. A személyes adat másolata a foglalkoztatási jogviszonyokra illetőleg az ügyfélkapcsolattal összefüggő jogviszonyokra vonatkozóan az azt tartalmazó (törzs) nyilvántartásban tárolt személyes adatok másolatát jelenti, nem pedig a személyes adat (Adatkezelési nyilvántartásban és tájékoztatóban meghatározott célból történő) felhasználásával készült irat vagy bármely – akár elektronikus – dokumentum másolatát. Amennyiben az érintett kifejezetten egy egész dokumentum másolatát kéri, az már nem érintetti joggyakorlásnak minősül.

Helyesbítési, törlési kérelem esetén amennyiben nem áll fenn megtagadási ok, a kérelmet fizikailag teljesíteni kell (papír alapú iratokon adat kijavítása, ill. az irat megsemmisítése, elektronikus dokumentumokban, adatbázisban az adat kijavítása a korábbi adat törlése mellett, ill. az adat törlése). A törlési kérelem teljesítéséről jegyzőkönyvet kell felvenni, amely azonban már nem tartalmazhat személyes adatot, kizárólag annyit, hogy érintetti kérelem folytán adattörlés történt. A jegyzőkönyvet az adatvédelmi felelős őrzi.

A kérelem alapján történő intézkedés kizárólag akkor tagadható meg, ha a Rendelet alapján azt nem kötelező teljesíteni. Pl. hozzájárulás visszavonása és törlési kérelem, ha más jogalap is fennáll. Megtagadás esetén előzetesen feltétlenül konzultálni kell külső szakértővel.

Kizárólag akkor számítható fel ésszerű összegű díj a kért információra illetve az intézkedés meghozatalával



járó adminisztratív költségekre is figyelemmel, ha az Adatkezelő bizonyítani tudja, hogy a kérelem egyértelműen megalapozatlan vagy (különösen ismétlődő jellege miatt) túlzó, továbbá ha második vagy további alkalommal került sor az érintett részéről adatmásolat kérelmezésre. Díjigény helyett a kérelem teljesítésének megtagadása is alkalmazható. Ebben az esetben az Érintettet arról kell elsődlegesen tájékoztatni, hogy az Adatkezelő álláspontja szerint díjfizetés ellenében kerülhet csak sor a kérelem teljesítésére, jelezni kell azokat a körülményeket, amelyek ezt alátámasztják, és közölni kell a megállapított díjat, valamint a befizetés határidejét (kézhezvételtől számított 30 nap) és módját (bankszámlaszám, közlemény). Arra is fel kell hívni az Érintett figyelmét, hogy amennyiben nem teljesíti a díjfizetési kötelezettségét, a kérelem teljesítését az Adatkezelő megtagadja. A panasztételi jogról való tájékoztatás ez esetben kiemelt jelentőségű! Az ésszerű díj mértékét esetleg, a vizsgaközpont vezetővel egyeztetve kell megállapítani, figyelembe véve a kérelem tárgyát, a megválaszolásra fordítandó munkaidőt, postaköltséget stb.

Elektronikus formában érkezett kérelmet elektronikusan (e-mailben) kell megválaszolni, kivéve, ha az érintett kifejezetten másként kéri. Postai úton vagy szóban érkezett kérelmet lehetőség szerint (amennyiben ismert az érintett elektronikus levélcíme) elektronikusan kell megválaszolni, ha ez nem lehetséges, postai úton. *A válasz küldhető e-mail szövegtörzsben vagy mellékletként pdf-ben. Hozzáférési kérelem esetén az excel, xml fájlt mellékletként kell küldeni (ha csak elektronikusan kezelt az adat, az Érintett beazonosítása során meg kell kísérelni az elektronikus levélcím felderítését, ha ez sikertelen, ki kell nyomtatni az excel vagy xml fájl tartalmát). A visszajelzést tartalmazó iratot minden esetben a bejövő kérelemhez csatolva kell tárolni.*

A visszajelzésben az alábbi információkat kötelező megadni az érintettnek:

- tájékoztatás a kérelem teljesítéséről, a kért intézkedés megtételéről (tájékoztatási jellegű kérelem esetén ez a megfelelő tájékoztatás nyújtását jelent) vagy
- az intézkedés elmaradásáról,
- az intézkedés elmaradásának jogszabály és jelen Szabályzat szerinti okai,
- amennyiben 1 hónapon belül a visszajelzés nem adható meg, ennek okai (pl. a kérelem bonyolultsága vagy a beérkezett kérelmek nagy száma miatt), és hogy további 2 hónapon belül kapja meg a visszajelzést az Érintett,
- ha csak díjazás ellenében teljesíthető a kérelem, ennek indokai, a díjazás összege, befizetésének módja, határideje,
- hogy az Érintett panaszt nyújthat be a NAIH-nál (megjelölve a NAIH elérhetőségeket) és élhet bírósági jogorvoslati jogával (a jogvita elbírálása a törvényszék hatáskörébe tartozik),
- ha további kiegészítő információ megadása vált szükségessé a kérelemmel összefüggő azonosítás céljából, akkor az erre vonatkozó figyelemfelhívás,
- adatkezelési tájékoztatás arra vonatkozóan, hogy a kérelmet az Adatkezelő 5 évig nyilvántartja.

A visszajelzés során fokozottan ügyelni kell arra, hogy az nem sértheti más érintetteknek a személyes adatok védelméhez fűződő jogát, azaz csak és kizárólag a kérelmező vonatkozásában teljesíthető a kérelem, más személyre vonatkozó utalás nem tehető.

A kérelmet tehát úgy kell intézni, hogy az 1 hónapos határidőn belül a válasz már ki is legyen küldve az Érintettnek. Szükség esetén az egy hónapos határidő további 2 hónappal meghosszabbítható, figyelembe véve a kérelem összetettségét és a kérelmek számát. Ilyen esetben először (az 1 hónapos határidőn belül) erről kell az érintettet tájékoztatni.

Szükség esetén a visszajelzéssel egyidejűleg kell értesíteni a címzetteket is, akikkel a személyes adatot közölték, kivéve, ha ez lehetetlen vagy aránytalan erőfeszítést igényel. Erről a tényről az érintettet csak kifejezett kérelem esetén kell tájékoztatni.

## **15.2. A hozzáférés joga**

Az érintett kérelmezheti a rá vonatkozó személyes adatokhoz való hozzáférést. Az érintett jogosult arra, hogy

kérelmére az Adatkezelőtől visszajelzést kapjon arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e, és ha ilyen adatkezelés folyamatban van, akkor jogosult arra, hogy hozzáférést kapjon a személyes adatokhoz és a következő (a tájékoztatóban egyébként kötelezően rögzítendő) információkhoz:

- a) az adatkezelés céljai;
- b) a 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) információ az érintett azon jogáról, hogy kérelmezheti az Adatkezelőtől a rá vonatkozó személyes adatok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen;
- f) információ a NAIH-hoz címzett panasz benyújtásának jogáról (megjelölve a NAIH elérhetőségeket);
- g) ha az adatokat nem az Érintettől gyűjtötték, a forrásukra vonatkozó minden elérhető információ;
- h) az automatizált döntéshozatal ténye, ideértve a profilalkotást is, valamint az alkalmazott logikára illetve az ilyen Adatkezelés jelentőségére és az érintettre nézve várható következményeire vonatkozó információk.

Jogosult továbbá arra, hogy másolatot kapjon az Adatkezelő által kezelt személyes adatairól. A másolat készítésénél azonban ügyelni kell arra, hogy más személy személyes adatai nem adhatók ki, tehát pl. a fénymásolaton ki kell takarni a más érintettek azonosítását lehetővé tevő adatokat, illetve elektronikus adatbázisból történő kimásolás esetén sem szabad mások adatait is kiadni az érintettével együtt.

Ha személyes adatoknak harmadik fél részére vagy nemzetközi szervezet részére történő továbbítására kerül sor, az érintett jogosult továbbá arra is, hogy tájékoztatást kapjon a továbbításra vonatkozóan a jogszabály által előírt (GDPR 46.-49. cikk) megfelelő garanciákról.

### **15.3. Helyesbítéshez való jog**

Az érintett erre vonatkozó kérelme esetén az Adatkezelő köteles indokolatlan késedelem nélkül helyesbíteni 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.

Az Adatkezelő minden olyan címzettet tájékoztat helyesbítésről (a személyes adatokra mutató linkek vagy az adott személyes adatok másolatának, másodpéldányának helyesbítése érdekében) 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.

### **15.4. Törléshez való jog**

Az érintett jogosult arra, hogy az Adatkezelőtől a rá vonatkozó személyes adatok törlését kérje, az Adatkezelő pedig köteles arra, hogy az érintettre vonatkozó személyes adatokat indokolatlan késedelem nélkül törölje (azaz nem kell megvárni az érintett kérelmét, hanem a jogszabályi feltétel bekövetkeztekor enélkül is törölni kell az adatot), ha az alábbi indokok valamelyike fennáll:

- a) a személyes adatokra már nincs szükség abból a célból, amelyből azokat gyűjtötték vagy más módon kezelték (kérelemre tekintet nélkül);
- b) ha az érintett (akár a kérelemmel egyidejűleg akár attól független formában) visszavonja az adatkezelés alapját képező hozzájárulását, és az adatkezelésnek nincs más jogalapja;
- c) ha az érintett tiltakozik a közérdekből, közhatalmi jogosítvány gyakorlása érdekében vagy a jogos érdekből történő adatkezelés ellen (amelyeket az adatkezelési nyilvántartás ilyen jogalappal tartalmaz), és nincs elsőbbséget élvező jogszerű ok az adatkezelésre,
- d) ha az érintett tiltakozik a közvetlen üzletszerzés érdekében történő adatkezelés ellen;

- e) ha a személyes adatokat jogellenesen kezelték (kérelemre tekintet nélkül);
- f) ha a személyes adatokat az Adatkezelőre alkalmazandó uniós vagy hazai jogban előírt jogi kötelezettség teljesítéséhez törölni kell (kérelemre tekintet nélkül);
- g) ha a személyes adatok gyűjtésére gyermekek számára nyújtott információs társadalommal összefüggő szolgáltatások kínálásával kapcsolatosan került sor, és az érintett kéri azok törlését.

Az Adatkezelő minden olyan címzettet tájékoztat a törlésről e személyes adatok másolatának, másodpéldányának törlése érdekében, akivel, illetve amellyel a személyes adatot közölték, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel. Az érintettet kérésére az Adatkezelő tájékoztatja őt ezen címzettekről. Amennyiben a személyes adatot nyilvánosságra hozta az Adatkezelő (pl. weboldalon), és azt törölni kell, 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.

Az érintett jogosult arra, hogy személyes adatainak kezeléséhez adott hozzájárulását bármely időpontban visszavonja. A hozzájárulás visszavonása nem érinti a hozzájáruláson alapuló, a visszavonás előtti adatkezelés jogszerűségét. A hozzájárulás visszavonását az érintett ugyanolyan egyszerű módon jogosult megtenni, mint annak megadását. Ezért amennyiben az érintett hozzájárulás visszavonási igényt jelez bármely módon az Adatkezelő felé, és nincs más jogalap, mely alapján az adatot kezelik, az Adatkezelést meg kell szüntetni és törölni kell az adatot. Amennyiben azonban van más jogalap is, a visszavonási kérelmet tiltakozásnak is tekinteni kell, és aszerint kell eljárni.

Az érintett törlési jogának korlátozására csak a GDPR-ban írt alábbi kivételek fennállása esetén kerülhet sor, azaz a fenti indokok fennállása esetén a személyes adatok további megőrzése jogszerűnek tekinthető az alábbi esetekben:

- ha a véleménynyilvánítás és a tájékozódás szabadságához való jog gyakorlása, vagy
- ha valamely jogi kötelezettségnek való megfelelés (azaz az adatkezelési nyilvántartásban Jogszabályi kötelezettség jogalappal rögzített tevékenység esetén az adatkezelés céljának megfelelő időtartam alatt), vagy
- ha közérdekből végzett feladat végrehajtása, vagy
- ha az Adatkezelőre ruházott közhatalmi jogosítvány gyakorlása miatt, vagy
- ha népegészségügy területét érintő közérdekből,
- ha közérdekű archiválás céljából, vagy
- ha tudományos és történelmi kutatás céljából vagy statisztikai célból, vagy
- ha jogi igények előterjesztéséhez, érvényesítéséhez illetve védelméhez

szükséges.

### **15.5. Az adatkezelés korlátozásához való jog**

A korlátozás általában egy átmeneti intézkedés egy érintetti igény elbírálásáig vagy egy intézkedés megtételéig. A korlátozás megvalósulhat az adatnak egy másik rendszerbe történő ideiglenes áthelyezésével, megjelölésével, a hozzáférés ideiglenes felfüggesztésével, vagy más, alkalmas módon. Az érintett kérelmére az Adatkezelő korlátozza az adatkezelést, ha

- a) az érintett vitatja a személyes adatok pontosságát, amely 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;
- d) az érintett Jogos érdek vagy közérdek jogalap alapján (az adatkezelési nyilvántartásban rögzített két jogalap szerinti tevékenységre vonatkozóan) végzett adatkezelés ellen tiltakozott; amely esetben a

korlátozás arra az időtartamra vonatkozik, amíg megállapításra nem kerül, hogy az Adatkezelő jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben.

Ha az adatkezelés a fentiek alapján korlátozás alá esik, az ilyen személyes adatokat a tárolás kivételével csak az alábbi esetekben lehet kezelni:

- 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.

Az Adatkezelő köteles a korlátozás feloldásáról a feloldást megelőzően tájékoztatni az érintettet, akinek kérése alapján az adatkezelés korlátozásra került.

Az Adatkezelő minden olyan címzettet tájékoztat a korlátozásról (a személyes adatokra mutató linkek vagy az adott személyes adatok másolatával, másodpéldányával kapcsolatos adatkezelés korlátozása érdekében) akivel, illetve amellyel a személyes adatot közölték, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel. Az érintettet kérésére az Adatkezelő tájékoztatja ezen címzettekről.

### **15.6. Az adathordozhatósághoz való jog**

A GDPR alapján az érintett jogosult arra, hogy a rá vonatkozó, általa az Adatkezelő rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja, továbbá jogosult arra, hogy ezeket az adatokat egy másik adatkezelőnek továbbítsa anélkül, hogy ezt akadályozná az az Adatkezelő, amelynek a személyes adatokat a rendelkezésére bocsátotta,

- ha az adatkezelés jogalapja az érintett hozzájárulása, vagy az érintettel kötött szerződés teljesítése (az adatkezelési nyilvántartásban ezen két jogalap szerint rögzített tevékenységre vonatkozóan)
- és az adatkezelés automatizált módon történik.

Az adatok hordozhatóságához való jog gyakorlása során az érintett jogosult arra, hogy – ha ez technikailag megvalósítható – kérje a személyes adatok adatkezelők közötti közvetlen továbbítását.

Az adathordozhatóság jogának gyakorlása nem sértheti a törléshez való jogot. Az adathordozás joga nem alkalmazandó abban az esetben, ha az adatkezelés közérdekű vagy az Adatkezelőre ruházott közhatalmi jogosítványai gyakorlásának keretében végzett feladat végrehajtásához (az adatkezelési nyilvántartásban ezen jogalap szerint rögzített tevékenységre vonatkozóan) szükséges.

Az adatok hordozhatóságához való jog nem érintheti hátrányosan mások jogait és szabadságait (azaz kizárólag az érintett adatait lehet átadni, nem pedig teljes vagy akár részleges adatbázist).

### **15.7. A tiltakozáshoz való jog**

Az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból bármikor tiltakozzon személyes adatainak közérdekéből, közhatalmi jogosítvány gyakorlása érdekében vagy az Adatkezelő (harmadik fél) Jogos érdekében történő kezelése ellen, ideértve az ezen alapuló profilalkotást is. Ebben az esetben az Adatkezelő a személyes adatokat nem kezelheti tovább, azaz törölni köteles, 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.

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. Ha az érintett tiltakozik a személyes adatok közvetlen üzletszerzés érdekében történő kezelése ellen, akkor a személyes adatok a továbbiakban e célból nem kezelhetők, azaz törölendők, nincs helye a kérelem

megtagadásának a fenti indokokra való hivatkozással sem. A tiltakozáshoz való 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 a tájékoztató szerint.

Ha a személyes adatok kezelésére 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.

Tiltakozás esetén az adott adatkezelésre vonatkozó érdekmérlegelési teszt alapján kell az érintettet tájékoztatni arról, hogy miért nem teljesíthető a kérelme.

### **15.8. Automatizált döntéshozatal, profilalkotás**

Az Adatkezelő jelenleg nem alkalmaz automatizált adatkezelésen – ideértve a profilalkotást is – alapuló döntést. Amennyiben ez bevezetésre kerül, már a folyamat bevezetése során gondoskodni kell a Szabályzat módosításáról, megfelelő eljárásrend kialakításáról, valamint (szükség esetén) a hatásvizsgálat lefolytatásáról.

### **15.8. Panasztétel joga**

Az érintett jogosult arra, hogy panasszal éljen az Adatkezelő adatkezelése ellen az illetékes felügyeleti hatóságnál, mely a NAIH. Erre a tájékoztatókban fel kell hívni a figyelmet, és közölni kell a NAIH elérhetőségeit.

## **16. Nyilvántartási kötelezettség**

A jogszabályoknak, különösen az Elszámoltathatóság elvének való megfelelés, az adatkezelési tevékenységek ellátásának, kérelmek teljesítésének elősegítése, valamint a hatósági ellenőrzés során történő információszolgáltatás érdekében az Adatkezelő adatkezeléssel kapcsolatos nyilvántartásokat vezet. A NAIH részére rendelkezésre kell bocsátani ezeket, ha ilyen felhívás érkezik.

### **16.1. Adatkezelési nyilvántartás**

Az Adatkezelő az általa végzett adatkezelési tevékenységekről nyilvántartást vezet a Rendelet 30. cikk (1) bekezdése alapján. A nyilvántartás jelen Szabályzat elválaszthatatlan mellékletét képezi azzal, hogy a nyilvántartás vezetése nem igényli a Szabályzat módosítását.

A nyilvántartást elektronikusan, excel táblázatban, jól elkülöníthető adatkezelési tevékenység-csoportonként kell vezetni.

Az Adatkezelő nevét és elérhetőségét fel kell tüntetni. A nyilvántartást az adatvédelmi felelős vezeti.

Az adott adatkezelési tevékenységet, folyamatot sorszámozva, összefoglaló néven kell a nyilvántartásba bevezetni az „Adatkezelés” oszlopba. Minden egyes tevékenységnél meg kell adni a kezelt Személyes adat kategóriákat („Adatfajta”, pl. név, születési hely, idő, lakcím, e-mail cím, felhasználói név, jelszó, bérösszege, iskolai végzettség stb.), az „Érintettek” kategóriáit (pl. munkavállaló, partneri kapcsolattartó), az „Adatkezelés jogalapját” (az 5.2.1. pontban felsorolt lehetőségek közül egy), az Adatkezelésben részt vevő munkatársakat (munkakör szerint – „Adatkezelést végző”), az „Adatkezelés célját”, valamint az adatok törlésére előírt határidőket („Megőrzési idő”).

Az „Adatkezelés helye, hozzáférés” oszlopba a személyes adat fizikai tárolási illetve kezelési helyét, módját (papír alapú és elektronikus adatkezelést egyaránt), valamint a hozzáférésre vonatkozó esetleges korlátozásokat kell bevezetni, melyek egyben adatbiztonsági intézkedések is. Ha az adat közlésre, továbbításra kerül, a címzettek a „Adattovábbítás” oszlopban kell feltüntetni. Külföldre vagy nemzetközi szervezet részére történő adatközlés esetén az országot és/vagy nemzetközi szervezetet is meg kell jelölni;

ha a Rendelet 49. cikkén alapul az adattovábbítás, meg kell jelölni, melyik bekezdésen alapul.

Az „Adatbiztonsági intézkedések” oszlopban röviden meg kell jelölni az alkalmazott technikai és szervezési intézkedéseket. Általános IT biztonsági intézkedések néven kell bevezetni az információbiztonsági szabályzat szerinti IT Biztonsági Intézkedéseket. Az „Adatfeldolgozó igénybevétele” oszlopban nevesíteni kell az Adatfeldolgozót, ha van, ellenkező esetben „nincs” szóval jelezni.

A „Kapcsolódó informatikai rendszerek” oszlopot technikai segítségként kell vezetni (az Adatkezelés helye, hozzáférés oszlop kiegészítéseként), hogy ha van speciális szoftver, egyéb IT rendszer, amelyben az elektronikus adatkezelés történik, ez könnyen azonosítható legyen. A „Tájékoztatás formája” szintén technikai segítség, annak rögzítésére, hogy az adott adatkezelésre vonatkozó tájékoztatót milyen formában, hogyan közli az Adatkezelő az érintettekkel (pl. weboldalon, szerződés részeként stb.).

A „Kockázatok” rovatban röviden jellemezni kell az adott személyes adat elvesztése, megsemmisülés illetve jogosulatlan hozzáférés esetén az érintettekre gyakorolt hatást (alacsony, közepes, magas). Egyebekben a kockázatelemzésre a Szabályzatban és információbiztonsági szabályzatban foglaltak az irányadók.

Az adatkezelési nyilvántartás tartalmát naprakészen kell tartani és rendszeresen – legalább félévente – felül kell vizsgálni. Ennek keretében rögzíteni kell az új adatkezelési tevékenységeket, különösen új adatkezelési cél vagy új érintetti kör esetén. Soron kívül kell frissíteni a nyilvántartást új adatfeldolgozó bevonása esetén.

Törölni kell a már nem végzett adatkezelési tevékenységeket, de a törölt tevékenységnek a törlés időpontjával együtt megállapíthatónak kell maradnia, ezért az adott sort eltérő színnel kell kiemelni, és a sor végén jelölni a törlés időpontját, vagy segéd táblába áthelyezni a törölt adatkezeléseket. Az újonnan bevezetett adatkezelések esetén pedig jelezni kell a megkezdés időpontját. Az adatörzési idők esetleges módosítását csak az Adatvédelmi felelős és szükség esetén külső szakértő véleménye alapján szabad módosítani.

A Szabályzat szerinti tájékoztatók az aktuális adatkezelési nyilvántartás alapján készülnek, ezért az adatkezelési nyilvántartás frissítésével egyidejűleg frissíteni szükséges a vonatkozó tájékoztatókat is, amelyek alapján szükség szerint ismételt tájékoztatni kell az érintetteket.

## **16.2. Adatfeldolgozói nyilvántartás**

Amennyiben az Adatkezelő Adatfeldolgozóként jár el valamely más adatkezelő részére, a Rendelet 30. cikk (2) bekezdése szerint adatfeldolgozói nyilvántartást is kell vezetni. A nyilvántartásban a megbízó adatkezelőnként kell feltüntetni a végzett adatkezelési tevékenységet, ha harmadik országba vagy Nemzetközi szervezethez történik adattovábbítás, ennek tényét, az ország/szervezet megnevezését, valamint a 49. cikk szerinti garanciák leírását, amennyiben releváns. Az adatfeldolgozói nyilvántartás tartalmát naprakészen kell tartani és rendszeresen – legalább félévente – felül kell vizsgálni. A nyilvántartást az adatvédelmi felelős vezeti, elektronikusan.

Az igénybe vett Adatfeldolgozókról – bár a Rendelet nem írja elő kötelezően – szintén nyilvántartást kell vezetni, mely tartalmazza az adatfeldolgozó nevét, címét, ha rendelkezik adatvédelmi tisztviselővel, az ő elérhetőségeit, továbbá hogy mely területen alkalmazza az Adatkezelő, milyen jellegű tevékenységre. Ezen nyilvántartást szintén az adatvédelmi felelős vezeti és frissíti, elektronikus formában.

## **16.3. Nyilvántartás az Adatvédelmi incidensekről**

Az Adatkezelő nyilvántartást vezet a bekövetkezett adatvédelmi incidensekről. Az adatvédelmi incidens nyilvántartást folyamatosan naprakészen kell tartani. A nyilvántartás a hatósági bejelentési kötelezettség alá tartozó és a hatósági bejelentési kötelezettség alá nem tartozó adatvédelmi incidenseket is tartalmazza.

A nyilvántartást az *Eljárás adatvédelmi incidens esetén* c. pont szerint kell vezetni.

#### 16.4. Nyilvántartás az érintetti kérelmekről

Az érintettek által előterjesztett kérelmeket iktatni és nyilvántartani kell annak érdekében, hogy a későbbi esetleges jogviták során az Adatkezelő birtokában legyen a szükséges bizonyítékoknak. A nyilvántartásban 5 évre visszamenőleg kell megőrizni a kérelmeket (dátum, időpont, kérelmező) és az azokra adott választ, illetve a végrehajtás időpontját nyomtatott formában. A nyilvántartást az adatvédelmi felelős vezeti.

### 17. Adatvédelmi felelős

Az Adatkezelő a jelen Szabályzat alkalmazásával kapcsolatos teendők koordinálására, a külső szakértővel, NAIH-hal történő kapcsolattartásra adatvédelmi felelőst bíz meg. Az adatvédelmi felelősi feladatokat elláthatja az Adatkezelő alkalmazottja, vagy szolgáltatási szerződés keretében más természetes vagy jogi személy. Megbízatása visszavonásig szól, és írásba kell foglalni. Az adatvédelmi felelős elérhetőségeit az Adatkezelő és az adatfeldolgozók munkatársaival meg kell ismertetni.

Az adatvédelmi felelős feladatai:

- a) tájékoztatást ad a jelen Szabályzat hatálya alá tartozó Adatkezelő és adatfeldolgozó, és a nevükben eljáró munkatársak részére a jelen Szabályzat szerinti kötelezettségeikkel kapcsolatban;
- b) ellenőrzi a jelen Szabályzatnak és az adatvédelemmel összefüggő egyéb szabályzatnak történő megfelelést az Adatkezelőnél és az adatfeldolgozónál, ennek keretében feladata a jelen Szabályzat naprakészen tartása, különös tekintettel az adatkezelési valamint egyéb nyilvántartások vezetésére, illetve a jelen Szabályzatban részére kijelölt feladatok és hatáskörök ellátására;
- c) javaslatot tesz a személyes adatok védelmével kapcsolatos belső szabályozásra, módosításra, véleményezi a szabályozókat a személyes adatvédelem szempontjából,
- d) szervezi és ellenőrzi a személyes adatkezelési műveletekben részt vevő személyzet tudatosság-növelését és képzését;
- e) részt vesz az adatvédelmi hatásvizsgálatban, kapcsolatot tart a külső szakértővel; őrzik a jelen Szabályzat által megőrzendő, adatkezeléssel kapcsolatos dokumentációkat;
- f) együttműködik és bármely kérdésben konzultációt folytat a NAIH-hal, kapcsolattartási pontként szolgál, ennek keretében részt vesz a jelen Szabályzat szerinti adatvédelmi incidenskezelési tevékenységben.

Ha az Adatkezelő vagy az adatfeldolgozó bármely munkavállalója, közreműködője a saját tevékenysége körében személyes adatkezeléssel összefüggően intézkedést igénylő körülményt észlel, az alábbiak szerint kell eljárnia:

- Ha valamely érintett személyes adatkezeléssel kapcsolatos kérelmet (akár szóban, akár írásban) juttat el hozzá vagy a társasághoz, köteles értesíteni az adatvédelmi felelőst, és a kérelmet átadni neki (tartalmát közölni).
- Ha adatvédelmi incidensre utaló eseményt tapasztal vagy ezzel kapcsolatban bármely más releváns információhoz jut, haladéktalanul köteles értesíteni az adatvédelmi felelőst, és köteles továbbítani neki a releváns dokumentumokat és információkat.

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

Az Adatkezelő köteles biztosítani, hogy az adatvédelmi felelős a személyes adatok védelmével kapcsolatos összes ügybe megfelelő módon és időben bekapcsolódhasson, köteles továbbá támogatni feladatai ellátásában. Biztosítja számára azokat az forrásokat, amelyek a feladatai végrehajtásához, a Személyes adatokhoz és az adatkezelési műveletekhez való hozzáféréshez szükségesek.

Az adatvédelmi felelőst feladatai ellátásával kapcsolatban titoktartási kötelezettség terheli. Más feladatokat is elláthat, és az Adatkezelő köteles gondoskodni arról, hogy ez ne okozzon összeférhetlenséget.

## 18. Adatbiztonság, kockázatelemzés

A Rendelet 32. cikke értelmében az Adatkezelő a tudomány és technológia állására, a megvalósítás költségeire figyelemmel, valamint az adatkezelési tevékenységei természetes személyek jogaira és szabadságaira jelentett kockázatait figyelembe véve megfelelő technikai és szervezési intézkedéseket hajt végre annak érdekében, hogy a kockázat mértékének megfelelő, azzal arányos védelmi intézkedések útján szintű adatbiztonságot garantálja. Az Adatkezelő egyúttal biztosítja, hogy a Személyes adatokhoz hozzáféréssel rendelkező alkalmazottai és közreműködői kizárólag a jogszabályoknak megfelelően kezelik a személyes adatokat kivéve, ha ettől való eltérésre uniós vagy tagállami jog kötelezi őket.

Ezek teljesülésének érdekében a jelen Szabályzatban valamint az informatikai biztonsági dokumentációkban meghatározott informatikai biztonsági intézkedéseket teszi az Adatkezelő az alábbi elvek figyelembe vételével:

- a biztonság megfelelő szintjének meghatározása, figyelembe véve az adatkezelésből eredő olyan kockázatokat, amelyek a személyes adatok véletlen vagy jogellenes megsemmisítéséből, elvesztéséből, megváltoztatásából, jogosulatlan nyilvánosságra hozatalából vagy az azokhoz való jogosulatlan hozzáférésekből erednek,
- fizikai vagy műszaki adatvédelmi incidens esetén az arra vonatkozó intézkedések, hogy a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását a kellő időben vissza lehessen állítani,
- a személyes adatok kezelésére használt informatikai rendszerek és szolgáltatások folyamatos bizalmas jellegének, integritásának, rendelkezésre állásának és ellenálló képességének biztosítására vonatkozó előírások;
- a személyes adatok lehetőség szerinti és mihamarabbi álnevesítésére vagy titkosítására vonatkozó előírások;
- az adatkezelés biztonságának garantálására hozott intézkedések hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárások (többek között az adatokhoz történő hozzáférés visszakövethetőségére vonatkozó intézkedések).

Az adatkezelő rendszerek vonatkozásában biztosítani kell megfelelő tűzfalak alkalmazását, a biztonsági frissítések rendszeres telepítését, a rosszindulatú kódok elleni védekezés folyamatos, naprakész megvalósítását, a hozzáférési jogosultságok megfelelő szabályozását és ennek gyakorlati alkalmazását. Az adatok tárolása során az NIST 800-111 vagy egyenértékű szabványnak megfelelő rendszereket és eljárásokat kell alkalmazni a tárolt adatok titkosítására, továbbá az adattovábbítás során legalább a TLS vagy IPsec protokollok szerint. Az adathordozó eszközöknek lemezalapú titkosítással kell rendelkezniük.

*Új technológia bevezetése esetén – akár szükséges hatásvizsgálat elvégzése, akár nem – a Beépített adatvédelem elvének megfelelően konzultáció szükséges az érintett szakterület, az informatika és az adatvédelmi felelős között, melynek eredményéről a vezetőséget értesíteni kell.*

A kockázat olyan eshetőség, mely a súlyosság és a valószínűség szempontjából jellemez valamilyen eseményt és annak következményeit. A valószínűség szempontjából a kockázat forrásait (külső, belső, szándékos, rosszindulatú, vagy véletlen, gondatlan) és a kiszolgáló környezetet (informatikai rendszerek, papír alapú adatkezelés), míg a súlyosság szempontjából a kockázattal érintett személyes adatokat és az érintettekre gyakorolt lehetséges hatásokat kell vizsgálni.

A kockázatelemzésnek kiemelt jelentősége van a megfelelő adatbiztonsági intézkedések megválasztásánál, továbbá az adatvédelmi incidens kezelése során.

A kockázatok értékelésénél figyelembe kell venni többek között az alábbiakat:

- a kezelt személyes adatok típusa – történik-e különleges adatok (Rendelet 9. cikk) kezelése;
- történik-e egyéb, különleges adatnak nem minősülő, de érzékeny adat kezelése – pl. pénzügyi helyzetre vonatkozó, társadalmi megbecsülésre kiható (játékszenvedély, rossz tanulmányi eredmények stb.), felhasználói nevek és jelszavak, személyiséglopásra alkalmas adatok (pl. okmánymásolat) kezelése;



- az érintettek speciális kategóriának (gyermek, idős, kiszolgáltatott helyzetben lévő stb.) adatait kezeli-e az Adatkezelő az adott adatkezelési folyamatban;
- a kezelt személyes adatok mennyisége, illetve az, hogy egy adatkezelésen belül az egyes személyes adatok összekapcsolásával mennyire könnyen azonosítható az érintett;
- az érintettek száma – egy folyamat milyen nagyságrendű érintett adatainak kezelését valósítja meg;
- a lehetséges incidens hatásai az érintettekre – egyszerű bosszúság, mert az adataikat újra meg kell adni, vagy akár az alább írt súlyosabb következmények;
- az adatkezelés egyéb speciális körülményei.

*A személyes adatokra vonatkozó kockázatelemzést az informatikai biztonsági dokumentációban meghatározottak szerint kell elvégezni, figyelemmel a fentebb felsorolt szempontokra is, és az Adatkezelési nyilvántartásban rögzíteni az érintettek szempontjából releváns kockázatokat (ez eltérhet az Adatkezelőnél fellépő kockázattól!). A kockázat szintjének megfelelő védelemlől az általános és speciális IT biztonsági intézkedésekkel, valamint egyéb technikai és szervezési intézkedésekkel kell gondoskodni.*

## 19. Adatfeldolgozók, közös adatkezelés

Amennyiben az Adatkezelő adatfeldolgozót bíz meg, a szerződés megkötése előtt meg kell győződni arról, hogy a leendő partner megfelelő garanciákat nyújt az adatkezelés jogszabályban (különösen a Rendeletben) előírt követelményeknek való megfelelését és az érintettek jogainak védelmét biztosító, megfelelő technikai és szervezési intézkedések végrehajtására. Az adatfeldolgozó (ideértve az irányítása alatt eljáró, a személyes adatokhoz hozzáféréssel rendelkező személyeket) kizárólag az Adatkezelő utasításainak megfelelően kezelheti.

Az adatfeldolgozási megállapodást írásban kell megkötni, az adatfeldolgozó igénybevitelére vonatkozó szerződésbe foglalva (szövegtörzsben vagy mellékletként) szerepeltetni kell a GDPR 28. cikke szerinti kötelező tartalmi elemeket is. A megállapodásokat az Adatkezelő a szerződések között nyilvántartja.

Az adatfeldolgozói megállapodásban külön ki kell térni a szerződésszegés jogkövetkezményeire, ezen belül a személyes adatok jogosulatlan (utasítástól eltérő) kezelésére, és az ebből eredő károkért való felelősségre.

Amennyiben a fentiekől eltérően az eset összes körülményét figyelembe véve nem adatfeldolgozásnak, hanem **közös adatkezelésnek** minősül a jogviszony, akkor az Adatkezelő és a további adatkezelők a közöttük létrejött megállapodásban kötelesek meghatározni a GDPR-ban foglalt kötelezettségek teljesítéséért fennálló felelősségük megosztását, különösen az érintettek jogainak gyakorlásával és tájékoztatásával kapcsolatban. A megállapodásban meg kell jelölni, hogy melyikük tartja a kapcsolatot az érintettel. A megállapodást e tekintetben jogi szakértővel kell elkészíttetni. A megállapodás lényegéről az érintetteket tájékoztatni kell. Biztosítani kell az érintett jogait abban az esetben is, ha azokat a megállapodás feltételeitől függetlenül kívánja gyakorolni.

Az adatfeldolgozók személyét és elérhetőségét (legalább cím), valamint az általuk végzett adatfeldolgozási tevékenység lényegét a tájékoztatókon feltüntetve közölni kell azon érintettekkel, akik adatai az adatfeldolgozó részére továbbításra kerülnek.

*Amennyiben az Adatkezelő jár el adatfeldolgozóként, a szerződéses feltételeket meg kell vizsgálni abból a szempontból, hogy megfelelnek-e a GDPR-nak. Szükség esetén a megbízó adatkezelővel egyeztetést kell kezdeményezni.*

Az Adatkezelő által adatfeldolgozói minőségében végzett adatkezelésről nyilvántartást kell vezetni.

## 20. Eljárás adatvédelmi incidens esetén

## 20.1. Általános szabályok

Mivel az adatvédelmi incidens megfelelő és kellő idejű intézkedés hiányában fizikai, vagyoni vagy nem vagyoni károkat okozhat az érintetteknek, többek között

- személyes adataik feletti rendelkezés elvesztését,
- jogaik korlátozását,
- hátrányos megkülönböztetést,
- személyazonosság-lopást,
- vagy személyazonossággal való visszaélést,
- pénzügyi veszteséget,
- az álnevesítés engedély nélkül történő feloldását,
- a jó hírnév sérelmét,
- a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülését,
- vagy bármilyen egyéb jelentős gazdasági vagy szociális hátrányt,

kiemelt fontosságú feladat az adatvédelmi incidensek megfelelő kezelése.

Az adatvédelmi incidensekről nyilvántartást kell vezetni.

Az adatvédelmi incidensek három kategóriába sorolhatók:

- nyilvántartásban rögzítendő, de NAIH és érintettek felé történő bejelentést nem igénylő – ha az incidens valószínűsíthetően nem jár kockázattal az érintettek jogaira és szabadságaira nézve;
- NAIH felé történő bejelentést igénylő – ha az incidens valószínűsíthetően kockázattal jár az érintettek jogaira és szabadságaira nézve;
- az érintettek soron kívüli tájékoztatását is igénylő – ha az incidens valószínűsíthetően magas kockázattal jár az érintettek jogaira és szabadságaira nézve.

Az Adatkezelő bármely munkatársa, illetve az adatfeldolgozó kijelölt kapcsolattartója a személyes adatkezeléssel összefüggésben tudomására jutott, intézkedést igénylő rendkívüli eseményre vonatkozó információt haladéktalanul jelenti az adatvédelmi felelősnek elektronikus levélben (szóbeli bejelentés esetén e-mail-es megerősítéssel).

Az incidenskezelés során az alábbi sorrend szerint kell cselekedni:

1. Az incidens bekövetkeztének a bizonyítása, megerősítése
2. Az incidens gyors körülhatárolása, megfékezése
3. Az incidenssel érintett Személyes adatok körének minimalizálása
4. Az adatkezelési műveletekben fellépő zavar csökkentése
5. Az incidenssel kapcsolatos bizonyítékok azonosítása és rögzítése
6. Megfelelő ajánlások és biztonsági lépések megfogalmazása és végrehajtás
7. Az incidens kockázatainak csökkentése, megszüntetése (jövőbeli előfordulás során)

Az adatvédelmi felelős vezetésével haladéktalanul meg kell kezdeni az incidens kivizsgálását. Az adatvédelmi felelős vezetésével működő munkacsoport az eseményről való tudomásszerzéstől számított 48 órán belül, de legkésőbb 60 órán belül – figyelembe véve az eset összes körülményét – elvégzi az adatvédelmi incidens kockázat értékelését és dönt arra vonatkozóan, hogy

- az adatvédelmi incidens jár-e kockázattal a természetes személyek jogaira és szabadságaira nézve (ez esetben lásd a Hatósági bejelentésnél írt teendőket),
- és ha jár, akkor az magas kockázat-e (ez esetben a hatósági bejelentés mellett az érintettek tájékoztatását is teljesíteni kell).

Ehhez az incidenst be kell sorolni az alábbi három kategóriába (lehetséges, hogy több kategóriába is tartozik), mivel a bejelentés során ez is lényeges információ:

- bizalmassági incidens: a személyes adatok véletlen, vagy felhatalmazás nélküli közlése, vagy az ezekhez való jogosulatlan hozzáférés;
- sértetlenséggel kapcsolatos incidens: a személyes adatok véletlen vagy jogellenes megváltoztatása;
- hozzáférhetőséggel kapcsolatos incidens: a személyes adatok véletlen vagy jogellenes megsemmisítése, vagy elvesztése.

A kockázatok lehetnek külső és belső eredetűek, véletlenek (pl. adathordozó elvesztése) vagy rosszhindulatúak (pl. hackertámadás). Érinthetik a kiszolgáló környezet egyes (pl. egyetlen pendrive tűnik el) vagy sok elemét (pl. teljes hálózat vírusfertőzöttsége).

A személyes adatokra gyakorolt hatások vizsgálata során a *Kockázatelemzés* c. pontban írtakat kell alapul venni.

Az adatvédelmi incidenst, függetlenül attól, hogy a NAIH részére be kell-e jelenteni, **nyilvántartásba** kell venni. A nyilvántartást az adatvédelmi felelős vezeti, és az incidens lezárásig folyamatosan tölti fel az adatokat. A nyilvántartást folyamatos sorszámozással kell ellátni, bejegyzett incidenst törölni nem lehet. Fel kell tüntetni az esemény megnevezését, leírását (mi, mikor, hol/melyik rendszerben, miért történt), hatásait (kockázati kategória, következmények, hatósági bejelentésre vonatkozó adatok, érintetti tájékoztatás) és az orvoslására tett intézkedéseket, valamint az incidens lezárásának időpontját.

Az incidens jövőbeli előfordulásának megakadályozása, vagy legalábbis ennek csökkentése érdekében le kell vonni a megfelelő konzekvenciákat és megtenni a szükséges intézkedéseket.

## 20.2. Hatósági bejelentés

Az adatvédelmi incidenst a tudomásra jutástól számítva haladéktalanul meg kell vizsgálni abból a szempontból, hogy szükséges-e a NAIH felé bejelenteni. Ha igen, az Adatkezelő a tudomására jutását követően indokolatlan késedelem nélkül, ha lehetséges, legkésőbb 72 órán belül bejelenteti a NAIH részére. A bejelentést, a NAIH által megadott formában és módon kell megtenni, a NAIH előírásai szerint.

## 20.3. Az Érintettek tájékoztatása

Az Adatkezelő indokolatlan késedelem nélkül tájékoztatja az érintette(ke)t az adatvédelmi incidensről, ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve.

Nem kell értesíteni az Érintettet az alábbi esetekben:

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

## 21. Belső adatvédelmi tudatosságnövelés

A beépített és alapértelmezett adatvédelem elveinek érvényesülése, valamint a jogszabályoknak való

megfeleléshez szükséges információk szervezeten belüli megfelelő kommunikációja miatt évente legalább egyszer adatvédelmi oktatást szervez az Adatvédelmi felelős, szükség szerint külső szakértő részvételével.

Ennek során meg kell ismertetni a munkatársakkal a GDPR alapvető rendelkezéseit, a jelen Szabályzat napi gyakorlatban történő érvényesítéséhez szükséges teendőket, és fokozni szükséges a munkatársak adatvédelmi és adatkezelési tudatosságát. A későbbiek során a szabályok és a jogalkalmazási gyakorlat, illetőleg a jelen Szabályzat változásaira kell felhívni a figyelmet.

A munkatársak részére tananyagokat és ellenőrző kérdéseket kell készíteni. Az új belépőket soron kívüli adatvédelmi oktatásban kell részesíteni.

A jelen Szabályzatot elérhetővé kell tenni valamennyi munkatárs számára.

## 22. Adatvédelmi hatásvizsgálat

Az adatvédelmi hatásvizsgálat célja az adatkezelés jellegének feltárása, szükségességének és arányosságának vizsgálata, valamint a személyes adatok kezeléséből eredően a természetes személyek jogait és szabadságait érintő kockázatok kezelésének elősegítése e kockázatok értékelésével és a kezelésükre szolgáló intézkedések meghatározásával.

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 adatkezelést megelőzően hatásvizsgálatot kell végezni 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.

A 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) személyes adatok különleges kategóriái, vagy a büntetőjogi felelősség megállapítására vonatkozó határozatokra és büncselekményekre vonatkozó személyes adatok nagy számban történő kezelése;
- c) nyilvános helyek nagymértékű megfigyelése.

A NAIH által közzétett jegyzékben szereplő adatkezelések esetén, melyekre vonatkozóan kötelező a hatásvizsgálat elvégzése, ezeket figyelembe kell venni.

Annak megállapítása során, hogy a hatásvizsgálat elvégzése szükséges-e, az alábbi szempontokra kell figyelemmel lenni:

1. történik-e értékelés, pontozás az érintettekkel kapcsolatban, ideértve a profilalkotást és az előrejelzést (pl. a honlapot felkeresők böngészési szokásai)?
2. történik-e automatizált döntéshozatal (amely joghatással bír az érintettekre, vagy jelentősen érinti őket – pl. diszkriminációt eredményez)?
3. sor kerül-e módszeres megfigyelésre (nyomon követés vagy ellenőrzés céljából, pl. hálózaton keresztül adatgyűjtés, nyilvános terek megfigyelése, GPS nyomkövetés)?
4. a tervezett adatkezelés kiterjed-e különleges adataira vagy fokozottan személyes jellegű adataira (pl. egészségügyi, genetikai, biometrikus adatok, büntetett előéletre vonatkozó adatok, elektronikus hírközlő eszközök használatára vonatkozó, vagy pénzügyi adatok, helymeghatározó adat), ezeket az adatokat az érintett maga nyilvánosságra hozta-e?
5. nagy számban történik-e a tervezett adatkezelés (nemcsak számadatként, hanem pl. lakosság arányában meghatározva, illetve az adatmennyiség, vagy az adatfajták széles köre, az adatkezelés hosszú időtartama vagy állandó jellege, illetve földrajzi kiterjedése is szempont)?

6. történik-e adatrészek egymással való megfeleltetése vagy összevonása az ésszerű mértéket meghaladóan (pl. eltérő céllal vagy más-más adatkezelő által kezelt adatok vonatkozásában)?
7. az érintettek kiszolgáltatott helyzetben vannak-e (pl. függés az Adatkezelőtől – munkavállalók, ill. gyermekek)?
8. sor kerül-e új technológiai vagy szervezési megoldások innovatív használatára (pl. ujjlenyomat és arcfelismerés együttes alkalmazása beléptetéshez)?
9. a tervezett Adatkezelés önmagában megakadályozza-e, hogy az érintettek jogukat gyakorolják, vagy szolgáltatásokat vegyenek igénybe, szerződést érvényesítsenek (az érintett számára szolgáltatás igénybe vételének vagy szerződés megkötésének lehetővé tételére, módosítására, elutasítására irányuló adatkezelések)?

Amennyiben a fenti szempontok közül több is megvalósul, nagy valószínűséggel a hatásvizsgálatot el kell végezni. Minél több szempont valósul meg, annál indokoltabb a vizsgálat lefolytatása. Különleges esetekben azonban már akár egy szempont megvalósulása indokoltá teheti a vizsgálatot.

A hatásvizsgálatnak ki kell terjednie legalább az alábbiakra:

- a tervezett adatkezelési művelet módszeres leírására és az adatkezelés céljainak ismertetésére, beleértve adott esetben az érvényesíteni kívánt Jogos érdeket;
- az adatkezelési célokra figyelemmel az adatkezelési művelet szükségességi és arányossági vizsgálatára;
- az érintett jogait és szabadságait érintő kockázatok vizsgálatára;
- a kockázatok kezelését célzó intézkedések bemutatására, ideértve a személyes adatok védelmét és a Rendelettel való összhang igazolását szolgáló, az érintettek és más személyek jogait és jogos érdekeit figyelembe vevő garanciákat, biztonsági intézkedéseket és mechanizmusokat.

A hatásvizsgálatot az adatkezelési művelet megkezdése előtt kell elvégezni. Az adatvédelmi felelős vezeti, és be kell vonni az adatkezelési műveletben érintett terület vezetőjét vagy az általa kijelölt munkatársat, egy informatikai munkatársat, továbbá ha van, a műveletben érintett adatfeldolgozót is. Szükség esetén külső szakmai tanácsadó segítségét is igénybe kell venni, továbbá lehetőség szerint ki kell kérni az érintettek, illetve reprezentatív csoportjuk véleményét is.

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 konzultálni kell a NAIH-hal.

A konzultáció során meg kell adni a NAIH részére az általa kívánt információkat, így különösen:

- az Adatkezelő feladatköreit, illetve ha adatfeldolgozó is részt vesz az adatkezelésben, akkor a feladatok megosztását;
- a tervezett adatkezelés céljait és módjait;
- az érintettek jogainak és szabadságainak védelmében hozott intézkedések és garanciák;
- a hatásvizsgálat eredménye.

A NAIH előírásait kötelezően figyelembe kell venni.

A hatásvizsgálattal érintett adatkezelést az adatvédelmi felelős legalább évente, illetőleg a kockázat változásakor soron kívül ellenőrzi.

## 23. Adattovábbítás

Az adattovábbítás alapulhat jogszabályon vagy szerződésen (pl. az adatfeldolgozó részére). Az adatkezelési nyilvántartás tartalmazza a címzetteket.

A címzettekről az érintettet tájékoztatni kell, azonban nem minősülnek címzettnek azok a közhatalmi szervek, amelyek jogszabályon alapuló egyedi vizsgálat keretében férnek hozzá a személyes adathoz.

Olyan személyes adatok továbbítására – ideértve a személyes adatok EU-n kívüli, 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, a Rendelet egyéb rendelkezéseinek betartása mellett, ha az Adatkezelő és az adatfeldolgozó teljesíti a Rendelet V. fejezetében rögzített feltételeket.

Ennek alapján az adattovábbítás történhet

- megfelelőségi határozat alapján, vagy
- megfelelő garanciák alapján, vagy
- különös helyzetekben.

A megfelelőségi határozatot a Bizottság hozza meg, és teszi közzé. Az adatvédelmi felelős feladata ezek folyamatos figyelemmel kísérése, amennyiben történik ilyen jellegű adattovábbítás.

Amennyiben nincs megfelelőségi határozat, az alábbi garanciák mellett történhet adattovábbítás:

- közhatalmi vagy egyéb, közfeladatot ellátó szervek közötti, jogilag kötelező erejű, kikényszeríthető jogi eszköz rendelkezik az adattovábbításról;
- kötelező erejű vállalati szabályok tartalmazzak garanciákat;
- a Bizottság által a Rendelet 93. cikk (2) bekezdésében említett vizsgálóbizottsági eljárással összhangban elfogadott általános adatvédelmi kikötéseknek megfelel;
- a felügyeleti hatóság által elfogadott és a Bizottság által jóváhagyott általános adatvédelmi kikötéseknek megfelel;
- a magatartási kódex alkalmazása a harmadik országbeli adatkezelő vagy adatfeldolgozó által, kötelezettségvállalásával együtt, hogy alkalmazza a megfelelő – ideértve az érintettek jogaira vonatkozó – garanciákat; vagy
- tanúsítási mechanizmushoz csatlakozott a harmadik országbeli adatkezelő vagy adatfeldolgozó, és kötelező erejű és kikényszeríthető kötelezettségvállalást tett, hogy alkalmazza a megfelelő garanciákat, ideértve az érintettek jogait illetően is.

Fentiekén túlmenően, ha sem megfelelőségi határozat, sem megfelelő garanciák nincsenek, az alábbi esetekben továbbítható a személyes adat az EU-n kívülre:

- az érintett kifejezetten hozzájárulását adta a tervezett továbbításhoz azt követően, hogy tájékoztatták az adattovábbításból eredő – a megfelelőségi határozat és a megfelelő garanciák hiányából fakadó – esetleges kockázatokról;
- az adattovábbítás az érintett és az adatkezelő közötti szerződés teljesítéséhez, vagy az érintett kérésére hozott, szerződést megelőző intézkedések végrehajtásához szükséges;
- az adattovábbítás az adatkezelő és valamely más természetes vagy jogi személy közötti, az érintett érdekét szolgáló szerződés megkötéséhez vagy teljesítéséhez szükséges;
- az adattovábbítás fontos közérdekből szükséges;
- az adattovábbítás jogi igények előterjesztése, érvényesítése és védelme miatt szükséges;
- az adattovábbítás az érintett vagy valamely más személy létfontosságú érdekeinek védelme miatt szükséges, és az érintett fizikailag vagy jogilag képtelen a hozzájárulás megadására;
- a továbbított adatok olyan nyilvántartásból származnak, amely az uniós vagy a tagállami jog értelmében a nyilvánosság tájékoztatását szolgálja, és amely vagy általában a nyilvánosság, vagy az ezzel kapcsolatos jogos érdekét igazoló bármely személy számára betekintés céljából hozzáférhető, de csak ha az uniós vagy tagállami jog által a betekintésre megállapított feltételek az adott különleges esetben teljesülnek.

Ha az adattovábbítás a fenti különös helyzeteken alapul, az érintettet a lehetőségek szerint tájékoztatni kell az adatok biztonsága és védelme érdekében tett intézkedésekről is.

## 24. A Szabályzat módosítása

Jelen Szabályzatot módosítani szükséges, amennyiben az adatkezelésben, illetőleg a vonatkozó jogszabályokban, vagy az adatkezelést érintő körülményekben jelentős változás következik be, mely nem kezelhető az eljárásrendek vagy a tájékoztatók módosításával. Továbbá módosítani javasolt, amennyiben az adatvédelmi gyakorlatban ismertté válnak olyan új döntések, körülmények, melyek a Szabályzat módosítását, kiegészítését teszik szükségessé. Ennek érdekében a Szabályzatot szükség szerint, de legalább évente felül kell vizsgálni. Az adatkezelési és adatfeldolgozói nyilvántartás folyamatos vezetése, valamint az eljárásrendek és tájékoztatók módosítása nem igényli a Szabályzat módosítását.

A módosítás a kihirdetéssel válik hatályossá.

## 25. Egyes adatkezelések

### 25.1. Az adatkezelési tevékenységek közös szabályai

Az Adatkezelő tevékenysége a Jogszabályi háttérnél megjelölt jogszabályok szerinti, szakmai és képesítő vizsgák megszervezése és lebonyolítása. Ennek során fogadja a vizsgákra történő jelentkezéseket, kapcsolatot tart a jelentkezőkkel, kiválasztja a vizsgáztatásban közreműködő, jogszabályban előírt feladatokat ellátó személyeket, velük szerződést köt. Sor kerül a vizsgák megfelelő dokumentálására, majd az eredmény megállapítására és ennek a vizsgázókkal való közlésére. Az Adatkezelő kapcsolatot tart továbbá a Nemzeti Szakképzési és Felnőttképzési Hivatallal, az IKK Innovatív Képzési Központ Zrt-vel, a szakképző intézményekkel, amelyek adatot továbbítanak az Adatkezelőnek, illetve akik részére adattovábbítás történik. A vizsgák lebonyolítása vagy elektronikus, online kapcsolat igénybe vételével történik, vagy pedig a résztvevők személyes jelenlétében. Az e-Kréta rendszer használata az Adatkezelő és a vizsgázók részére is kötelező. Az Adatkezelő eljárását a jogszabályok és a Vizsgaszabályzat határozza meg.

Az adatkezelés **jogalapjával** kapcsolatosan, amennyiben konkrét jogszabályi előírás kapcsolódik az adott adatkezelési tevékenységhez, mindig meg kell vizsgálni, hogy a vonatkozó jogszabály megfelel-e a Rendelet 6. cikk (3) bekezdésében és az Infotv. 5.§ (3) bekezdésében foglaltaknak. Amennyiben igen, az adatkezelés jogalapja Jogszabályi kötelezettség teljesítése, ha viszont nem (pl. a Kr. esetében), akkor az Adatkezelőnek az adott jogszabály betartására vonatkozó Jogos érdeke.

A jelentkezőktől, illetve a vizsgázóktól a jogszabályok által előírtakon felül kizárólag olyan **adat** kérhető és kezelhető, amely a vizsga megszervezéséhez és lebonyolításához feltétlenül szükséges.

Az adatkezelések során elsődlegesen az Adatkezelő munkatársai (vizsgaközpont vezető, vizsgaadminisztrátor) működnek közre, akik jogosultak a kezelt adatok megismerésére, de a vizsgák lebonyolításában a jogszabályban meghatározott feladatkört betöltő, független külső személyek is részt vesznek, akikkel megfelelő tartalmú **adattfeldolgozói** szerződést kell kötni, illetve az ő személyes adataik kezelése során az Adatkezelő a jelen Szabályzatban foglaltak szerint jár el.

A kezelt adatok **megőrzési ideje** főszabály szerint az Sztv. 117.§-ában foglaltak alapján 5 év.

Az online vizsgáztatás esetén igénybe vett elektronikus rendszer kiválasztása során fokozott figyelmet kell fordítani az **adatbiztonsági** intézkedésekre, és lehetőség szerint az EU-n belül tevékenységi hellyel rendelkező adatfeldolgozót kell választani, akivel, mint a rendszer üzemeltetőjével megfelelő tartalmú adattfeldolgozói szerződést kell kötni. Az online vizsga egészéről vagy egy részéről felvétel készülhet, melyet az esetleges, a vizsga integritását sértő magatartások kivizsgálása céljából készít az Adatkezelő, és amennyiben nem érkezik bejelentés, 15 nap elteltével töröl. Az Adatkezelő helyiségeiben működő **biztonsági kamerákkal** végzett adatkezelésről mind a vizsgázókat, mind a vizsgáztatásban közreműködőket előzetesen tájékoztatni kell, azzal a tartalommal, amelyet az Adatkezelő helyiségeibe belépő személyek részére kifüggesztett tájékoztatóban is megtalálható.

Az e-Kréta rendszerbe **továbbított adatok** vonatkozásában a rendszer üzemeltetője címzettnek minősül, és

a továbbítást követően a saját adatkezelési szabályai szerint kezeli az adatokat.

A jogszabályi előírások értelmében adott esetben sor kerülhet a jelentkezők, illetve vizsgázók **különleges adatainak**, főként egészségügyi adatainak kezelésére (pl. SNI, vizsgaidőpont halasztási vagy mulasztási kérelemhez csatolt orvosi igazolás, baleset, rosszullet a vizsgán). Ezek esetében a Rendelet 6. cikke szerinti jogalap mellett meg kell állapítani a 9. cikk (2) bekezdése szerinti körülményt, mely alapján a különleges adat kezelhető. ez jellemzően a b) pont (szociális biztonságot szolgáló jogi előírásokból fakadó kötelezettség teljesítése) vagy az érintett kifejezett hozzájárulása (a) pont).

### **25.2. Vizsgajelentkezéssel kapcsolatos adatkezelések**

A vizsgázó jelentkezése történhet jelentkezési lap megküldésével, vagy közvetlenül az e-Kréta rendszeren keresztül. Az e-Kréta rendszerben csak a vizsgázó tud jelentkezni, ennek adatait a rendszer továbbítja az Adatkezelőnek. Jelentkezési lapot a vizsgázó vagy meghatalmazottja, illetve törvényes képviselője küldhet be – ez utóbbi esetben a képviselő adatainak kezelésére is sor kerül. Az Adatkezelő által rendszeresített jelentkezési lapon csak olyan adat megadása kérhető, amelyet a jogszabályok előírnak, továbbá amely a kapcsolattartáshoz szükséges (telefonszám, e-mail cím).

A jelentkezéssel együtt felmentési, méltányossági vagy vizsgarész-beszámítási kérelemmel is élhet a jelentkező. A jelentkezés elfogadását vissza kell igazolni, vagy hiánypótlást kiadni, a Vizsgaszabályzatban foglaltak szerint. Amennyiben egészségügyi adat is felmerül pl. a méltányossági kérelemmel összefüggésben, a fentiek szerint, fokozott gondossággal kell eljárni.

A vizsgázók, vizsgacsoport e-Kréta rendszerben való rögzítése során a rendszer által megkívánt adatokat kell továbbítani. A vizsga időpontjáról és a vizsgával kapcsolatos tudnivalókról a jelentkezőt a megadott értesítési csatornán keresztül ki kell értesíteni.

Amennyiben a vizsgázót díjfizetési kötelezettség terheli, a pénzügyi elszámolás során a könyvelőiroda, mint adatfeldolgozó működik közre, akivel megfelelő tartalmú adatfeldolgozói szerződést kell kötni.

Az adatkezelések jogalapja a Kr. vonatkozó rendelkezéseinek betartására, illetve a kapcsolattartásra vonatkozó Jogos érdek.

### **25.3. Vizsga lebonyolításával kapcsolatos adatkezelések**

A vizsga során az Adatkezelő munkatársain kívül a jogszabályokban és a Vizsgaszabályzatban meghatározott feladatkört ellátó személyek (jegyző, vizsgabizottsági tag, vizsgafelügyelő, mérő stb.) működnek közre. Ezen személyek a jogszabály erejénél fogva jogosultak a személyes adatok kezelésére, amelyek a feladatuk ellátásával összefüggésben tudomásukra jutnak.

Ugyanakkor képzéssel és megfelelő tartalmú adatfeldolgozói szerződés kötésével kell biztosítani, hogy tisztában legyenek a feladatuk adatkezelési vonatkozásaival és az őket terhelő titoktartási kötelezettséggel.

A közreműködő személyes adatokat tartalmazó dokumentumokat nem hagyhat elöl, őrizetlenül, illetve azokat illetéktelen személyektől elzártan, nem hozzáférhetően kell tárolnia. Személyes adatokat tartalmazó dokumentumokat nem oszthat meg illetéktelenekkel, nem mutathat meg. A közreműködő a személyes adatokat tartalmazó dokumentumokat nem másolhatja, az adatokról semmilyen elektronikus vagy papíralapú másolatot, archívumot nem készíthet, adatokat nem rögzíthet, továbbíthat és kezelhet, azokat saját céljaira nem használhatja fel.

Elektronikus dokumentum-küldés esetében a közreműködő köteles meggyőződni, hogy az elektronikus dokumentumokat/adatokat az elküldést, feltöltést követően törölte saját tárolójáról, köteles biztonságos, megbízható fájlküldő szolgáltatást igénybe venni, a fájlküldést, ha lehet mindenképpen korlátozott letöltési időre állítsa be és jelszóval védje, illetve adott időtartamon belül a fájlküldő szerver törölje azt a rendszerből. A küldés során a küldő felelőssége, hogy a szkennelt eredeti dokumentumok ne sérüljenek, és



eredeti ép állapotukban, biztonságosan kerüljenek tárolásra és visszaküldésre az Adatkezelő részére.

A vizsga kezdetén a vizsgázót azonosítani kell. Ez a személyazonosító okmányok megtekintésével történik, melyben a jegyző és a vizsgafelügyelő működik közre. Ennek során az okmányok fénymásolására nem kerülhet sor, kizárólag a megtekintett okmány adatok és az előzetesen a vizsgázó által megadott adatok összevetése történik meg. Amennyiben hibát (pl. elírás, további keresztnév) észlel az azonosítást végző, azt az adatbázisban javítja. Online vizsga esetén az azonosítás folyamatáról is felvétel készül, melyet 15 nap elteltével törölni kell.

Az online vizsgák elektronikus kapcsolattartásra használt csatornája esetében, amennyiben az EU-n kívüli adattovábbításra sor kerül, meg kell határozni ennek jogalapját (jellemzően a 49. cikk (1) bekezdés b) pontja) és meghozni a szükséges adatbiztonsági intézkedéseket.

A vizsgázó által készített projektfeladatot a szükséges, jogszabályban előírt mértékig kell dokumentálni, a vizsgázó azonosításához minimálisan szükséges személyes adattartalommal.

Amennyiben rendkívüli eseményre kerül sor (pl. szabálytalanság), vagy a vizsgázó panasszal él, a Kr. szerinti eljárásban, a feltétlenül szükséges személyes adatok rögzítésével kell dokumentálni. A jogorvoslati kérelmet az NSZFH-nak kell továbbítani.

Az adatkezelések jogalapja a Kr. vonatkozó rendelkezéseinek betartására, illetve a panaszok dokumentálása esetén a minőségbiztosításra vonatkozó Jogos érdek.

#### **25.4. Vizsgaeredmény megállapításával kapcsolatos adatkezelések**

A vizsgáról a jogszabályok szerint elkészítendő dokumentumokat (pl. vizsgajegyzőkönyv, törzslap) a vonatkozó előírások szerinti adattartalommal kell kiállítani, és az e-Kréta rendszerbe továbbítani (illetve a vizsga törzslapot az NSZFH részére is), valamint megőrizni.

A vizsgaeredményekről a vizsgázókat az Adatkezelő kiértesíti a jogszabályban meghatározott tartalommal, az adatokat az e-Kréta rendszerben rögzíti, továbbá részükre bizonyítványt állít ki és küld meg, amelynek sorszámát kell az e-Kréta rendszerben rögzíteni. A vizsgatörzslap és a bizonyítvány másolatát az NSZFH részére is továbbítja az Adatkezelő.

Az adatkezelések jogalapja a Kr. vonatkozó rendelkezéseinek betartására vonatkozó Jogos érdek.

#### **25.5 A vizsgáztatásban közreműködők adatainak kezelése**

A vizsga lebonyolításában közreműködő, jogszabályban meghatározott feladatkört ellátó személyek jelentkezés útján kerülnek kiválasztásra. A jelentkezés során azon személyes adatokat kezelheti az Adatkezelő, amelyek szükségesek a jelölt alkalmasságának megítéléséhez, azaz a személyazonosító adatokon felül a szakmai pályafutásra vonatkozó adatok, valamint az ezt alátámasztó dokumentumok (pl. végzettséget igazoló bizonyítvány). Ezen felül kizárólag kapcsolattartási adat (név, telefonszám) kérhető. Az adatok a Szerződés teljesítése (szerződés megkötéséhez szükséges adatok bekérése) és a kapcsolattartásra vonatkozó Jogos érdek alapján kezelhetők.

Amennyiben a jelöltet nem kívánja megbízni az Adatkezelő, a jelentkezés során megadott adatokat a jelentkező értesítését követően késedelem nélkül törölni kell. A megbízási szerződés megkötése esetén az 5 éves adatőrzési idő irányadó a közreműködő adatainak kezelésére.

A jelölt köteles részt venni egy belső vizsgaközponti képzésen, melyet az Fktv. szabályai alapján bonyolít az Adatkezelő, ennek megfelelően a Jogszabályi kötelezettség teljesítése jogalapon történik a képzésen keletkezett adatok és a kiadott tanúsítvány kezelése, valamint az adattovábbítás a Felnőttképzési Adatszolgáltatási Rendszerbe. A közreműködők személyéről az Oktatási Hivatal és az NSZFH-t is

értesíteni kell.

A megbízási szerződésben az azonosító és az ellátandó feladatra vonatkozó adatokon felül a megbízási díj és a kiegyenlítéséhez szükséges személyes adatok (adóazonosító jel/adószám, bankszámlaszám) is kezelendő, a Szerződés teljesítése és a Kr. előírásainak történő megfelelésre vonatkozó Jogos érdek jogalapon. A közreműködő partnerek adatait belső adatbázisban szükséges rögzíteni.

A vizsga lebonyolítása során a közreműködők pártatlanságát, az összeférhetetlenség kizárását biztosítani kell, az erre vonatkozó adatok kezelésére jogosult az Adatkezelő, a Kr. betartására vonatkozó Jogos érdeke alapján.

Az online vizsgák esetén készült felvételen a közreműködő is megjelenik, ezért az adatkezelési tájékoztatóban erre ki kell térni, az adatkezelés azonos módon történik a vizsgázóknál írtakkal.

A közreműködők feladata a vizsga dokumentálása, illetve az ebben történő részvétel, a papír alapú vizsgadokumentumokat aláírásukkal hitelesítik, valamint nevük, feladatkörük szerepel benne. Ezen dokumentumok kezelése is a vizsgázói adatkezelésnél leírtak szerint történik.

A megbízási szerződésben foglaltak szerint illeti meg díjazás a közreműködőt, amelyre való jogosultságról teljesítési igazolást állít ki az Adatkezelő. A közreműködő számlát állít ki, melynek feldolgozása során az Adatkezelő a könyvelési szolgáltatót, mint adatfeldolgozót veszi igénybe.

#### **25.6. Adattovábbítás**

Az adatkezelés során, amennyiben azt jogszabály előírja, az adatokat továbbítani kell az e-Kréta rendszerbe, az IKK Zrt., az NSZFH részére, vagy az Oktatási Hivatalnak. Ezen szervek címzettnek minősülnek, és saját adatkezelési szabályzatuk szerint kezelik a kapott adatokat. Amennyiben az adattovábbítási csatornát az Adatkezelő választhatja meg, lehetőség szerint a titkosítás vagy álnevesítés alkalmazása mellett kell a továbbítást megvalósítani.

Az adatfeldolgozók részére történő adattovábbítás szabályait az adatfeldolgozási megállapodásokban kell rögzíteni, a megfelelő IT biztonsági intézkedések alkalmazása mellett.

A szakképző intézmények továbbíthatnak vizsgázói adatokat az Adatkezelő részére.

Jelen Szabályzat 2022. szeptember 1. napján lép hatályba.