



DEBRECENI EGYETEM

BELSŐ ADATVÉDELMI SZABÁLYZATA

Hatályos 2021.szeptember 24. napjától

Tartalomjegyzék

<u>A SZABÁLYZAT CÉLJA</u>	5
<u>I. FEJEZET</u>	5
<u>A SZABÁLYZAT HATÁLYA ÉS ALAPFOGALMAK</u>	5
<i>A szabályzat tárgyi hatálya</i>	5
<i>A szabályzat személyi hatálya</i>	6
<i>Fogalom meghatározások</i>	7
<u>II. FEJEZET</u>	10
<u>AZ ADATKEZELÉS JOGSZERŰSÉGÉNEK ALAPVETŐ KÖVETELMÉNYEI</u>	10
<i>Az adatkezelés alapelvei</i>	10
<i>A hozzájárulás, mint jogalap alkalmazásának követelményei</i>	12
<i>A szerződéses jogalap alkalmazásának követelményei</i>	13
<i>Jogi kötelezettség jogalap alkalmazásának követelményei</i>	13
<i>Vis maior jogalap alkalmazásának követelményei</i>	14
<i>A jogos érdek, mint jogalap alkalmazásának követelményei</i>	14
<i>Különleges adatok kezelése</i>	15
<i>Előzetes tájékoztatás kötelezettsége</i>	16
<u>III. FEJEZET</u>	17
<u>AZ EGYETEM ÁLTAL VÉGZETT ADATKEZELÉSEKRE VONATKOZÓ KÖVETELMÉNYEK</u>	17
<i>Adatkezelési tevékenységek nyilvántartása</i>	17
<i>Tájékoztató megalkotására vonatkozó eljárásrend</i>	17
<i>A hallgatók adatainak kezelésével összefüggő követelmények</i>	18
<i>Hallgatói nyilvántartás</i>	18
<i>A foglalkoztatottak személyes adatainak kezelésére vonatkozó alapvető követelmények</i> ..	20
<i>Bér- és munkaügyi nyilvántartás</i>	22
<i>Az Egyetem által fenntartott Köznevelési intézményekben nyilvántartott és kezelt személyes és különleges adatok</i>	22
<i>Az Egyetem által fenntartott gyermekjóléti intézményben nyilvántartott és kezelt személyes és különleges adatok</i>	22
<u>IV. FEJEZET</u>	23
<u>ÉRINTETTI JOGGYAKORLÁS</u>	23
<i>A feladatok megoszlása az érintetti joggyakorlás során</i>	23
<i>Hozzáféréshez való jog</i>	23
<i>Másolat kéréséhez való jog</i>	24

<i>Helyesbítéshez való jog</i>	25
<i>Törléshez való jog</i>	25
<i>Elfeledtetéshez való jog</i>	25
<i>Korlátozáshoz való jog</i>	26
<i>Adathordozhatósághoz való jog</i>	27
<i>Tiltakozás joga</i>	28
<i>Az érintett azonosítása</i>	28
<i>A kérelem teljesítésének határideje</i>	29
<i>Az érintetti kérelem teljesítése</i>	29
<i>Az érintetti kérelem megtagadása</i>	30
V. FEJEZET	31
ALAPVETŐ ADATBIZTONSÁGI INTÉZKEDÉSEK	31
<i>Informatikai biztonsági intézkedések</i>	31
<i>Szervezési biztonsági intézkedések</i>	32
VI. FEJEZET	33
ADATVÉDELMI INCIDENSEK KEZELÉSE ÉS BEJELENTÉSE	33
<i>Adatvédelmi incidensek esetei</i>	33
<i>Tudomásszerzés az adatvédelmi incidensről</i>	34
<i>Adatkezelés felfüggesztése adatvédelmi incidens esetén</i>	34
<i>Az adatvédelmi incidens bejelentése és kivizsgálása</i>	35
<i>Az adatvédelmi incidens bejelentésének mellőzése</i>	36
<i>Érintettek tájékoztatása</i>	37
<i>Jegyzőkönyv a kivizsgálásról és az incidens-nyilvántartás</i>	38
VII. FEJEZET	39
ADATVÉDELMI TISZTVISELŐ ÉS AZ ADATVÉDELMI KÖZPONT	39
<i>Adatvédelmi tisztviselőre vonatkozó rendelkezések</i>	39
<i>Együttműködés a felügyeleti hatósággal</i>	41
<i>Adatvédelmi Központ</i>	41
<i>Területi adatvédelmi felelős</i>	41
VIII. FEJEZET	42
ADATKEZELÉSEL ÖSSZEFÜGGŐ TOVÁBBI KÖTELEZETTSÉGEK	42
<i>Adatfeldolgozó igénybevétele</i>	42
<i>Adatvédelmi hatásvizsgálat</i>	43
<i>Közös adatkezelés</i>	44

IX. FEJEZET	45
FELELŐSSÉG AZ ADATKEZELÉSI SZABÁLYOK BETARTÁSÁÉRT, ELLENŐRZÉS	45
X. fejezet	46
ADATTOVÁBBÍTÁS	46
Adattovábbítás	46
<i>Harmadik országba történő adattovábbítással összefüggő kötelezettségek</i>	46
<i>Adattovábbítási nyilvántartás</i>	48
XI. FEJEZET	48
<i>Elektronikus megfigyelő rendszer</i>	48
XII. FEJEZET	48
VEGYES ÉS ZÁRÓ RENDELKEZÉSEK	48
MELLÉKLETEK	50
<i>1. számú melléklet</i>	50
<i>2. számú melléklet</i>	53
<i>3. számú melléklet</i>	55
<i>4. számú melléklet</i> Adatkezelési nyilvántartás	60
<i>5. számú melléklet</i>	61
<i>6. számú melléklet</i>	62
<i>7. számú melléklet</i>	64
<i>8. számú melléklet</i>	65
<i>9. számú melléklet</i>	66
<i>10. számú melléklet</i>	67
<i>11. számú melléklet</i>	68
<i>12. számú melléklet</i>	71
<i>13. számú melléklet</i>	77
<i>14. számú melléklet</i>	80

A Debreceni Egyetem Szenátusa annak érdekében, hogy az alkalmazottakra, a hallgatókra és más érintettekre vonatkozó adatkezeléseit jogszerűen és tisztességesen, valamint az érintett számára átlátható módon végezze az EU 2016/679 rendelete a természetes személyeknek a személyes adatok tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint 95/46/EK rendelet hatályon kívül helyezéséről (a továbbiakban: európai általános adatvédelmi rendelet), továbbá az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Info tv.), a nemzeti felsőoktatásról szóló 2011. évi CCIV. törvény (a továbbiakban: Nftv.), a munka törvénykönyvéről szóló 2012. évi I. törvény (a továbbiakban: Mt.), a nemzeti felsőoktatásról szóló törvény egyes rendelkezéseinek végrehajtásáról szóló 87/2015. (IV. 9.) Korm. rendelet (a továbbiakban: Vhr.), a felsőoktatási felvételi eljárásról szóló 423/2012. (XII. 29.) Korm. rendelet (a továbbiakban: felvételi kormányrendelet), a felnőttképzésről szóló 2013. évi LXXVII. törvény (a továbbiakban: felnőttképzési törvény, a nemzeti köznevelésről szóló 2011. évi CXCV. törvény, a gyermekjóléti intézményekre, a pedagógus továbbképzésre, valamint egyéb vonatkozó jogszabályok alapján, összhangban az egyetemi szabályok rendelkezéseivel az alábbi belső szabályzatot (a továbbiakban: szabályzat) alkotja, amelyben bemutatja, hogy teljesíti a tevékenységére vonatkozó jogszabályokból fakadó adatvédelmi kötelezettségeket.

A SZABÁLYZAT CÉLJA

A szabályzat célja, hogy a Debreceni Egyetemen (a továbbiakban: Egyetem) vezetett adatkezelési nyilvántartások, az adatok kezelése, védelme a jogszabályoknak megfelelően, biztonságosan történjék, az Egyetem az európai általános adatvédelmi rendelet (GDPR) szabályainak megfelelően.

I. FEJEZET

A SZABÁLYZAT HATÁLYA ÉS ALAPFOGALMAK

A szabályzat tárgyi hatálya

1. §

- (1) A szabályzat kiterjed az Egyetem valamennyi adatkezelésére, függetlenül attól, hogy az adatkezelés alkalmazottakra, illetve munkavégzésre irányuló egyéb jogviszonyban foglalkoztatottakra, hallgatókra vagy más érintettekre vonatkozik.

- (2) Az egészségügyi nyilvántartás és adatkezelés speciális szabályait - jelen szabályzat és az egészségügyi adatok kezelésére vonatkozó egyéb jogszabályok alapján - az Egyetem külön szabályzatban határozza meg.

Szabályzat elérhetősége:

<https://mad-hatter.it.unideb.hu/portal/displayDocument/id/2355067>

A szabályzat személyi hatálya

2. §

- (1) A jelen szabályzat személyi hatálya kiterjed:

- a) az Egyetem hallgatójára, függetlenül az oktatás formájára,
- b) az Egyetem fenntartásában működő köznevelési intézményekben óvodai nevelésben, oktatásban résztvevőkre, bölcsődei ellátásban részesülő gyermekekre, törvényes képviselőikre,
- c) az a) pont szerinti jogviszonyban nem álló, habilitációs eljárásra jelentkező, illetve ilyen eljárásokban részt vevő személyekre, valamint a doktorjelölti jogviszonyban álló személyekre,
- d) az Egyetem foglalkoztatottjára, függetlenül attól, hogy alkalmazására milyen jogviszonyban kerül sor (ideértve a megbízási vagy más munkavégzésre irányuló egyéb jogviszonyban foglalkoztatott személyeket is),
- e) az a) és d) pont szerinti jogviszonyban nem álló, az Egyetem által szervezett, bonyolított felnőttképzésben, tanfolyamon (a továbbiakban: együtt felnőttképzés), pedagógus-továbbképzésben részt vevő; doktori fokozatszerzési eljárásra jelentkező, illetve ilyen eljárásokban részt vevő, valamint az Egyetem könyvtári rendszerét használó személyekre,
- f) az adatkezelést végző valamennyi egyetemi szervezeti egységére,
- g) egyes címekkel (pl.: a professzor emeritus és a professzor emerita, doctor honoris causa címmel) rendelkezőkre,
- h) továbbá azon személyekre, akik az Egyetemmel nem állnak jogviszonyban, azonban adataikat az Egyetem – jogviszony létesítése céljából, valamint a jogviszony megszűnését követően – kezeli, vagy személyes adataikat jogszabályi előírás alapján kezelni köteles, illetve azon személyekre, akik az Egyetem adatkezelési tevékenységében bármilyen jogcímen részt vesznek, ideértve például a tudományos munkában részt vevő középiskolás hallgatókat is.

Fogalom meghatározások

3. §

- (1) **Érintett:** bármely információ alapján azonosított, vagy azonosítható természetes személy. Azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító, vagy egy, vagy több tényező alapján azonosítható.
- (2) **Személyes adat:** azonosított vagy azonosítható természetes személyre vonatkozó bármely információ.
- (3) **Különleges adat:** a szabályzat alapján különleges adatnak minősülnek elsődlegesen az egészségügyi adatok. Különleges adatnak tekinthető továbbá a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adat, valamint a természetes személyek egyedi azonosítását célzó genetikai és biometrikus adat, a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok.
- (4) **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.
- (5) **Üzleti partnerek kapcsolattartói:** azok a természetes személyek, akik valamely jogi személy vagy más szervezet képviselőjeként az Egyetemmel való kapcsolatuk során az Egyetem rendelkezésére bocsátják a személyes adataikat. Az üzleti partnerek kapcsolattartóira vonatkozó rendelkezéseket megfelelően alkalmazni kell az egyéni vállalkozókra is.
- (6) **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.
- (7) **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.

- (8) **Adattovábbítás:** az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele.
- (9) **Nyilvánosságra hozatal:** az adat bárki számára történő hozzáférhetővé tétele.
- (10) **Adattörlés:** az adat felismerhetetlenné tétele oly módon, hogy a helyreállítása többé nem lehetséges.
- (11) **Adatkezelés korlátozása:** a tárolt adat zárolása az adat további kezelésének korlátozása céljából történő megjelölés útján.
- (12) **Adatmegsemmisítés:** az adatot tartalmazó adathordozó teljes fizikai megsemmisítése.
- (13) **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.
- (14) **Adatfeldolgozó:** az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az Adatkezelő nevében személyes adatokat kezel.
- (15) **Harmadik fél:** az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely nem azonos az érintettel, az adatkezelővel, az adatfeldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére felhatalmazást kaptak.
- (16) **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.
- (17) **Hozzájárulás:** az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez.
- (18) **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.
- (19) **Üzleti titok:** a közérdekű vagy közérdekből nyilvános adatnak nem minősülő, az Egyetem gazdasági tevékenységéhez kapcsolódó minden nem közismert vagy az

érintett gazdasági tevékenységét végző személyek számára nem könnyen hozzáférhető olyan tény, tájékoztatás, egyéb adat és az azokból készült összeállítás, amelynek illetéktelenek által történő megszerzése, hasznosítása, másokkal való közlése vagy nyilvánosságra hozatala az Egyetem jogos pénzügyi, gazdasági vagy piaci érdekét sértené vagy veszélyeztetné, feltéve, hogy a titok megőrzésével kapcsolatban a vele jogszerűen rendelkező jogosultat felróhatóság nem terheli. Az üzleti titokkal azonos védelemben részesül az azonosításra alkalmas módon rögzített, vagyoni értéket képviselő műszaki, gazdasági vagy szervezési ismeret, tapasztalat vagy ezek összeállítása (védett ismeret).

- [20] **Banktitok:** minden olyan tény, információ, megoldás vagy adat, amely valamely pénzügyi intézménynél az Egyetem vagyoni helyzetére, üzleti tevékenységére, gazdálkodására, tulajdonosi, üzleti kapcsolataira, valamint a pénzügyi intézmény által vezetett számlájának egyenlegére, forgalmára, továbbá a pénzügyi intézménnyel kötött szerződéseire vonatkozik.
- [21] **GDPR:** az Európai Parlament és a Tanács 2016. április 27-i (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/37/EK irányelv hatályon kívül helyezéséről (európai általános adatvédelmi rendelet). A rendeletnek a gyakorlatban elterjedt rövidítése az angol elnevezéséből (General Data Protection Regulation) képzett GDPR mozaikszó.
- [22] **Irányadó jog:** a GDPR, illetve a rendelkezéseinek értelmezésével összefüggésben kiadott 29. cikk szerinti Adatvédelmi Munkacsoport véleményei, iránymutatásai, és az Európai Adatvédelmi Testület dokumentumai, valamint a GDPR által biztosított felhatalmazás alapján vagy erre tekintettel megalkotott magyar jogszabályok, más adatvédelmi tárgyú jogszabályok, valamint a Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: **NAIH**) által kiadott dokumentumok, illetve az Egyetemre, az adatkezelőre vagy az adatfeldolgozóra vonatkozó magatartási kódexek.
- [23] **EGT-állam:** Az Európai Unió tagállama és az Európai Gazdasági Térségről szóló megállapodásban részes más állam, továbbá az az állam, amelynek állampolgára az Európai Unió és tagállamai, valamint az Európai Gazdasági Térségről szóló megállapodásban nem részes állam között létrejött nemzetközi szerződés alapján az Európai Gazdasági Térségről szóló megállapodásban részes állam állampolgárával azonos jogállást élvez.
- [24] **Harmadik ország:** Minden olyan állam, amely nem EGT-állam.
- [25] **Adatvédelmi tisztviselő:** a személyes adatok védelmére vonatkozó jogi előírások és jogalkalmazási gyakorlat megfelelő szintű ismeretével rendelkező, az egyetem kancellárja által megbízott személy, aki alkalmas az Info tv. 25/M. § (1) bekezdésében meghatározott feladatok ellátására.

- (26) **Jogi képviselő:** az Egyetem által megbízott ügyvéd, európai közösségi jogász, külföldi jogi tanácsadó, kamarai jogtanácsos, alkalmazott ügyvéd, alkalmazott európai közösségi jogász, ügyvédjelölt és ügyvédi kamarai nyilvántartásba vett jogi előadó, aki az adatvédelmi tárgyú ügyekben az Egyetem képviseletében eljár vagy közreműködik az ilyen ügyek elintézésében.
- (27) **Adatvédelem:** olyan eljárások összessége, amelynek célja, a természetes személyek személyes adatainak védelme.
- (28) **Adatbiztonság:** tárgya maga az adat, amely az adat bizalmosságának a védelmét jelenti, megteremtését technikai, szervezési intézkedések szolgálják.
- (29) **Magáncélú felhasználás:** személyes adatoknak minden olyan célra történő felhasználása, amely jelen szabályzatban meghatározott jogalap hiányában történik.
- (30) **Szervezeti egység:** A Debreceni Egyetem mindenkor hatályos Szervezeti és Működési Szabályzatában az egyetem szervezete részben felsorolt oktatási és tudományos kutatási szervezeti egységek, szolgáltató és igazgatási szervezeti egységek, funkcionális szervezeti egységek, és a Hallgatói Önkormányzat.
- (31) **Jogalap:** a jog által meghatározott azon esetek köre, amikor a személyes adatok kezelése törvényes.

II. FEJEZET

AZ ADATKEZELÉS JOGSZERŰSÉGÉNEK ALAPVETŐ KÖVETELMÉNYEI

Az adatkezelés alapelvei

4. §

- (1) Amennyiben az Egyetem határozza meg az adatkezelés körülményeit, módját, akkor az adatkezelésnek meg kell felelnie a GDPR-ban foglalt alapelveknek, illetve a jelen szabályzatban kifejtett követelményeknek.
- (2) Személyes adatok csak abban az esetben kezelhetők, ha az adatkezelés célját egyéb eszközzel észszerű módon nem lehetséges elérni.
- (3) Az Egyetemnek az adatkezelést úgy kell megterveznie és végeznie, hogy a személyes adatok kezelése jogszerű és tisztességes, valamint az érintett számára átlátható legyen [jogszerűség, tisztességes eljárás és átláthatóság]. Az

Egyetemnek a személyes adatok kezeléséhez megfelelő joggalappal kell rendelkeznie. Az Egyetem csak akkor kezelhet személyes adatot, ha az adatkezeléshez a GDPR 6. cikk, 8. cikk vagy 9. cikk szerinti joggalappal rendelkezik, és a jogalap alkalmazásával összefüggésben teljesülnek az irányadó jogban előírt követelmények. Az Egyetem azokat az adatokat tarthatja nyilván, amelyek a GDPR 6. cikk (1) bekezdés e) pontja alapján közérdekű feladatának ellátásához, rendeltetésszerű működéséhez, a munkáltatói jogok gyakorlásához, a képzés megszervezéséhez stb. nélkülözhetetlenek, továbbá amelyek a jogszabályokban és a szervezeti és működési szabályzatában biztosított kedvezményekre való igényjogosultság elbírálásához és igazolásához szükségesek.

- (4) Az Egyetemnek az adatkezelés meghatározása során biztosítani kell, hogy adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történjék. Az adatkezelés céljának kifejezettnek, pontosan megfogalmazottnak és jogszerűnek, továbbá már az adatkezelés megkezdésének időpontjában meghatározottnak kell lennie. A személyes adatok nem kezelhetők az eredeti adatkezelési célokkal össze nem egyeztethető módon (célhoz kötöttség).
- (5) Az Egyetemnek az adatkezelést úgy kell megterveznie és végeznie, hogy a személyes adatok, az adatkezelés céljai szempontjából megfelelőek és relevánsak legyenek, és a kezelésük a szükséges mértékre korlátozódjék. Az Egyetemnek biztosítani kell különösen azt, hogy a személyes adatok tárolása a lehető legrövidebb időtartamra korlátozódjék. Ennek biztosítása érdekében az Egyetem az adatkezelés céljához vagy a jogszabályi kötelezettségekhez igazodó tárolási határidőt állapít meg. (adattakarékosság, korlátozott tárolhatóság)
- (6) Az Egyetemnek biztosítani kell azt, hogy a személyes adatok az adatkezelés során pontosak és szükség esetén naprakészek legyenek. (pontosság)
- (7) Az Egyetemnek az adatkezelést úgy kell megterveznie és végeznie, hogy a személyes adatok tárolása olyan formában történjék, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé. (korlátozott tárolhatóság)
- (8) Az Egyetemnek az adatkezelés megtervezése során figyelemmel kell lennie arra, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve. (integritás és bizalmas jelleg)
- (9) Az Egyetem felelős azért, hogy az adatkezelés megfeleljen a GDPR 5. cikk (1) bekezdésének. Az Egyetemnek képesnek kell lennie arra, hogy igazolja azt, hogy az adatkezelése megfelel a GDPR 5. cikk (1) bekezdésének. Ezen kötelezettség

teljesítésében valamennyi alkalmazottat, az Egyetemmel szerződéses viszonyban álló adatkezelőt és adatfeldolgozót közreműködési kötelezettség terhel. (elszámoltathatóság)

A hozzájárulás, mint jogalap alkalmazásának követelményei

5. §

- (1) Az Egyetem a hozzájárulás jogalapját kizárólag akkor alkalmazhatja, ha jelen szabályzat és az irányadó jog alapján a hozzájárulással összefüggésben előírt követelmények teljesülnek.
- (2) Az Egyetemnek képesnek kell lennie annak igazolására, hogy az érintett személyes adatainak kezeléséhez hozzájárult. Ezen kötelezettségének az Egyetem elsődlegesen elektronikus úton történt naplózással vagy az érintett által tett írásbeli hozzájárulásnak a megőrzése útján tesz eleget.
- (3) Az Egyetemnek az adatkezelés során biztosítani kell azt, hogy adatkezelésre csak akkor kerüljön sor, ha az érintett egyértelmű megerősítő cselekedettel, például írásbeli – ideértve az elektronikus úton tett –, vagy szóbeli nyilatkozattal önkéntes, konkrét, előzetes tájékoztatáson alapuló és egyértelmű hozzájárulását adja az adatkezeléshez. Ha az érintettől a hozzájárulást az Egyetem honlapjain keresztül kéri, akkor ezt a megfelelő informatikai megoldással teszi meg (pl.: a jelölőnégyzetet (checkbox) kell elhelyeznie, amelyen keresztül az érintettől hozzájárulását szerezheti be).
- (4) A hallgatás, az előre bejelölt négyzet vagy a nem cselekvés nem minősül hozzájárulásnak.
- (5) Az Egyetemnek az adatkezelés megtervezése és végrehajtása során biztosítani kell azt, hogy az érintett adatkezelési célonként külön-külön tudjon hozzájárulni a különböző célú adatkezelésekhez.
- (6) Ha az érintett hozzájárulását olyan írásbeli nyilatkozat keretében adja meg, amely más ügyekre is vonatkozik, az Egyetemnek biztosítania kell azt, hogy a hozzájárulás iránti kérelmet ezektől a más ügyektől egyértelműen megkülönböztethető módon adja elő, érthető és könnyen hozzáférhető formában, világos és egyszerű nyelvezettel. Az Egyetemnek az elektronikus vagy papír alapú formanyomtatványain biztosítani kell, hogy a hozzájárulást kérő szövegrészek elkülönüljenek a formanyomtatvány többi részétől.
- (7) Az érintett hozzájárulásának önkéntesnek kell lennie, ennek biztosítása érdekében az Egyetemnek figyelembe kell venni, hogy
 - a) nem teheti szerződés teljesítését attól függővé, hogy az érintett hozzájárul-e olyan adatkezeléshez, amely nem szükséges a szerződés teljesítéséhez,

- b) az érintett valós vagy szabad választási lehetőséggel rendelkezék, és lehetősége legyen a hozzájárulás anélküli megtagadására vagy visszavonására, hogy ez kárára válna,
 - c) az Egyetem és az érintett között ne álljon fenn olyan egyenlőtlen viszony, amely miatt valószínűtlen, hogy a szóban forgó hozzájárulás megadása önkéntesen történt.
- (8) Az Egyetemnek a hozzájárulás visszavonását ugyanolyan egyszerű módon kell lehetővé tenni, mint annak megadását.
- (9) Az Egyetem az alkalmazottakat érintő adatkezelések esetében kivételesen, csak abban az esetben alkalmazhatja a hozzájárulás jogalapját, ha a fenti követelmények teljesülnek.
- (10) Az érintett hozzájárulását megadottnak kell tekinteni az érintett közszereplése során általa közölt, vagy nyilvánosságra hozatalra általa átadott személyes adatok tekintetében.
- (11) Kétség esetén azt kell vélelmezni, hogy az érintett a hozzájárulását nem adta meg.

A szerződéses jogalap alkalmazásának követelményei

6. §

- (1) Az Egyetem a szerződéses jogalapot kizárólag akkor alkalmazhatja, ha jelen szabályzat és az irányadó jog által a szerződéses jogalappal összefüggésben előírt követelmények teljesülnek.
- (2) A szerződéses jogalap alkalmazása során, az Egyetemnek igazolnia kell, hogy
- a) az érintettel kötött szerződés teljesítéséhez szükséges meghatározott személyes adatok kezelése,
 - b) az adatkezelés a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges.

Jogi kötelezettség jogalap alkalmazásának követelményei

7. §

- (1) Az Egyetem a jogi kötelezettség jogalapját kizárólag akkor alkalmazhatja, ha a jelen szabályzat és az irányadó jog alapján előírt követelmények teljesülnek.
- (2) Jogi kötelezettség jogalapjának alkalmazásához az Egyetemnek meg kell jelölnie azt az uniós vagy hazai jogszabályt, amely a személyes adatok kezelését előírja, vagy amely a személyes adatok kezelését szükségessé teszi.

- (3) Amennyiben a jogszabály meghatározza az adatkezelés körülményeit, akkor az Egyetem más célból nem kezelheti az adatokat, az adatkezelés időtartamától nem térhet el, és más személyes adatokra nem terjesztheti ki az adatkezelést.
- (4) Amennyiben a jogi kötelezettséget meghatározó jogszabály nem rendezi az adatkezelés célját, időtartamát, a kezelt adatok körét, illetve az adatkezelés feltételeit, akkor azt az Egyetemnek a jelen szabályzat 4. §-ában szereplő alapelvek és az irányadó jog követelményeinek betartásával kell meghatározni azokat.

Vis maior jogalap alkalmazásának követelményei

8. §

- (1) Az Egyetem valamennyi polgára jogosult arra, hogy az érintett létfontosságú érdekeinek védelméhez szükséges személyes adatokat kezelje. (Ilyennek tekinthető pl.: az, ha az érintetthez mentőt kell hívni, és ennek során közölni kell az érintett személyes adatait vagy egészségügyi adatait.)
- (2) Amennyiben az Egyetem bármely alkalmazottja a vis maior jogalap alkalmazásával személyes adatokat továbbít, azonban az érintett vagy más személy vitatja az adattovábbítás jogszerűségét, az Egyetem közreműködik az adatkezelés körülményeinek tisztázásában.

A jogos érdek, mint jogalap alkalmazásának követelményei

9. §

- (1) Az Egyetem a jogos érdek jogalapját kizárólag akkor alkalmazhatja, ha a jelen szabályzat és az irányadó jog alapján az érdekmérlegelés jogalapjával összefüggésben előírt követelményei teljesülnek.
- (2) Az Egyetem jogos érdekének vagy harmadik fél jogos érdekének ténylegesnek, egyértelműnek és jogszerűnek kell lennie. Az Egyetemnek törekednie kell arra, hogy amennyiben lehetséges, írásbeli dokumentummal (például szerződéssel, NAIH állásfoglalásával, határozatával, más uniós tagállami adatvédelmi hatóság döntésével) igazolja a jogos érdekét.
- (3) A jogos érdek fennállásának megállapításához az Egyetemnek meg kell vizsgálnia többek között azt, hogy az érintett a személyes adatok gyűjtésének időpontjában és azzal összefüggésben számíthat-e észszerűen arra, hogy adatkezelésre az adott célból kerülhet sor. Jogos érdekről lehet szó például olyankor, amikor releváns és megfelelő kapcsolat áll fenn az érintett és az Egyetem között, például olyan esetekben, amikor az érintett az Egyetem polgára.
- (4) Az Egyetemnek a jogos érdekjogalapjának alkalmazásához be kell mutatnia az érintettek jogos érdekeit és elvárásait érdekmérlegelési teszt elkészítésével.

Amennyiben lehetséges, az Egyetemnek ki kell kérnie az érintettek vagy képviselőik véleményét a tervezett adatkezelésről. Ha az Egyetem elmulasztja az érintett érdekeinek bemutatását, az adatkezelés nem végezhető el.

- (5) Ahhoz, hogy az Egyetemnek az érdekmérlegelés jogalapjának az alkalmazásával végzett adatkezelése ne korlátozza aránytalanul az érintettek jogait és szabadságait, megfelelő garanciális intézkedéseket kell hoznia. Amennyiben lehetséges, az Egyetemnek ki kell kérnie az érintettek vagy képviselőik véleményét a tervezett garanciális intézkedésekről. Ha az Egyetem elmulasztja a garanciális intézkedések bemutatását, az adatkezelés nem végezhető el.
- (6) Amennyiben az egyetemi szervezeti egység a jogos érdek jogalapját kívánja alkalmazni, akkor a jelen szabályzat **1. számú melléklete** szerinti kérdéssor felhasználásával kell igazolnia a tervezett adatkezelés jogszerűségét, és érdekmérlegelési tesztet szükséges készítenie. (**2. számú melléklet**).

Különleges adatok kezelése

10. §

- (1) Az Egyetem különleges adatot akkor kezelhet, ha jogszabály kifejezetten előírja valamely különleges adat kezelését, vagy a jogszabályi kötelezettség teljesítéséhez nyilvánvalóan szükséges a különleges adat kezelése.
- (2) Az Egyetem az érintett kifejezett hozzájárulása alapján akkor kezelhet különleges adatot, ha az érintett valamely őt megillető jog gyakorlásának érdekében adja meg az Egyetem számára. Az érintett nyilatkozatából, közléséből ki kell derülnie annak a körülménynek, hogy az érintett tisztában van azzal, hogy a különleges adatot milyen őt megillető jog gyakorlása érdekében adja meg.
- (3) Amennyiben a különleges adatok kezelése jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez szükséges, akkor az Egyetemnek dokumentálnia kell, hogy miért szükséges a különleges adat kezelése (felhasználása, továbbítása). Dokumentációként elfogadható az is, ha az eljárás során készített bármely iratban az Egyetem kifejezetten kitér a különleges adat kezelésének (felhasználásának, továbbításának) szükségességére.

Előzetes tájékoztatás kötelezettsége

11. §

- (1) Az Egyetemnek valamennyi adatkezeléséről tájékoztatni kell az érintetteket. Amennyiben az Egyetem előzetesen nem tájékoztatja az adatkezelésről az érintetteket, az adatkezelés nem végezhető el.
- (2) Az Egyetem a tájékoztatási kötelezettségét adatkezelési tájékoztatók megalkotásával és nyilvánosságra hozatalával vagy közlésével teljesíti. Minden szervezeti egység köteles a saját tevékenységi körét érintően adatkezelési tájékoztatót készíteni. **(3. számú melléklet)** Egy szervezeti egység vezetője jelentősen összetett feladatok ellátása esetén - szükségszerűen- dönthet akként is, hogy a szervezeti egység több adatkezelési tájékoztatót készít. Kivételesen elfogadható az is, ha az Egyetem valamely adatkezeléshez kapcsolódóan eseti tájékoztatást ad át az érintetteknek.
- (3) Amennyiben az Egyetem a személyes adatokat az érintettől veszi fel, akkor az adatkezelési tájékoztatónak az alábbi adatkezelési körülményekre kell kiterjednie:
 - a) az Egyetem neve, székhelye, központi e-mail címe, adott szervezeti egység neve, képviselője, elérhetősége,
 - b) az adatkezelési tevékenység megnevezése, célja, kezelt adatok köre, jogalapja, illetve a személyes adatok tárolásának időtartama, vagy ha ez nem lehetséges, akkor ezen időtartam meghatározásának szempontjai,
 - c) jogos érdek jogalapjának alkalmazása esetén az Egyetem vagy harmadik fél jogos érdekei,
 - d) a személyes adatok címzettjei vagy a címzettek kategóriái,
 - e) az érintettet megillető jogok, illetve a NAIH-hoz fordulás lehetősége,
 - f) a hozzájárulás, illetve az arra vonatkozó tájékoztatás bármely időpontban való visszavonásához való jog, illetve az arra vonatkozó tájékoztatás, hogy ez nem érinti a visszavonás előtt a hozzájárulás alapján végrehajtott adatkezelés jogszerűségét,
 - g) a személyes adatok megadása jogszabályon alapul-e vagy szerződés kötésének előfeltétele-e, valamint, hogy az érintett köteles-e a személyes adatokat megadni, továbbá hogy milyen lehetséges következményekkel járhat az adatszolgáltatás elmaradása.
- (4) Amennyiben az Egyetem a személyes adatokat nem az érintettől kapja meg, akkor az adatkezelési tájékoztatóban meg kell jelölni, hogy milyen forrásból szerezte meg a személyes adatokat.
- (5) Az adatkezelési tájékoztatónak átláthatónak kell lenni. A tájékoztatót bekezdésekre kell tagolni, és ahol szükséges, felsorolást kell alkalmazni a szöveg könnyebb áttekinthetősége, olvashatósága érdekében.

- (6) Az adatkezelési tájékoztatót könnyen hozzáférhető formában kell rendelkezésre bocsátani.
- (7) Az adatkezelési tájékoztatót közérthetően kell megfogalmazni. Az adatkezelési tájékoztatóban kerülni kell a jogszabály szó szerinti megismétlését, és törekedni kell az egyszerű, világos megfogalmazásra.

III. FEJEZET

AZ EGYETEM ÁLTAL VÉGZETT ADATKEZELÉSEKRE VONATKOZÓ KÖVETELMÉNYEK

Adatkezelési tevékenységek nyilvántartása

12.§

- (1) Minden szervezeti egység a felelősségi körébe tartozóan végzett adatkezelési tevékenységekről nyilvántartást vezet.
- (2) A nyilvántartás elemeit a 4. számú melléklet tartalmazza.
- (3) Az adatkezelési nyilvántartást az Egyetem szervezeti egységeinek az Adatvédelmi Központ részére meg kell küldeni.

Tájékoztató megalkotására vonatkozó eljárásrend

13. §

- (1) Az egyetemi szervezeti egységnek az adatkezelési tájékoztatóra vonatkozó javaslatát az Egyetem Adatvédelmi Központjának kell továbbítani. Az Adatvédelmi Központ a javaslatot véleményezi az irányadó joggal, jelen szabályzattal és más belső szabályzatokkal, utasításokkal való összhang szempontjából. Véleményezést követően az adatkezelési tájékoztatót a helyben szokásos és általában ismert módon vagy a honlapon közzé kell tenni. Az Egyetem az egyes szervezeti egységekre vonatkozó adatkezelési tájékoztatókat összegyűjtve az Egyetem honlapján Adatkezelési tájékoztatók cím alatt is közzéteszi.

A hallgatók adatainak kezelésével összefüggő követelmények

14. §

- (1) A nemzeti felsőoktatásról szóló 2011. évi CCIV. törvény (a továbbiakban: Nftv.) 3. számú melléklet I/B. pontja alapján az Egyetem a felvétellel összefüggésben személyes adatokat kezel.
- (2) Az Egyetem a hallgatói jogviszony létesítését követően az Nftv. 3. számú mellékletének I/B. pontja alapján kezeli a személyes adatokat.
- (3) Az Egyetem a személyes adatokat a hallgatói jogviszony megszűnésétől számított nyolcvan évig őrzi meg.

Hallgatói nyilvántartás

15. §

- (1) A hallgatói nyilvántartás a hallgatói jogviszonyra vonatkozó tények dokumentálására szolgáló adatkezelés, melynek jogszabályi alapját az Nftv., az Nftv.vhr., az Egyetem Szervezeti és Működési Szabályzata, a Hallgatói Térítési és Juttatási Szabályzata, valamint a Tanulmányi és Vizsgaszabályzata, Doktori Szabályzata, illetve egyéb vonatkozó szabályzatai képezik.
- (2) A hallgatói nyilvántartás céljából az Egyetem egyetlen integrált informatikai rendszert üzemeltet, a Neptun Egységes Tanulmányi Rendszert.
- (3) A hallgatói nyilvántartás adatai a hallgató tanulmányi és vizsgakötelezettségeinek teljesítésével, valamint az ösztöndíj illetve költségtérítés, térítési díj stb. megállapításával, folyósításával illetve megfizetésével és minden, a hallgatói jogviszonnyal kapcsolatos szervezési és adminisztratív feladat ellátásával kapcsolatos tevékenységhez használhatók fel.
- (4) A Neptun Egységes Tanulmányi Rendszer egyetemi szintű koordinációjáról, a rendszer működtetésében, fejlesztésében, karbantartásában közreműködő szervezetek munkájának összehangolásáról a Hallgatói Kapcsolatok és Szolgáltatások Központja gondoskodik.
- (5) A hallgatói nyilvántartás adatait a felvételi adatbázis, valamint a hallgató által kitöltött beiratkozási lapok szolgáltatják. Az oktatási és adminisztratív feladatok ellátásában közreműködő személyek adatait a szervezeti egységek a saját nyilvántartásuk alapján töltik fel a rendszerbe. Az adatbázisba bekerülő adatok forrása kizárólag elektronikus úton előállított vagy papíralapú dokumentum lehet. Szóbeli közlés alapján az adatbázisba semmilyen adat nem kerülhet be.

(6) Az adatrögzítés módja:

Az adatbázisban rögzített adatok nem térhetnek el az adat forrásául szolgáló dokumentumban szereplő adattól. Az adatok egyezőségéért az adatrögzítő személy felelősséggel tartozik.

Amennyiben az adatok forrásául szolgáló dokumentumban szereplő adat értelmezhetetlen, olvashatatlan, ellentmondásos vagy hiányos, az adat nem vihető be az adatbázisba. Ilyen esetben az adat forrásául szolgáló dokumentum kijavítását, illetve kiegészítését kell kérni az adatalanytól, vagy ha az adat nem az adatalanytól származik, akkor az eredeti dokumentum kiállítójától.

(7) A hallgató adatainak kezelője annak a karnak - illetve karoknak - a tanulmányi hivatala, illetve tanszékeinek alkalmazottja, amelynek keretében a hallgató tanulmányait folytatja. A hallgatóval kapcsolatos adatokat a Neptunban kezeli még a HKSZK (ezen belül ETIK, HAK, Kollégium, Mentálhigiénés és Esélyegyenlőségi Központ), valamint a NOKK, Nemzetközi Iroda, Doktori Tanácsok, a szerepkörben beállított jogosultságuk és feladatkörük szerint.

(8) A Neptun Egységes Tanulmányi Rendszer adatait védeni kell a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés ellen. Ezen védelem biztosítása a rendszer üzemeltetőjének, az Informatikai Szolgáltató Központnak (ISZK), valamint a Hallgatói Kapcsolatok és Szolgáltatások Központjának (HKSZK), továbbá az adatkezelést, illetve adatfeldolgozást végző személyeknek és szervezeti egységeknek a feladata.

(9) A rendszert üzemeltető Informatikai Szolgáltató Központ a szervergépeken tárolt adatok biztonsága érdekében a következő intézkedéseket teszi és azokat folyamatosan magas színvonalon biztosítja:

a) a szervergépeket megfelelő fizikai védelemmel ellátott, zárt helyiségben tárolja. A szervergépek működésének környezeti és műszaki feltételeit biztosítja;

b) a személyes adatokat tartalmazó adatbázisok aktív adataiból napi rendszerességgel biztonsági mentést készít. A biztonsági mentésnek és az éles adatbázisnak különböző telephelyen található tároló eszközökön kell lennie;

c) biztosítja, hogy a személyes adatokat tartalmazó szerverek közvetlen hálózati úton ne legyenek elérhetőek, és a rendszer feltörése hálózati hozzáféréssel ne legyen lehetséges;

d) gondoskodik arról, hogy áramkimaradás esetén a szervergépek szabályosan, adatvesztés nélkül leállíthatók legyenek;

- e) gondoskodik a szervergépek vírusvédelméről;
- f) amennyiben az adatbázisszerver elérése terminálszervereken keresztül történik, úgy gondoskodik a terminálszerverekre történő belépéshez szükséges azonosítók és jelszavak kiosztásáról és visszavonásáról, az adatkezelés céljának minimálisan megfelelő jogosultságok beállításáról;
- g) a szerver és az informatikai rendszer rendszergazdai jelszavát tűzbiztos fémkazettában elzárva kell őrizni. A jelszavak változtatását legalább fél éves gyakorisággal el kell végezni.
- (10) A Neptun Egységes Tanulmányi Rendszernek lehetővé kell tennie az adatmódosítások tényének, időpontjának és végrehajtójának naplózását. A HKSZK a rendszert úgy állítja be, hogy a naplózás megtörténjen.
- (11) Hallgatói adatok nyilvántartása a kollégiumban: A Debreceni Egyetem integrált informatikai rendszerében tárolt adatokon kívül, a kollégiumi felvételi adatbázis, illetve a hallgató által kitöltött beiratkozási lap adatai képezik a kollégium hallgatói nyilvántartásának alapját. A nyilvántartás adatai felhasználhatók a kollégiumi jogviszonnyal kapcsolatos szervezési és adminisztratív feladatok ellátására. A kollégiumi nyilvántartó rendszer működtetéséről, fejlesztéséről, az abban tárolt adatoknak a Debreceni Egyetem Belső adatvédelmi Szabályzatában leírtak szerinti kezeléséről a Hallgatói Kapcsolatok és Szolgáltatások Központja Egyetemi Kollégiumi Igazgatóság gondoskodik, a területi adatvédelmi felelős koordinálásával.
- (12) Hallgatói adatok nyilvántartása a kollégiumi felvételi és rendszeres szociális ösztöndíj rendszerben: A kollégiumi, diákotthoni felvételi, valamint a rendszeres szociális ösztöndíj eljárást az Nftv. alapján működő egyetemi Kollégiumi Felvételi és Szociális Bizottság (KFSZB) folytatja le a mindenkori hatályos jogszabályoknak megfelelően. A pályázatokhoz kért személyes adatok körét a vonatkozó jogszabályokban foglaltak alapján a Szenátus által jóváhagyott Hallgatói Térítési és Juttatási Szabályzat határozza meg.

A foglalkoztatottak személyes adatainak kezelésére vonatkozó alapvető követelmények

16. §

- (1) Az Egyetem kezeli az Nftv. 3. számú mellékletben rögzített alkalmazotti adatokat,
- (2) A felsőoktatási intézmény a személyes és különleges adatokat csak a foglalkoztatással, juttatások, kedvezmények, kötelezettségek megállapításával és teljesítésével kapcsolatosan, továbbá nemzetbiztonsági okból, az e törvényben meghatározott nyilvántartások kezelése céljából, célnak megfelelő mértékben, célhoz kötötten kezelheti.

- (3) Az (1) bekezdésben meghatározott adatok kezelője a Humán Gazdálkodási Igazgatóság, valamint a rektor munkáltatói jogkörébe tartozók esetében a Rektori Kancellári Kabinet Oktatói-Kutatói Humánpolitikai Osztály, továbbá az egyes szervezeti egységek munkáltatói jogkör gyakorlója által kijelölt személyek.
- (4) Az Egyetem a személyes adatokat a foglalkoztatás megszűnésétől az iratkezelési szabályzatnak megfelelő időtartamig őrzi meg.
- (5) Az informatikai rendszert üzemeltető Informatikai Szolgáltató Központ a szervergépeken tárolt adatok biztonsága érdekében a következő intézkedéseket teszi és azokat folyamatosan magas színvonalon biztosítani köteles:
- a) a szervergépeket megfelelő fizikai védelemmel ellátott, zárt helyiségben tárolja. A szervergépek működésének környezeti és műszaki feltételeit biztosítja;
 - b) a személyes adatokat tartalmazó adatbázisok aktív adataiból napi rendszerességgel biztonsági mentést készít. A biztonsági mentésnek és az éles adatbázisnak különböző telephelyen található tároló eszközökön kell lennie;
 - c) biztosítja, hogy a személyes adatokat tartalmazó szerverek közvetlen hálózati úton ne legyenek elérhetőek, és a rendszer feltörése hálózati hozzáféréssel ne legyen lehetséges;
 - d) gondoskodik arról, hogy áramkimaradás esetén a szervergépek szabályosan, adatvesztés nélkül leállíthatók legyenek;
 - e) gondoskodik a szervergépek vírusvédelméről;
 - f) amennyiben az adatbázisszerver elérése terminálszervereken keresztül történik, úgy gondoskodik a terminálszerverekre történő belépéshez szükséges azonosítók és jelszavak kiosztásáról és visszavonásáról, az adatkezelés céljának minimálisan megfelelő jogosultságok beállításáról;
 - g) a szerver és az informatikai rendszer rendszergazdai jelszavát tűzbiztos fémkazettában elzárva kell őrizni. A jelszavak változtatását legalább fél éves gyakorisággal el kell végezni.

Bér- és munkaügyi nyilvántartás

17. §

- (1) A bér és munkaügyi nyilvántartás a munkaviszony és az egyéb munkavégzésre irányuló jogviszonyra vonatkozó tények dokumentálására szolgáló adatkezelés, melynek jogszabályi alapját az Nftv., Mt., valamint az Egyetem Szervezeti és Működési Szabályzata és Kollektív Szerződése képezik.
- (2) A bér- és munkaügyi nyilvántartás adatai, a munkavállaló munkaviszonyával és az egyéb munkavégzésre irányuló jogviszony keretében foglalkoztatott alkalmazott jogviszonyával kapcsolatos tények megállapítására, a besorolási követelmények igazolására, bérszámfejtésre, társadalombiztosítási ügyintézésre és statisztikai adatszolgáltatásra használhatók fel.
- (3) A bér- és munkaügyi nyilvántartás kezelője a Humán Gazdálkodási Igazgatóság.
- (4) A nyilvántartás kezelése számítógépen történik. Az adatok biztonságáról az adatkezelő gondoskodik.
- (5) Az Egyetem szervezetén belül a bér- és munkaügyi nyilvántartásból adatszolgáltatás csak a rektor, a kancellár, valamint azon szervezeti egységek vezetői, illetve személyzeti kérdésekben illetékes ügyintézői részére teljesíthető, amelyeknél az alkalmazott a munkát végzi, valamint azon szervezeti egység ügyintézői részére, amelyeknek a feladat ellátásához a személyes adatok meghatározott körére szükség van.

Az Egyetem által fenntartott Köznevelési intézményekben nyilvántartott és kezelt személyes és különleges adatok

18.§

- (1) Az Egyetem által fenntartott köznevelési intézmények a nemzeti köznevelésről szóló 2011. évi CXCV. törvény 41.§-a szerint kötelesek a jogszabályban előírt nyilvántartásokat vezetni, a köznevelés információs rendszerébe bejelentkezni, valamint az Országos statisztikai adatgyűjtési program keretében előírt, valamint a lemorzsolódással veszélyeztetett tanulókról összesített adatokat szolgáltatni.

Az Egyetem által fenntartott gyermekjóléti intézményben nyilvántartott és kezelt személyes és különleges adatok

19.§

- (1) A gyámhatóságok, a területi gyermekvédelmi szakszolgálatok, a gyermekjóléti szolgálatok és a személyes gondoskodást nyújtó szervek és személyek által kezelt személyes adatokról 235/1997. (XII. 17.) Korm. rendelet 1.§-a szerint a gyámhatóságok, a személyes gondoskodást nyújtó gyermekjóléti alapellátást biztosító szervek és személyek, a területi gyermekvédelmi szakszolgálatok vezetői a Kormányrendelet 1. számú mellékletben meghatározott nyilvántartásokat vezetik. Az adatkezelés tekintetében a Gytv. további részletszabályokat tartalmaz.

IV. FEJEZET

ÉRINTETTI JOGGYAKORLÁS

A feladatok megoszlása az érintetti joggyakorlás során

20. §

- (1) Amennyiben az Egyetem egy szervezeti egységéhez érkezik az érintett valamely jogának gyakorlására irányuló adatkezelési, adatvédelmi jogával kapcsolatos kérelem, akkor a kérelemről, illetve az érintettnek küldendő válaszlevélről az adott szervezeti egység vezetőjének tájékoztatni kell az Adatvédelmi tisztviselőt.
- (2) Az Adatvédelmi tisztviselőhöz érkező kérelem esetén a kérelem megválaszolása érdekében a tisztviselő felveszi a kapcsolatot az érintett szervezeti egység vezetőjével és közreműködik a kérelem megválaszolásában.

Hozzáféréshez való jog

21. §

- (1) Amennyiben az érintett hozzáféréshez való jogát gyakorolja (vagy tájékoztatást kér a személyes adatait érintő adatkezelésekről), akkor az Egyetemnek tájékoztatást kell nyújtania:
- a) pontosan mely személyes adatait is kezeli az érintettnek; ebben az esetben nem elegendő az adatok kategóriájának megnevezése, a konkrét személyes adatot kell megjelölni;
 - b) milyen adatkezelések vannak az érintett vonatkozásában, és az adatkezeléseknek mi a célja és a jogalapja;
 - c) az adatkezelés időtartama, illetve ezen időtartam meghatározásának szempontjai;
 - d) kiknek továbbítja a személyes adatokat az Egyetem;
 - e) az érintettet az adatkezeléssel összefüggésben megillető jogokról;

- f) amennyiben nem az érintettől vették fel a személyes adatokat, akkor azok forrásáról;
- g) a NAIH-nak címzett panasz benyújtásának jogáról.

Másolat kéréséhez való jog

22. §

- (1) Amennyiben az érintett kérése kifejezetten arra irányul, hogy másolatot kapjon a személyes adatairól vagy a személyes adatait tartalmazó dokumentumról, akkor az Egyetemnek az érintett rendelkezésére kell bocsátania a személyes adatok másolatát.
- (2) Az érintett által kért további másolatokért az adatkezelő az adminisztratív költségeken alapuló, észszerű mértékű díjat számíthat fel. Ha az érintett elektronikus úton nyújtotta be a kérelmet, az információkat széles körben használt elektronikus formátumban kell rendelkezésre bocsátani, kivéve, ha az érintett másként kéri.
- (3) Ha az érintett törvényben rögzített határidőn belül a kamera felvételének másolatát kéri, akkor az érintettnek fel kell ajánlani a felvételekbe való betekintés lehetőségét. Ennek érdekében az érintettel telefonhívás vagy elektronikus levelezés útján időpontot kell egyeztetni. Amennyiben az érintett él a betekintés lehetőségével, akkor erről jegyzőkönyvet kell készíteni.
- (4) Amennyiben az érintett nem él a betekintés lehetőségével vagy emellett másolatot is kér a felvételtől, akkor az Egyetem kizárólag abban az esetben adhatja ki, ha az érintett megjelöli, hogy mely napon, mely órában és becslése szerint mely percben készült a felvétel, és
 - a) a felvételen kizárólag az érintett látható, vagy
 - b) ha a felvételen más érintettek képmása is szerepel, akkor a felvételt az Egyetem által megbízott adatfeldolgozó anonimizálja (a felvételen szereplő más érintettek képmását technikai úton felismerhetetlenné teszi).
- (5) Az (4) bekezdés b) alpontjának esetében az Egyetem az anonimizálás végrehajtásáért adminisztratív díjon alapuló költséget számít fel. Erről az összegről az érintettet tájékoztatni kell. Az érintett kérelmét abban az esetben lehet teljesíteni, ha ezt az összeget az érintett megfizette.
- (6) Az (5) bekezdés b) alpontja esetében az érintett kérelme az Egyetemhez történő beérkezésnek időpontjától kezdődően az Egyetem a felvételt elektronikus adathordozóra történő kimentés útján zárolja. A zárolás addig tart, amíg a felvétel (5) bekezdés szerinti anonimizálása megtörténik, vagy az érintett úgy nyilatkozik, hogy az anonimizálás költségét nem fizeti meg. Amennyiben az érintett a 90 napon belül nem nyilatkozik arról, hogy az anonimizálás költségeit megfizeti-e, akkor az Egyetem a zárolt felvételeket törli.

Helyesbítéshez való jog

23. §

- (1) Az érintett kérheti, hogy az Egyetem a rá vonatkozó pontatlan személyes adatokat helyesbítse.
- (2) Az érintett kérelme akkor teljesíthető, ha abban megjelölte, hogy mely személyes adat módosítását kéri és mi a helyes személyes adata.

Törléshez való jog

24. §

- (1) Az Egyetemnek a személyes adatokat törölnie kell, ha
 - a) megszűnt az adatkezelés célja,
 - b) az érintett a hozzájárulását visszavonta, és az adatkezelésnek nincs más jogalapja,
 - c) az érintett tiltakozik az adatkezelése ellen, és nincs elsőbbséget élvező jogszerű ok az adatkezelésre,
 - d) a személyes adatok jogellenes kezelését a NAIH vagy bíróság megállapította,
 - e) a személyes adatokat az Egyetemre alkalmazandó uniós vagy magyar jogban előírt jogi kötelezettség teljesítéséhez törölni kell.
- (2) Az érintett törlési kérelmét az Egyetem akkor tagadhatja meg, ha az Egyetem bizonyítani tudja, hogy az adatkezelés szükséges:
 - a) véleménynyilvánítás szabadságához és a tájékozódáshoz való jog gyakorlása céljából,
 - b) a személyes adatok kezelését előíró, az Egyetemre alkalmazandó uniós vagy magyar jog szerinti kötelezettség teljesítése céljából,
 - c) jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez (így például a felvétel feljelentéshez vagy polgári peres eljárás megindításához szükséges).

Elfeledtetéshez való jog

25. §

- (1) Amennyiben az Egyetem a személyes adatokat nyilvánosságra hozta, és a belső adatvédelmi szabályzat értelmében a személyes adatokat törölni kell, akkor az elérhető technológia és a megvalósítás költségeinek figyelembevételével megteszi az ésszerűen 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.

- (2) Az elfeledtetéshez való joggyakorlás teljesítéséhez szükséges az, hogy az érintett jelölje meg, hogy mely személyes adatát is hozta nyilvánosságra. Amennyiben az érintett ezt a kérelmében nem tüntette fel, akkor az Egyetem felveszi az érintettel a kapcsolatot annak érdekében, hogy jelölje meg, hogy az Egyetem mely személyes adatát is hozta nyilvánosságra.
- (3) Amennyiben az Egyetem a saját honlapján hozta nyilvánosságra a személyese adatokat, akkor onnan el kell távolítani.
- (4) Amennyiben az Egyetem által nyilvánosságra hozott személyes adatokat más adatkezelő is nyilvánosságra hozta, akkor ezen adatkezelőket is értesíteni kell arról, hogy a személyes adatot törölnie kell.
- (5) Az Egyetemnek az érintett által megjelölt személyes adatra rá kell keresnie a Google keresőszolgáltatón keresztül, hogy a Google az Egyetem adatkezelésével összefüggésben listázza-e az adott személyes adatot. Amennyiben igen, akkor a Google keresőmotor bejelentő felületén keresztül ("Tartalom eltávolítása a Google-ből") az érintett által megjelölt személyes adat eltávolítását kell kérni.
- (6) A belső adatvédelmi szabályzatban a "Törléshez való jognál" szereplő kivételeket az elfeledtetéshez való jog gyakorlása esetén szintén alkalmazni kell.

Korlátozáshoz való jog

26. §

- (1) Ha az érintett vitatja a személyes adatok pontosságát, akkor ebben az Egyetem arra az időtartamra korlátozza az adatkezelést, amíg az Egyetem ellenőrzi a személyes adatok pontosságát. Ebben az esetben az Egyetem:
 - a) az elektronikus úton tárolt, vitatott pontosságú adat esetében korlátozza az adathoz való hozzáférést,
 - b) a papír alapon tárolt irat esetében a többi irattól elkülönítetten, zárt borítékban tárolja a vitatott pontosságú adatot tartalmazó iratot.Ha az érintett kérelme megalapozott, akkor az Egyetem a személyes adatot helyesbíti.
- (2) Ha az adatkezelés jogellenes, és az érintett ellenzi az adatok törlését, akkor kérheti a személyes adatok felhasználásának korlátozását. Ebben az esetben az Egyetem:
 - a) az elektronikus úton tárolt személyes adat esetében az adatot külső adathordozóra (így például pendrive vagy cd-lemez) kimentti, és törli az elektronikus úton tárolt adatot az informatikai rendszerből,
 - b) a papír alapon tárolt irat a többi irattól elkülönítetten, zárt borítékban tárolja az érintett által megjelölt személyes adatot tartalmazó iratot, majd azt az

érintettnek átadja úgy, hogy az Egyetemenél az iratról nem marad másolat vagy másodpéldány.

Az érintettnek a kérelemben meg kell jelölnie, hogy meddig kéri a felhasználás korlátozását. Amennyiben az érintett nem jelölte meg, akkor elektronikus levelében - ha nem áll rendelkezésre e-mail cím, akkor postai úton - fel kell őt hívni arra, hogy jelölje meg, milyen időtartamra kéri a felhasználás korlátozását.

- (3) Az érintett jogosult arra, hogy kérje az adatkezelés korlátozását, ha az Egyetemnek már nincs szüksége a személyes adatokra, de az érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez. Ebben az esetben az Egyetemnek:

- a) az elektronikus úton tárolt személyes adat esetében az adatot külső adathordozóra (így például pendrive vagy cd-lemez) kimentti, és törli az elektronikus úton tárolt adatot az informatikai rendszerből,
- b) a papír alapon tárolt irat a többi irattól elkülönítetten, zárt borítékban tárolja az érintett által megjelölt személyes adatot tartalmazó iratot, majd azt az érintettnek átadja úgy, hogy az Egyetemenél az iratról nem marad másolat vagy másodpéldány.

Az érintettnek a kérelemben meg kell jelölnie, hogy meddig kéri a felhasználás korlátozását. Amennyiben az érintett nem jelölte meg, akkor elektronikus levelezés útján - ha nem áll rendelkezésre e-mail cím, akkor postai úton - fel kell hívni arra, hogy jelölje meg, milyen időtartamra kéri a felhasználás korlátozását.

- (4) Az érintett jogosult arra, hogy a kérje az adatkezelés korlátozását, amennyiben a tiltakozás jogát gyakorolja. Ebben az esetben az Egyetem arra az időtartamra korlátozza az adatkezelést, amíg a tiltakozási kérelmének jogszerűségét megvizsgálja. Az Egyetem:

- a) az elektronikus úton tárolt személyes adat esetében korlátozza az adathoz való hozzáférést,
- b) a papír alapon tárolt irat esetében a többi irattól elkülönítetten, zárt borítékban tárolja a vitatott pontosságú adatot tartalmazó iratot.

Ha az érintett kérelme megalapozott, akkor az Egyetem törli a személyes adatot.

Adathordozhatósághoz való jog

27. §

- (1) Ha az adatkezelés jogalapja az érintett hozzájárulása vagy a szerződéses jogalap, és az adatkezelés automatizált módon történik, akkor az érintett jogosult arra, hogy
- a) a rá vonatkozó, általa az Egyetem rendelkezésére bocsátott személyes adatokat széles körben használt, géppel olvasható formátumban megkapja, vagy
 - b) ezeket az adatokat egy másik Adatkezelőnek továbbítsa anélkül, hogy ezt az Egyetem akadályozná.

- (2) Amennyiben az Egyetem és az érintett által megjelölt másik adatkezelő között technikailag megvalósítható, akkor az érintett jogosult arra, hogy kérje a személyes adatok adatkezelők közötti közvetlen továbbítását.
- (3) Az Egyetem a (1) bekezdés a) alpont szerinti esetben a személyes adatokat külső adathordozóra (például pendrive vagy cd-lemez) kimentti. A külső adathordozót az érintett is biztosíthatja.

Tiltakozás joga

28. §

- (1) Az érintett jogosult arra, hogy bármikor tiltakozzon személyes adatainak érdek mérlegelés jogalapjának [GDPR 6. cikk (1) bekezdés f) pont] alkalmazásával történő kezelése ellen.
- (2) Tiltakozás esetén meg kell vizsgálni azt, hogy az érintett által megjelölt adatkezelés esetében az érintett által hivatkozott tények, érvek miatt az Egyetemnek van-e lehetősége arra, hogy a személyes adatokat törölje, vagy az adatkezelést az érintett vonatkozásában megszüntesse.
- (3) Az Egyetem akkor kezelheti tovább a személyes adatokat, ha bizonyítja, hogy
 - a) az adatkezelést olyan kényszerítő erejű jogos okok indokolják, amelyek elsőbbséget élveznek az érintett érdekeivel, jogaival és szabadságaival szemben
 - b) az adatkezelés jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódik.

Az érintett azonosítása

29. §

- (1) Ha az Egyetemnek megalapozott kétségei vannak a kérelmet benyújtó természetes személy kilétével kapcsolatban, az érintett személyazonosságának megerősítését kérheti. Ennek során az Egyetem az alábbi lépéseket alkalmazhatja:
 - a) telefonhívás útján az Egyetem számára rendelkezésre álló további személyes adatokra történő rákérdezés, és helyes válaszok esetén a személyazonosság megerősítését el lehet fogadni,
 - b) az Egyetem arra kéri az érintett, hogy teljes bizonyító erejű magánokiratban nyújtsa be a kérelmét,
 - c) az érintett az Egyetem székhelyén bemutatja valamely személyazonosító igazolványát (személyazonosító igazolvány, jogosítvány, útlevel).

- (2) Az érintett a kilétének megerősítésére más módszert ajánl fel, és ha azt az Egyetem vállalja, akkor az is elfogadható a személyazonosság megerősítéseként. Az Egyetem maga is felajánlhat más módszert.

A kérelem teljesítésének határideje

30. §

- (1) Az Egyetem az érintett kérelmét annak beérkezésétől számított 1 hónapon belül teljesíti. A kérelem beérkezésének napja a határidőbe nem számít bele.
- (2) Szükség esetén, figyelembe véve a kérelem bonyolultságát és a kérelmek számát, ez a határidő további 2 hónappal meghosszabbítható. A határidő meghosszabbításáról az Egyetem a késedelem okainak megjelölésével a kérelem kézhezvételétől számított 1 hónapon belül tájékoztatja az érintettet.

Az érintetti kérelem teljesítése

31. §

- (1) Az Egyetem kizárólag az érintett elektronikus úton vagy papír alapon küldött kérelmét teljesíti. *(5. számú melléklet)* Telefonhívás útján előterjesztett kérelem nem teljesíthető. Erről az Egyetem az érintettet telefonhívás során tájékoztatni köteles. Ha az érintett az Egyetem székhelyén szóban terjeszti elő a kérelmét, akkor azt írásba kell foglalni.
- (2) Az Egyetemnek olyan módon kell teljesíteni az érintett kérelmét, amilyen formátumban az érintett kéri.
- (3) Ha az érintett elektronikus úton nyújtotta be a kérelmet, és a másolatot is elektronikus formátumban kéri, akkor az Egyetemnek a másolatot széles körben használt elektronikus formátumban kell rendelkezésre bocsátani.
- (4) Ha az érintett a kérelmében nem jelölte meg, hogy milyen formátumban kéri a másolatot, akkor az Egyetemnek fel kell vennie az érintettel a kapcsolatot, és tisztázni kell, hogy milyen formátumban szeretné a másolatot megkapni. A kapcsolatfelvételnek elsődlegesen telefonhívás vagy elektronikus levelezés útján kell megtörténnie, ha erre nincs lehetőség, akkor az érintettet postai úton kell értesíteni.
- (5) Az Egyetemnek az érintett kérelmében megjelölt érintetti jogot kell teljesíteni. Amennyiben az érintetti kérelem nem pontos, és a kérelem alapján nem lehet eldönteni, hogy milyen jogot is akar az érintett gyakorolni, akkor ennek tisztázása érdekében fel kell vennie a kapcsolatot vele.

- (6) Ha az érintett a kérelmében több jogot is gyakorolni kíván, akkor azok mindegyikét teljesíteni kell (például hozzáféréshez való jog és törléshez való jog egyidejű gyakorlása esetén egyrészt tájékoztatni kell az érintettet arról, hogy milyen személyes adatait kezeli az Egyetem, másrészt pedig végre kell hajtani a személyes adatok törlését - ha nem áll fenn valamely kivétel - és erről az érintettet tájékoztatni kell).
- (7) Az érintett kérelmének teljesítését díjmentesen kell biztosítani.

Az érintetti kérelem megtagadása

32. §

- (1) Az érintetti kérelem kizárólag akkor tagadható meg, ha uniós vagy tagállami jogszabály a GDPR 23. cikk (1) bekezdésében felsorolt érdekek védelme miatt korlátozza vagy kizárja az érintetti joggyakorlás teljesítését.
- (2) Ha az érintett kérelme egyértelműen megalapozatlan vagy - különösen ismétlődő jellege miatt - túlzó, az Egyetem megtagadhatja a kérelem alapján történő intézkedést.
- (3) Az érintett kérelmének megtagadásáért nem lehet díjat felszámítani.
- (4) Ha az Egyetem nem teljesíti az érintett kérelmét, akkor 1 hónapon belül tájékoztatja az érintettet:
 - a) az intézkedés elmaradásának ténybeli és jogi okairól (mely jogszabály vagy a GDPR mely rendelkezése az, amely alapján jogszerűen tagadhatja meg a kérelem teljesítést),
 - b) valamint arról, hogy az érintett panaszt nyújthat be valamely felügyeleti hatóságnál, és élhet bírósági jogorvoslati jogával.

V. FEJEZET

ALAPVETŐ ADATBIZTONSÁGI INTÉZKEDÉSEK

Informatikai biztonsági intézkedések

33. §

- (1) Az Egyetem valamennyi adatkezelés során köteles olyan informatikai biztonsági intézkedéseket hozni, amelyek a személyes adatokat tartalmazó informatikai rendszerek esetében
- a) megakadályozzák, hogy jogosulatlan személyek hozzáférést szerezzenek vagy belépjenek ezen rendszerekbe,
 - b) szabályozza a megfelelő hozzáférési jogosultságok beállítását, illetve felhasználó nevet és a jelszót rendelnek hozzá az egyes jogosultságokhoz, valamint a szabályozza a jelszóhasználati előírásokat (például a jelszó minimum hossza, használható karakterek, érvényesség időtartam, téves jelszóhasználatok száma a fiók zárolása előtt),
 - c) biztosítják, hogy a jogosultsággal rendelkező személyek a személyes adatokhoz csak a hozzáférési engedélyük keretein belül férhessenek hozzá,
 - d) naplózás útján biztosítják annak ellenőrizhetőségét és megállapíthatóságát, hogy mely felhasználó lépett be és milyen szoftverbe,
 - e) lehetővé teszik annak ellenőrizhetőségét és megállapíthatóságát, hogy mely személyes adatokat mikor és ki vitte be, módosította vagy továbbította,
 - f) biztosítják azt, hogy a személyes adatok engedély nélkül nem olvashatók, másolhatóak, módosíthatók vagy távolíthatók el,
 - g) garantálják a hálózatbiztonságot (például tűzfal, behatolásérzékelő, illetve más, a hálózatbiztonságról gondoskodó aktív vagy passzív rendszer),
 - h) biztosítják a megfelelő vírusvédelmet, illetve a más rosszindulatú software-ek elleni védelmet,
 - i) biztosítják a munkaállomások védelmét (például automatikus zárás, rendszeres frissítés),
 - j) biztosítják a rendszerek folyamatos rendelkezésre állását,
 - k) fizikai vagy műszaki incidens esetén biztosítják az arra való képességet, hogy a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását kellő időben vissza lehet állítani, az ilyen incidensekről jelentés készül, illetve az ilyen incidensek nem hatnak ki az adat integritására,
 - l) - amennyiben az adott adatkezelés végrehajtásához indokolt - garantálják a személyes adatok titkosítását vagy álnevesítését,
 - m) - amennyiben az adott adatkezelés végrehajtásához indokolt és lehetséges - garantálják, hogy a személyes adatokat (vagy az egyes adatbázist) elkülönítve tárolják, amellyel egy adatvédelmi incidens esetén

csökkenthető annak az esélye, hogy a személyes adatok egymással összefüggésbe hozhatók,

n) biztosítják, hogy adatfeldolgozó igénybevétele esetén megfelelő garanciák vonatkoznak az általuk végzett tevékenységre (például a személyes adatokat titkosítva adják át a számukra, jogosultságkezelés és hitelesítés).

- (2) Az Informatikai Szolgáltató Központ igazgatójának a belső adatvédelmi szabályzat **6. számú melléklete** szerinti nyilvántartás kitöltésével dokumentálnia kell azt, hogy az Egyetem informatikai rendszerei teljesítik az (1) bekezdés szerinti követelményeket.
- (3) A jogosultság beállítása iránti igényt az adatkezelést végző szervezeti egység vezetője nyújtja be az Informatikai Szolgáltató Központ vezetőjének.
- (4) Az alkalmazottak kizárólag az Egyetem által biztosított informatikai eszközt használhatják az Egyetem kezelésében levő üzleti titkok (ideértve a védett ismereteket is), banktitkok és személyes adatok tárolására. Az alkalmazottak ezen adatokat nem tárolhatják a saját vagy más tulajdonában álló informatikai eszközökön.
- (5) Az alkalmazottak nem használhatják magáncélra az Egyetem által az alkalmazott számára létrehozott e-mail címet (a továbbiakban: egyetemi e-mail cím), illetve nem tárolhatnak semmilyen személyes adatot az egyetemi e-mail címet kiszolgáló fiókban, Magáncélú használatnak minősül különösen bármilyen, nem az alkalmazott munkaköréhez, munkavégzéséhez kapcsolódó vagy nem az Egyetem érdekében történő e-mail küldés vagy fogadás. Az ilyen tartalmú leveleket az alkalmazottnak haladéktalanul törölnie kell.
- (6) Az informatikai rendszerek üzemeltetését ellátó munkatársak a feladataik ellátásához szükséges mértékig a személyes adatokhoz hozzáférhetnek, az adatokat azonban más célra nem használhatják fel, és mások tudomására nem hozhatják.

Szervezési biztonsági intézkedések

34. §

- (1) Az Egyetem valamennyi adatkezelés során köteles olyan szervezési biztonsági intézkedéseket hozni, amelyek biztosítják, hogy
 - a) bizonyos helyiségekbe csak meghatározott, arra feljogosított személyek léphetnek be,
 - b) az adatokat jól zárható, száraz, tűzvédelmi és vagyonvédelmi berendezéssel ellátott helyiségben helyezi el,
 - c) a személyes adatokat tároló, zárható iratszekrényhez csak meghatározott személynek lehessen hozzáférése,

- d) a személyes adatokat tartalmazó dokumentumokhoz való hozzáférés csak olyan személyek részére megengedett, akiknek a munkavégzéséhez nélkülözhetetlen ezen dokumentumokhoz való hozzáférés biztosítása,
 - e) a folyamatos aktív kezelésben lévő iratokhoz csak az illetékesek férhetnek hozzá,
 - f) az alkalmazott a nap folyamán, illetve a nap végén csak úgy hagyhatja el az olyan helyiséget, ahol a személyes adatot tartalmazó dokumentumokat tárolják vagy az e dokumentumokkal munkát végez, hogy a dokumentumot elzárja, vagy az irodát bezárja.
- (2) Az Egyetem valamennyi alkalmazottja köteles az Egyetemmel fennálló jogviszonya alatt tudomására jutott üzleti titkok (védett ismeretek), banktitok, illetve az Egyetem által kezelt személyes adatok bizalmosságát megőrizni. Ez a kötelezettség a jogviszony megszűnését követően is fennmarad.

VI. FEJEZET

ADATVÉDELMI INCIDENSEK KEZELÉSE ÉS BEJELENTÉSE

Adatvédelmi incidensek esetei

35. §

- (1) Az Egyetem esetében adatvédelmi incidens különösen:
- a) a személyes adatokat tároló, kezelő informatikai rendszer vagy szoftverhez történő jogosulatlan hozzáférés,
 - b) a személyes adatok jogosulatlan titkosítása, amelynek következtében a személyes adatokhoz - akár átmenetileg - nem lehet hozzáférni vagy az adatkezelések során felhasználni,
 - c) ha az Egyetem alkalmazottja jogosulatlanul hozzáfér személyes adatokhoz, a jogosultsági szintjét meghaladóan fér hozzá a személyes adatokhoz, vagy az alkalmazott által jogosulatlanul végrehajtott adatkezelési művelet (például a személyes adatokat tartalmazó adatbázis kimentése külső adathordozóra),
 - d) személyes adatok véletlen vagy szándékos, felhatalmazás nélküli nyilvánosságra hozatala,
 - e) személyes adatokat tartalmazó dokumentum más számára történő hozzáférhetővé tétele,
 - f) személyes adatokat tartalmazó postai küldemény téves címzethez történő elpostázása,
 - g) személyes adatokat tartalmazó e-mail téves címzettnek történő kiküldése,
 - h) személyes adatokat tartalmazó adathordozó vagy informatikai eszköz elvesztése,

- i) a személyes adatokat tároló informatikai eszköz vagy az ilyen adatokat tartalmazó dokumentumok sérülése, megsemmisülése (ideértve a tüzesetet vagy a vízkár által okozott sérülést vagy megsemmisülést), amelynek következtében a személyes adatokhoz - akár átmenetileg - nem lehet hozzáférni vagy az Egyetem adatkezelései során felhasználni.

Tudomásszerzés az adatvédelmi incidensről

36. §

- (1) Tudomásszerzésnek minősül az, ha
- a) az adatvédelmi incidens bekövetkezésére utaló körülményt az Egyetem alkalmazottja fedezi fel,
 - b) az Egyetemnek e-mailen, postai levélben vagy más kommunikációs eszköz útján küldött üzenet, levél adatvédelmi incidens bekövetkezésére utaló körülményt tartalmaz (abban az esetben is, ha az üzenet vagy a levél névtelen),
 - c) a sajtóban vagy más honlapon, adatvédelmi incidens bekövetkezésére utaló körülmény jelent meg, amelyről az Egyetem értesül, vagy arról értesítik,
 - d) az Egyetem által megbízott adatfeldolgozó e-mailben jelzi, hogy az Egyetem által kezelt személyes adatokkal összefüggésben adatvédelmi incidens következett be.
- (2) Az Egyetem alkalmazottai az adatvédelmi incidens bejelentését a **www.adatvedelem.unideb.hu** oldalon történő bejelentkezés után az incidens bejelentés menüpont alatt, vagy az Adatvédelmi tisztviselőnek az adatvedelmi.tisztviselo@unideb.hu e-mail címre megküldve is megtehetik.
- (2a) Az Egyetem alkalmazottai az egészségügyi adatokat érintő adatvédelmi incidens bejelentését a www.adatvedelem.unideb.hu oldalon történő bejelentkezés után az incidens bejelentés menüpont alatt, vagy az Egészségügyi Adatvédelmi Tisztviselőnek az egeszsegugyi.tisztviselo@unideb.hu e-mail címre megküldve is megtehetik
- (3) Az Egyetem alkalmazottja soron kívül köteles értesíteni a hivatali út betartásával a közvetlen munkahelyi felettesét, a területi adatvédelmi felelőst és az Adatvédelmi tisztviselőt. Az egyes szervezeti egységek az Adatvédelmi tisztviselőnek történő bejelentést megelőző szakaszra vonatkozóan külön belső szabályokat állapíthatnak meg magukra.
- (4) Amennyiben az Egyetem alkalmazottja úgy ítéli meg, hogy közvetlen felettese az adott ügyben érintett, akkor a vezető felettesét kell értesítenie.

Adatkezelés felfüggesztése adatvédelmi incidens esetén

37. §

- (1) Adatvédelmi incidensre vonatkozó értesítést követően haladéktalanul fel kell függeszteni azt az adatkezelést, amit az adatvédelmi incidens érintett.
- (2) A felfüggesztés különösen az alábbi esetekben szüntethető meg, ha
 - a) a rendelkezésre álló információk alapján az adatvédelmi incidensnek nincsenek és nem is várhatóak súlyos következményei, vagy
 - b) a felfüggesztést követően az Egyetem olyan intézkedéseket hozott, amelyek biztosítják, hogy az adatvédelmi incidensnek nincsenek és nem is várhatóak súlyos következményei.
- (3) A felfüggesztés megszüntetéséről az Adatvédelmi tisztviselő javaslata alapján a Kancellár dönt. A javaslatban ki kell térni arra, hogy
 - a) milyen adatvédelmi incidens történt (a személyes adatok típusa, mennyisége, érintettek száma, kategóriái, milyen következményei voltak vagy lehettek volna az érintettre),
 - b) miért javasolja a felfüggesztés megszüntetését.

Az adatvédelmi incidens bejelentése és kivizsgálása

38. §

- (1) Az adatvédelmi incidenst az Egyetemnek- az Adatvédelmi tisztviselőn keresztül - a tudomásszerzést követő 72 órán belül be kell jelentenie a NAIH honlapján, függetlenül attól, hogy mennyi információ áll az Egyetem rendelkezésére az adatvédelmi incidenssel összefüggésben. Ha az Egyetem a bejelentési kötelezettséget akadályoztatása miatt határidőben nem teljesíti, azt az akadály megszűnését követően haladéktalanul teljesíti, és a bejelentéshez mellékeli a késedelem okait feltáró nyilatkozatát is.
- (2) Az adatkezelés felfüggesztését követően haladéktalanul meg kell kezdeni az adatvédelmi incidens kivizsgálását. A kivizsgálás során az alábbi körülményeket kell tisztázni:
 - a) az adatvédelmi incidens típusa (bizalmassági, integritási vagy elérhetőségi),
 - b) az adatvédelmi incidens bekövetkezése előtt alkalmazott intézkedések,
 - c) az adatvédelmi incidens oka (valószínűsíthető oka),
 - d) az adatvédelmi incidenssel érintett személyes adatok típusa és mennyisége (legalább becsléssel),
 - e) az érintettek száma (legalább becsléssel),
 - f) az érintettek kategóriái, így különösen, hogy az adatvédelmi incidensben van-e sérülékeny érintetti kör (például gyerekek, idős emberek, vagy más ország állampolgárai),
 - g) mennyire egyszerű az érintettek azonosítása azon adatkör alapján, amelyet az adatvédelmi incidens érintett,
 - h) az adatvédelmi incidens lehetséges vagy már megtörtént következményei, illetve azok súlyossága az érintettekre nézve,

- i) szükséges-e az érintetteket tájékoztatni az adatvédelmi incidensről, és amennyiben nem, akkor ennek indoka,
 - j) milyen intézkedéssel lehet az adatvédelmi incidens következményeit mérsékelni vagy azokat megszüntetni.
- (3) Az adatvédelmi incidens kivizsgálását a Debreceni Egyetem Információbiztonsági Havarria team (a továbbiakban: Havarria team) végzi. (**7. számú melléklet**)
A Havarria team állandó tagja az Adatvédelmi tisztviselő és az Informatikai Biztonsági Központ vezetője és az Informatikai Szolgáltatási Központ igazgatója. Az állandó tagok mellett a Havarria team tagja lehet:
- a) az adatvédelmi incidenssel érintett szervezeti egység vezetője,
 - b) az adatvédelmi incidenssel érintett szervezeti egység területi adatvédelmi felelősét,
 - c) az adatvédelmi incidens bejelentője,
 - d) amennyiben az Egyetem által megbízott adatfeldolgozó tevékenysége során merült fel az adatvédelmi incidens, az adatfeldolgozó képviselője.
- (3a) Amennyiben a vizsgálat eredményeként a Havarria Team úgy ítéli meg, hogy az incidens informatikai jellegű, a további vizsgálatot az Informatikai Biztonsági Központ és az Informatikai Szolgáltató Központ végzi, és megteszi a szükséges intézkedéseket, melynek eredményéről az Adatvédelmi Központot tájékoztatja.
- (4) Amennyiben az adatvédelmi incidens kivizsgálás függetlensége vagy hatékonysága az Egyetem szervezetén belül nem biztosítható, akkor az adatvédelmi incidens kivizsgálásával külső szakértőt kell megbízni.
- (5) Az adatvédelmi incidens kivizsgálása során feltárt új körülményeket az Adatvédelmi tisztviselőnek haladéktalanul be kell jelentenie a NAIH-nak.

Az adatvédelmi incidens bejelentésének mellőzése

39. §

- (1) Abban az esetben, ha bizonyítottan adatvédelmi incidens történt, azonban arról történő tudomásszerzés időpontjában megállapítható, hogy az incidensnek valószínűsíthetően nincs kockázata az érintetteknek nézve, akkor az incidensről nem kell bejelentést tenni a NAIH-nak.
- (2) Ilyen adatvédelmi incidensnek tekinthető különösen az, ha a személyes adatokat tartalmazó, az érintett téves lakcímére küldött postai küldemény felbontás nélkül visszaérkezik az Egyetemhez.
- (3) Az adatvédelmi incidens bejelentésének mellőzéséről az Adatvédelmi tisztviselő javaslata alapján a Kancellár dönt. A javaslatban ki kell térni arra, hogy

- a) milyen adatvédelmi incidens történt (a személyes adatok típusa, mennyisége, érintettek száma, kategóriái, milyen következményei voltak vagy lehettek volna az érintettre),
 - b) miért nem következett be az érintettekre nézve kockázatot jelentő adatvédelmi incidens,
 - c) - amennyiben az adott adatvédelmi incidens kapcsán értelmezhető - hogyan lehet megelőzni azt, hogy a jövőben ne következzen be hasonló adatvédelmi incidens,
 - d) miért javasolja azt, hogy erről az Egyetem ne tegyen bejelentést a NAIH-nak.
- (4) Amennyiben a Kancellár a javaslatot elfogadja, akkor az adatvédelmi incidenst fel kell vezetni az incidens-nyilvántartásba. Az adatvédelmi incidens-nyilvántartást az Adatvédelmi tisztviselő vezeti. **(8. számú melléklet)**

Érintettek tájékoztatása

40. §

- (1) Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár az érintettek nézve, az Egyetemnek indokolatlan késedelem nélkül tájékoztatnia kell az érintettet az adatvédelmi incidensről.
- (2) Az adatvédelmi incidens magas kockázattal jár, és az érintetteket tájékoztatni kell, ha az incidens az alábbi adatkategóriák egyikére vonatkozik:
- a) a különleges adatok,
 - b) az érintett pénzügyi helyzetére vonatkozó adatok (például tartozás),
 - c) az érintett társadalmi megbecsülésére kiható adatok (például rossz iskolai eredmények),
 - d) felhasználónév, jelszó,
 - e) a személyiséglopásra alkalmas adatok.
- (3) Az érintetteknek adott tájékoztatóban ismertetni kell
- a) az adatvédelmi incidens jellegét,
 - b) a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit,
 - c) ismertetni kell az adatvédelmi incidens lehetséges vagy már megtörtént következményeit, illetve azok súlyosságát az érintettek nézve,
 - d) az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.
- (4) Az előzetes tájékoztatást az érintettek e-mail címére kell elküldeni. Ha nem áll rendelkezésre az érintettek e-mail címe, akkor a postai elérhetőségekre kell továbbítani a tájékoztatást. Amennyiben van olyan érintett, akit nem lehet az

adatvédelmi incidensről tájékoztatni, vagy az érintettek tájékoztatása aránytalan erőfeszítést tenne szükségessé, akkor a honlapon közlemény helyezhető el.

- (5) A (3) bekezdésében szereplő tájékoztató szövegére és a tájékoztatás (4) bekezdés szerinti formájára, illetve tartalmára az Adatvédelmi tisztviselő tesz javaslatot, és arról a Kancellár dönt.
- (6) Az előzetes tájékoztatás mellőzhető, ha
 - a) az Egyetem megfelelő adatbiztonsági intézkedéseket hajtott végre, és ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében alkalmazták, így különösen olyan intézkedések jöhetnek szóba, amelyek a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik az adatokat (például titkosítás alkalmazása),
 - b) az Egyetem az adatvédelmi incidenst követően olyan további intézkedéseket tett, amelyek biztosítják, hogy az adatvédelmi incidens valószínűsíthetően nem jár magas kockázattal az érintettekre nézve.
- (7) Az érintettek előzetes tájékoztatásának mellőzéséről az Adatvédelmi tisztviselő javaslata alapján a Kancellár dönt. A javaslatban ki kell térni arra, hogy
 - a) milyen adatvédelmi incidens történt (a személyes adatok típusa, mennyisége, érintettek száma, kategóriái, milyen következményei voltak vagy lehettek volna az érintettre),
 - b) miért lenne szükséges az érintettek tájékoztatása,
 - c) miért javasolja azt, hogy az Egyetem ne tájékoztassa az érintetteket az adatvédelmi incidensről.

Jegyzőkönyv a kivizsgálásról és az incidens-nyilvántartás

41. §

- (1) Az adatvédelmi incidens kivizsgálását írásban, jegyzőkönyvben kell rögzíteni, amelyben javaslatot kell tenni az adatvédelmi incidens orvoslására és az okainak megszüntetésére. A szükséges intézkedések meghozataláról és bevezetéséről a Kancellár dönt.
- (2) Az Egyetemenél történt valamennyi adatvédelmi incidensről a belső adatvédelmi szabályzat szerinti nyilvántartást kell vezetni, függetlenül attól, hogy a NAIH-nak kellett-e bejelentést tenni vagy sem.
- (3) Az incidens-nyilvántartást adatvédelmi incidensenként külön-külön kell vezetni, úgy, hogy annak alapján a NAIH ellenőrizhesse az irányadó jognak való megfelelést. Az adatvédelmi incidens nyilvántartást az Adatvédelmi Központ vezeti.

VII. FEJEZET

ADATVÉDELMI TISZTVISELŐ ÉS AZ ADATVÉDELMI KÖZPONT

Adatvédelmi tisztviselőre vonatkozó rendelkezések

42. §

- (1) Az Egyetem a személyes adatok kezelésére vonatkozó jogi előírások teljesítésének és az érintettek jogai érvényesülésének elősegítése érdekében adatvédelmi tisztviselőt alkalmaz.
- (2) Az Adatvédelmi tisztviselő feladatai:
 - a) tájékoztat és szakmai tanácsot ad az Egyetem, továbbá az adatkezelést végző alkalmazottak részére az irányadó jog szerinti kötelezettségeikkel kapcsolatban,
 - b) elősegíti az érintettet megillető jogok gyakorlását, így különösen kivizsgálja az érintettek panaszait és kezdeményezi a panasz orvoslásához szükséges intézkedések megtételét,
 - c) ellenőrzi az irányadó jognak, továbbá az Egyetem személyes adatok védelmével kapcsolatos belső szabályainak való megfelelést, ideértve a feladatkörök kijelölését, az adatkezelési műveletekben résztvevő személyzet tudatosság-növelését és képzését, valamint a kapcsolódó auditokat is,
 - d) együttműködik a NAIH-hal, az adatkezeléssel összefüggő ügyekben kapcsolattartó pontként szolgál a NAIH felé, valamint adott esetben bármely egyéb kérdésben konzultációt folytat vele,
 - e) ellátja jelen belső adatvédelmi szabályzat alapján rá ruházott feladatokat, közreműködik a belső adatvédelmi szabályzat megalkotásában, módosításában,
 - f) ellátja azokat a feladatokat, amelyekkel a Kancellár megbízza,
 - g) nyilvántartja az Egyetem adattérképét,
 - h) vezeti az alábbi nyilvántartásokat:
 - adatvédelmi tisztviselői nyilvántartás *(9. számú melléklet)*
 - adatvédelmi incidens-nyilvántartás
 - adatvédelmi tisztviselői bejelentések nyilvántartás
 - oktatási tevékenységek nyilvántartása
 - i) az adatvédelmi tudatosság erősítése érdekében az egyetemen oktatásokat tart. *(10. számú melléklet)*
- (3) Az Adatvédelmi tisztviselőnek joga van ellenőrizni a GDPR, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezéseknek, továbbá az adatkezelő személyes adatok védelmével kapcsolatos belső szabályainak való megfelelést. Jogosult betekinteni az adatkezelésekbe. Az adatkezelést végző egységek vezetőitől és munkatársaitól szóban vagy írásban felvilágosítást kérhet. Törvénysértés esetén az Adatvédelmi tisztviselő ennek

megszüntetésére köteles felszólítani az adatkezelőt, és a jogsértést a Kancellárnak jelenti. Az Adatvédelmi tisztviselő az ellenőrzések során tett megállapításait az ellenőrzés lezárultát követően haladéktalanul köteles jelenteni az Egyetem Kancellárja felé.

- (4) Az Egyetem köteles:
- a) biztosítani azt, hogy az Adatvédelmi tisztviselő a személyes adatok védelmével kapcsolatos összes ügybe megfelelő módon és időben bekapcsolódjon,
 - b) támogatni az Adatvédelmi tisztviselőt a feladatai ellátásában azáltal, hogy biztosítja számára azokat a forrásokat, amelyek e feladatok végrehajtásához, a személyes adatokhoz és az adatkezelési műveletekhez való hozzáféréshez, valamint a szakértői szintű ismereteinek fenntartásához szükségesek,
 - c) biztosítani azt, hogy az Adatvédelmi tisztviselő a feladatai ellátásával kapcsolatban utasításokat senkitől ne fogadjon el,
 - d) biztosítani azt, hogy ha az Adatvédelmi tisztviselő más feladatokat is ellát, akkor e feladatokból ne fakadjon összeférhetlenség.
- (5) Az Egyetemnek biztosítania kell, hogy az Adatvédelmi tisztviselő közvetlenül a Kancellárnak tartozzon felelősséggel.
- (6) A Kancellár az Adatvédelmi tisztviselőt feladatai ellátásával összefüggésben nem bocsáthatja el és szankcióval nem sújthatja.
- (7) Az Egyetemnek az Adatvédelmi tisztviselő nevét és elérhetőségét be kell jelentenie a NAIH által vezetett nyilvántartásba.
- (8) Az Adatvédelmi tisztviselő elérhetősége: adatvedelmi.tisztviselo@unideb.hu

Az elérhetőség az Egyetem honlapján közzétételre került:

<https://unideb.hu/hu/adatvedelmi-tisztviselo>

- (8a) Egészségügyi adatkezeléssel és adatvédelemmel kapcsolatos kérdésekben az egészségügyi adatvédelmi tisztviselő hivatott eljárni, aki feladatai ellátása során köteles együttműködni az Adatvédelmi tisztviselővel. Továbbá bejelentési köztelezettség terheli egészségügyi adatokat érintő adatvédelmi incidens esetén az Egyetem Adatvédelmi tisztviselője felé.
- (8b) Az egészségügyi adatvédelmi tisztviselő elérhetősége: egeszsegugyi.tisztviselo@unideb.hu. Az elérhetőség az Egyetem honlapján közzétételre került: <https://unideb.hu/hu/adatvedelmi-tisztviselo>
- (9) Az Adatvédelmi tisztviselő jogviszonyának fennállása alatt és annak megszűnését követően is titokként megőrzi a tevékenységével, annak ellátásával kapcsolatban tudomására jutott személyes adatot, minősített adatot, illetve törvény által védett titoknak és hivatás gyakorlásához kötött titoknak minősülő adatot, valamint

minden olyan adatot, tényt vagy körülményt, amelyet az őt alkalmazó adatkezelő vagy adatfeldolgozó nem köteles törvény előírásai szerint a nyilvánosság számára hozzáférhetővé tenni.

- (10) Az Adatvédelmi tisztviselői feladatokhoz kapcsolódó tájékoztató anyagok elérhetőek bejelentkezést követően a Kancellária honlapon Adatvédelem menüpont alatt.

Együttműködés a felügyeleti hatósággal

43. §

- (1) A felügyeleti hatóságtól - így különösen a NAIH-tól - érkező megkereséseket vagy végzéseket haladéktalanul továbbítani kell az Adatvédelmi tisztviselőnek.
- (2) Az Adatvédelmi tisztviselőnek a megkeresésében vagy végzésében szereplő határidő lejárta előtt négy nappal előterjesztést kell készíteni a Kancellárnak. A NAIH megkeresésére vagy végzésére válasz a Kancellár aláírásával küldhető ki.

Adatvédelmi Központ

44. §

- (1) Az Adatvédelmi tisztviselőt a feladatai ellátásában az Adatvédelmi tisztviselő szakmai irányításával működő Adatvédelmi Központ segíti.
- (2) Az Egyetem köteles biztosítani azt, hogy az Adatvédelmi Központ munkatársa a személyes adatok védelmével kapcsolatos összes ügybe megfelelő módon és időben bekapcsolódjon, támogatni az Adatvédelmi Központ munkatársát a feladatai ellátásában azáltal, hogy biztosítja számára azokat az forrásokat, amelyek e feladatok végrehajtásához, a személyes adatokhoz és az adatkezelési műveletekhez való hozzáféréshez, valamint a szakértői szintű ismereteinek fenntartásához szükségesek, biztosítani azt, hogy az Adatvédelmi Központ munkatársa a feladatai ellátásával kapcsolatban - az Adatvédelmi tisztviselőt kivéve - utasításokat senkitől ne fogadjon el, biztosítani azt, hogy ha az Adatvédelmi Központ munkatársa más feladatokat is ellát, akkor e feladatokból ne fakadjon összeférhetlenség. A Kancellár az Adatvédelmi Központ munkatársát az adatvédelemmel összefüggő feladatai ellátásával kapcsolatban (így különösen szakmai véleményének megfogalmazása miatt) nem bocsáthatja el és szankcióval nem sújthatja.

Területi adatvédelmi felelős

45. §

- (1) Az Egyetem szervezeti egységei egy-egy területi adatvédelmi felelőst (továbbiakban együtt: területi adatvédelmi felelős) kötelesek kijelölni az Egyetem alkalmazottai közül, akinek személyét, elérhetőségét a szervezeti egység vezetője

kapcsolattartás céljából bejelenti az Egyetem Adatvédelmi Központjának. A Debreceni Egyetem szervezeti egységei, jelentősen összetett feladatok ellátása esetén - szükségszerűen- több területi adatvédelmi felelőst is kijelölhetnek a részterületek ez irányú feladatainak ellátására.

- (2) A területi adatvédelmi felelős feladata különösen:
- a) ellenőrzi a területéhez tartozó szervezeti egységben folytatott adatkezelést és adatfeldolgozást, és ennek során betekinthez az adatvédelemmel kapcsolatos iratokba és dokumentációba, jelentését az adatvédelmi tisztviselőnek, valamint a vezetőjének megküldi,
 - b) haladéktalanul bejelenti az Egyetem Adatvédelmi tisztviselőjének és a közvetlenül felette álló vezetőnek a területéhez tartozó szervezeti egységben történt, vagy észlelt adatvédelmi incidenst,
 - c) jelzi az adatkezeléssel és adatvédelemmel kapcsolatos problémákat az egyetemi adatvédelmi tisztviselőnek,
 - d) közreműködik az elektronikusan kezelt adatokhoz történő hozzáférés szabályozásában, valamint az Egyetem adatvédelmi és adatbiztonsági szabályzatának elkészítésében, módosításában,
 - e) előkészíti az adott szervezeti egység vonatkozásában az érintettek adatbetekintésre, adattörlésre, adatkezelés tiltására vonatkozó kérelmeit és azokat a szervezeti egység vezetője elé terjeszti. Vezeti az ezzel kapcsolatos nyilvántartásokat.
 - f) az Adatvédelmi Központ közreműködésével részt vesz az adatvédelmi tudatosság erősítésében, oktatások tartásában,
 - g) együttműködik az Adatvédelmi Központ munkatársaival.
- (3) A területi adatvédelmi felelőst titoktartási kötelezettség terheli, amely egyetemi alkalmazásának megszűnését követően is fennáll.

VIII. FEJEZET

ADATKEZELÉSSEL ÖSSZEFÜGGŐ TOVÁBBI KÖTELEZETTSÉGEK

Adatfeldolgozó igénybevétele

46. §

- (1) Az Egyetem kizárólag olyan adatfeldolgozót vehet igénybe, aki vagy amely megfelelő garanciákat nyújt arra, hogy megfelel a GDPR követelményeinek.
- (2) Az Egyetem az új adatfeldolgozó igénybevételel összefüggésben három eljárást alkalmazhat:
- a) amennyiben az adatfeldolgozó olyan belső szabályzatot mutat be, nyilatkozatot ad át, vagy honlapjain olyan kötelezettségvállalást hozott nyilvánosságra, amely alapján egyértelműen megállapítható, hogy az

- adatfeldolgozó tevékenysége megfelel a GDPR-nak, akkor ezt az Egyetem ezt önmagában elfogadhatja, és nem kell alkalmazni b) vagy c) pontot,
- b) amennyiben nem teljesülnek az a) pontban foglaltak és az Egyetem adatkezelése szempontjából az adatfeldolgozó tevékenysége nem jelent magas kockázatot, akkor a belső adatvédelmi szabályzat **11. számú mellékletében** szereplő nyilatkozatot kell kiküldeni az adatfeldolgozónak,
- c) amennyiben az adatfeldolgozó az Egyetem adatkezelése szempontjából magas kockázatú tevékenységet végez, akkor szükséges a belső adatvédelmi szabályzat **12. számú melléklete** szerinti adatfeldolgozói szerződés megkötése.
- (3) Arról, hogy az új adatfeldolgozó igénybevétel esetén a (2) bekezdésben szereplő eljárások közül az Egyetem melyiket alkalmazza, az érintett szervezeti egység vezetője dönt. Szükség esetén beszerzi az Adatvédelmi Tisztviselő véleményét.

Adatvédelmi hatásvizsgálat

47. §

- (1) Az Egyetemnek hatásvizsgálatot kell elvégeznie, ha az adatkezelés figyelemmel annak jellegére, hatókörére, körülményére és céljaira valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira.
- (2) Adatvédelmi hatásvizsgálatot kell elvégezni különösen akkor, ha
- a) az Egyetem olyan adatkezelést végez, amely az érintettek módszeres és kiterjedt értékelésére épül, és amely adatkezelés alapján az érintettre nézve joghatással bíró vagy más hasonló jelentős döntést hoznak,
 - b) az Egyetem a mindenki számára korlátozás nélkül igénybe vehető területen kamerás megfigyelést alkalmaz,
 - c) az Egyetem által végzett adatkezelés szerepel a NAIH által, az adatvédelmi hatásvizsgálat elvégzésével összefüggésben nyilvánosságra hozott jegyzékben.
- (3) Az adatvédelmi hatásvizsgálat ki kell terjednie legalább:
- a) a tervezett adatkezelés módszeres leírására és az adatkezelés céljainak ismertetésére, beleértve adott esetben az Egyetem által érvényesíteni kívánt jogos érdeket,
 - b) az irányadó jog vonatkozó rendelkezéseire, illetve - amennyiben lehetséges - a NAIH vagy bíróságok gyakorlatára, a kialakult gyakorlatra,
 - c) az adatkezelés céljaira figyelemmel az adatkezelési műveletek szükségességi és arányossági vizsgálatára,
 - d) az érintett jogait érintő kockázatok vizsgálatára és a kockázatok kezelését célzó intézkedések bemutatása.

- (4) Az Egyetem a NAIH által a honlapján nyilvánosságra hozott adatvédelmi hatásvizsgálat szoftver használatával is elvégezheti a hatásvizsgálatot.
- (5) Amennyiben a (3) bekezdés d) pont szerint az Egyetem által feltérképezett kockázatok mérséklését követően továbbra is magas kockázatúnak tekinthető az adatkezelés, akkor előzetes konzultáció kérelmével a NAIH-hoz kell fordulni. Az Adatvédelmi tisztviselő javaslatára a Kancellár dönt arról, hogy szükséges-e előzetes konzultáció érdekében a NAIH-hoz fordulni
- (6) Az adatvédelmi hatásvizsgálatot az érintett szervezeti egység végzi el, kérésre az Adatvédelmi tisztviselő szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomon követi a hatásvizsgálat elvégzését. A hatásvizsgálat eredményét a Kancellár hagyja jóvá. Amennyiben a hatásvizsgálat elvégzésének függetlensége vagy hatékonysága az Egyetemen belül nem biztosítható, akkor az adatvédelmi hatásvizsgálat elvégzésével külső szakértőt kell megbízni.

Közös adatkezelés

48. §

- (1) Amennyiben az adatkezelő másik adatkezelővel közösen végzi az adatkezelést, akkor két adatkezelőnek a belső adatvédelmi szabályzat **13. számú melléklete** szerinti megállapodást kell megkötnie.
- (2) A közösen végzett adatkezelés addig nem kezdhető meg vagy a már folyamatban levő adatkezelést fel kell függeszteni addig, amíg a közös adatkezelésben részt vevő valamennyi adatkezelő nem írta alá a megállapodást.
- (3) Abban az esetben, ha a közösen végzett adatkezelés felfüggesztése aránytalanul hátráltatná az Egyetem tevékenységét, és a közösen végzett adatkezelésnek az Egyetem tevékenysége szempontjából nincs magas kockázata, akkor a felfüggesztés megszüntethető.
- (4) A felfüggesztés megszüntetéséről az Adatvédelmi tisztviselő javaslata alapján a Kancellár dönt. A javaslatban ki kell térni:
 - a) a közös adatkezelés körülményeire,
 - b) miért javasolja a felfüggesztés megszüntetését.

IX. FEJEZET

FELELŐSSÉG AZ ADATKEZELÉSI SZABÁLYOK BETARTÁSÁÉRT, ELLENŐRZÉS

49. §

- (1) Az egyes szervezeti egységek vezetőinek és munkatársainak az adatkezeléssel összefüggő kötelezettségeit, az adatvédelmi előírások megtartásához fűződő személyi felelősségét az egyetemi Adatvédelmi tisztviselő/területi adatvédelmi felelős nem helyettesíti, hanem azt támogatja, koordinálja.
- (2) Az adatvédelemmel kapcsolatos előírások, így különösen jelen szabályzat rendelkezéseink betartását az adatkezelést végző szervezeti egységek vezetői folyamatosan kötelesek ellenőrizni.
- (3) A szervezeti egység vezetője az adatvédelemmel kapcsolatos jogsértés észlelése esetén a területi adatvédelmi felelős illetve az Adatvédelmi tisztviselő közreműködésével haladéktalanul intézkedik annak megszüntetéséről. Amennyiben az intézkedés nem jár sikerrel, az Egyetemi Adatvédelmi felelősön keresztül értesítik a Rektort és a Kancellárt, akik különösen súlyos visszaélés esetén kezdeményezik a felelősség megállapítását, indokolt esetben kártérítési eljárás megindítását, és intézkednek a törvényes állapot helyreállítása iránt.
- (4) Az egyetem Rektora, Kancellárja a szervezeti egység vezetőjének előzetes tájékoztatása mellett korlátlan, a Rektorhelyettesek, valamint a szervezeti egységek vezetői (beleértve a bizottsági és más testületi elnököket is) hatáskörükbe tartozó területen betekintési joggal rendelkeznek a szervezeti egységek adatkezelésébe. A vezetők betekintési jogukat más személyekre átruházhatják. A betekintés során megismert személyes adatokkal kapcsolatban titoktartási kötelezettség áll fenn.
- (5) Az adatkezelést végző személyek kötelesek az általuk megismert, kezelt személyes adatokat intézményi titokként megőrizni, minden erőfeszítést megtenni azok megfelelő védelmének biztosítására. Ilyen munkakörben csak olyan személy foglalkoztatható, aki titoktartási nyilatkozatot tett.
- (6) Amennyiben ezen személy munkaköre vagy tisztsége alapján személyes, különleges vagy bűnügyi személyes adatokba nyer betekintést, vagy azok birtokába jut, köteles az Info tv.-ben foglaltaknak megfelelően eljárni, így különösen a személyes adatokat csupán az előre rögzített célra használhatja fel és az adatokat óvni kell az illetéktelen hozzáféréstől.

- (7) Az Egyetem által kezelt – vagy az Egyetem feladatainak ellátásához más adatkezelő által rendelkezésre bocsátott – személyes adatok magáncélra való felhasználása tilos.
- (8) Ha az adatkezelő tudomást szerez arról, hogy az általa kezelt személyes adat hibás, hiányos vagy időszerűtlen, köteles azt helyesbíteni, vagy helyesbítését az adat rögzítéséért felelős munkatársnál kezdeményezni.

X. fejezet

ADATTOVÁBBÍTÁS

Adattovábbítás

50.§

- (1) Személyes adatok továbbítása során, amennyiben az postai küldeményként történik, biztosítani kell, hogy a küldemény zártan kerüljön feladásra. Személyes adatok elektronikus továbbítása során biztonsági, védelmi intézkedések megtétele kötelező.
- (2) Az Egyetem egyes szervezeti egységei által kezelt személyes adatok kizárólag a feladatok ellátása céljából, a feladat elvégzéséhez szükséges mértékben, a megfelelő jogalap megléte esetén továbbíthatók az Egyetem illetékes másik szervezeti egységéhez. Az adattovábbítás jogosságának elbírálásánál figyelembe kell venni, hogy az adatot kérő szervezet jogosult-e a kért adatok kezelésére.
- (3) Az Egyetemen kívüli szervtől vagy magánszemélytől érkező, adatközlésre irányuló megkeresés csak akkor teljesíthető, ha azt jogszabály vagy a GDPR rendelkezése megengedi.
- (4) Amennyiben az adatkezelő szervezeti egység olyan adatra vonatkozó megkeresést kap, melynek jogszerűségét nem tudja megítélni, köteles azt az Egyetem Adatvédelmi tisztviselőjének jelenteni és javaslatát kikérni.

Harmadik országba történő adattovábbítással összefüggő kötelezettségek

51. §

- (1) Az Egyetem csak abban az esetben továbbíthat harmadik országban található adatkezelő számára személyes adatot, vagy harmadik országban található adatfeldolgozót csak abban az esetben bízhat meg, ha az irányadó jogban és a belső adatvédelmi szabályzatban foglalt feltételek fennállnak.
- (2) Amennyiben az Európai Unió jogalkotási aktus vagy nemzeti jogszabály megállapította, hogy harmadik ország, a harmadik ország valamely területe, vagy egy vagy több meghatározott ágazata, vagy a szóban forgó nemzetközi szervezet

megfelelő védelmi szintet biztosít, akkor e vonatkozásban a személyes adatok továbbításának nincs akadálya.

- (3) Amennyiben az adattovábbítással összefüggésben az Európai Unió Bizottsága nem fogadott el határozatot, akkor az Egyetemnek az alábbi jogi eszközök közül kell választani:
- a) kötelező erejű vállalati szabályok megalkotása vagy abban történő részvétel,
 - b) az Európai Unió Bizottsága által elfogadott általános adatvédelmi kikötések,
 - c) a NAIH által elfogadott és az Európai Unió Bizottsága által jóváhagyott általános adatvédelmi kikötések,
 - d) a NAIH engedélyezi az Egyetem és más adatkezelő vagy adatfeldolgozó között létrejött szerződéses rendelkezéseket.
- (4) A harmadik országba történő adattovábbítás jogszerű abban az esetben is, ha
- a) a harmadik országbeli adatkezelő vagy adatfeldolgozó magára nézve elfogadja a GDPR 41. cikk szerinti, jóváhagyott magatartási kódexet és kötelező erejű és kikényszeríthető kötelezettségvállalást tesz azzal összefüggésben,
 - b) a harmadik országbeli adatkezelő vagy adatfeldolgozó magára nézve elfogadja a GDPR 43. cikk szerinti, jóváhagyott tanúsítási mechanizmust és kötelező erejű és kikényszeríthető kötelezettségvállalást tesz azzal összefüggésben.
- (5) Amennyiben a 2-4. alpont nem alkalmazható, kivételesen akkor kerülhet sor a harmadik országba történő adattovábbításra, ha
- a) az érintett kifejezetten hozzájárulását adta az adattovábbításhoz azt követően, hogy tájékoztatták az adattovábbításból eredő - a megfelelőségi határozat és a megfelelő garanciák hiányából fakadó - esetleges kockázatokról,
 - b) az adattovábbítás az érintett és az Egyetem közötti szerződés teljesítéséhez, vagy az érintett kérésére hozott, szerződést megelőző intézkedések végrehajtásához szükséges;
 - c) az adattovábbítás az Egyetem és valamely más természetes vagy jogi személy közötti, az érintett érdekét szolgáló szerződés megkötéséhez vagy teljesítéséhez szükséges;
 - d) az adattovábbítás fontos közérdekből szükséges;
 - e) az adattovábbítás jogi igények előterjesztése, érvényesítése és védelme miatt szükséges;
 - f) az adattovábbítás az érintett vagy valamely más személy létfontosságú érdekeinek védelme miatt szükséges, és az érintett fizikailag vagy jogilag képtelen a hozzájárulás megadására;
 - g) 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.

Adattovábbítási nyilvántartás

52.§

- (1) Az Egyetemen kívülre történő adattovábbításról nyilvántartást kell vezetni az adattovábbítást végző szervezeti egységen belül, amely nyilvántartás tartalmazza az adattovábbítás időpontját, jogalapját és címzettjét, a továbbított adat körének meghatározását és a jogszabályban előírt egyéb adatokat. A nyilvántartást meg kell küldeni az Egyetem Adatvédelmi tisztviselőjének. *(14. számú melléklet)*

XI. FEJEZET

Elektronikus megfigyelő rendszer

53.§

- (1) Az Egyetemen elektronikus megfigyelő rendszer működik.
- (2) Az Egyetem gondoskodik arról, hogy az Egyetem épületeibe látogatókat a jogszabályban előírt részletességgel, előzetesen tájékoztassa az elektronikus megfigyelő rendszerrel kapcsolatos adatkezelés lényeges követelményeiről. A kamerarendszer adatkezelési tájékoztatója elérhető a Kancellária honlapján.

XII. FEJEZET

VEGYES ÉS ZÁRÓ RENDELKEZÉSEK

54. §

- (1) A szervezeti egységek vezetői, az Egyetemi Hallgatói Önkormányzat és annak részönkormányzatai, valamint az Egyetemi Doktorandusz Önkormányzat és annak keretein belül működő kari doktorandusz képviselők elnökei kötelesek gondoskodni a jelen szabályzatban foglaltak betartásáról és betartatásáról.
- (2) Az Egyetem által fenntartott köznevelési intézmény vezetője gondoskodik arról, hogy e szabályzatot megfelelően alkalmazzák a velük munkaviszonyban vagy megbízási, illetőleg tanulói jogviszonyban álló személyekre, valamint a tanárjelöltekre.

- (3) Jelen Szabályzatot a Debreceni Egyetem Szenátusa a 2021. szeptember. 23. napján tartott ülésén a 16/2021. (XI.23.) számú határozatával elfogadta. A Szabályzat az elfogadás napját követő napon lép hatályba.
- (4) Jelen szabályzat hatálybalépésével hatályát veszti a Debreceni Egyetem Szenátusa által a 2019. január 24-én tartott ülésén 26/2019.(I.24) sz. határozatával elfogadott, és többször módosított Belső Adatvédelmi Szabályzata.

Debrecen, 2021.szeptember 23.

Prof. Dr. Szilvássy Zoltán
rektor

Prof. Dr. Bács Zoltán
kancellár

MELLÉKLETEK

1. számú melléklet

Kérdéssor az érdekmérlegelés jogalapjának alkalmazásához

1. Az alapelvek megtartása az adatkezelés során

1.1. A Debreceni Egyetem ... (Kar, szervezeti Egység) milyen tevékenysége teszi szükségessé a személyes adatok kezelését?

1.2. Ez a tevékenység végezhető-e más módszerrel, személyes adatok kezelése nélkül?

1.3. Az adattakarékosság elvének igazolása:

Kezelt személyes adat	A konkrét személyes adat kezelésének indoka
<i>Például: név</i>	<i>Például: az érintett hitelt érdemlő azonosítása a vele kötött szerződésben</i>

1.4. Mennyi ideig tart az adatkezelés? Mi az oka annak, hogy ezen időtartamig szükséges az adatkezelés?

1.5. Milyen érintetti körre vonatkozik az adatkezelés?

1.6. Van-e olyan sérülékeny érintetti kör, amely többlet védelmi intézkedést igényelne?
(Például: idősek, gyermekek)

2. A szükségességi teszt

2.1. Miért fontos az adatkezelőnek az adatkezelés? *(Még ha mindenki számára nyilvánvaló és számukra is jogszerű az adatkezeléshez fűződő érdek, akkor is ezt megfelelően magyarázni kell az érintettek számára. Pusztán abból fakadóan, hogy az adatkezelés az Adatkezelő tevékenységének az alapját jelenti, ez ön magában még nem teszi jogszerűvé az adatkezelést.)*

2.2. Ha van harmadik fél az adatkezelésben, akkor számunkra miért fontos az adatkezelés?

3. Az arányosság

3.1. Az érintettek számíthatnak a hozzájárulásuk nélkül, érdekmérlegelés jogalapjának alkalmazásával végzett adatkezelésre?

3.2. Az adatkezelésnek van hozzáadott értéke az érintett által használt termék vagy szolgáltatás vonatkozásában?

3.3. Az adatkezelés hátrányos hatással járhat az érintettek jogaira nézve?

3.4. Az adatkezelés az érintettek számára indokolatlanul okozhat-e kárt vagy más hátrányt?

3.5. Hátrányosan érinti-e az Adatkezelőt az, ha nem végezheti az adatkezelést?

3.6. Hátrányosan érinti-e az harmadik felet az, ha nem végezheti az adatkezelést?
Válasz:

3.7. Az adatkezelés az érintettek érdekében is áll?

3.8. Egybeesnek-e az érintettek és az Adatkezelő (vagy a harmadik fél) jogos érdekei?

3.9. Az adatkezelés (akár helyi, akár széles körű) társadalmi érdeknek minősül-e?

3.10. Milyen kapcsolat van az érintett és az adatkezelő között? *(Például: hallgató, volt hallgató, alkalmazott, más megbízási vagy vállalkozási jogviszonyban dolgozó személy, üzleti partner, jövőbeli hallgató, aki még nem áll kapcsolatban az Egyetemmel.)*

3.11. Milyen időszakot ölel fel az érintett és az adatkezelő közötti kapcsolat? *(Például: folyamatos viszony áll fenn az adtakezelő és az érintett között, vagy csak meghatározott időszakonként kerül kapcsolatba az adatkezelő az érintettel, vagy pedig egy alkalommal került kapcsolatba az érintett az adatkezelővel, avagy az adatkezelést megelőzően semmilyen kapcsolat nem volt az érintett és az adatkezelő között)*

3.12. Milyen személyes adatokra vonatkozik az adatkezelés? Kiterjed-e különleges adatokra az adatkezelés?

3.13. Az adatkezelés ellehetetleníti vagy korlátozza az érintettnek a GDPR 15-22. cikk szerinti jogainak gyakorlását?

3.14. Az Adatkezelő a személyes adatokat közvetlenül az érintettől szerzi meg vagy közvetett módon, más forrásból?

3.15. Az érintettek valószínűleg számíthatnak arra, hogy a tervezett adatkezelési célból az Adatkezelő kezelni fogja a személyes adatait?

3.16. Az adatkezelést az érintettek az adatkezelés jellegéhez képest tolaakodónak vagy aránytalannak tarthatják?

3.19. Az adatkezeléshez készült megfelelő részletezettségű, közérthető és világos adatkezelési tájékoztató?

3.18. Az érintett tud kontrollt gyakorolni a személyes adatai kezelésével kapcsolatban, így különösen kérheti-e a személyes adatainak a törlését? Amennyiben az érintettnek nincs kontrollja, akkor mi ennek az oka?

3.19. Az adatkezelés körülményei (például milyen érintetti körre és mely személyes adatokra terjed ki az adatkezelés, mennyi ideig tart az adatkezelés) szűkíthetők-e, csökkenthetők-e?

4. Az érdekmérlegelés jogalapja által érintett jogok

4.1. Milyen módon korlátozza az adatkezelés az érintett személyes adatai feletti rendelkezési jogát? *(Például a hozzájárulása nélkül nyilvánosságra hozhatják, más személy hozzáférhet)*

4.2. Érinti-e az adatkezelés az érintett más jogát, szabadságát vagy érdekét? *(Például: a véleménynyilvánítás szabadsága, a magán- és a családi élet, az otthon és a kapcsolattartás tiszteletben tartásához való jog, vagy a hatékony jogorvoslathoz és a tisztességes eljáráshoz való jog.)*

4.3. Milyen elvárásai lehetnek (vannak) az érintettnek az Adatkezelővel szemben, hogy milyen garanciák betartására legyen figyelemmel az adatkezelés során?

5. Garanciális intézkedések az adatkezelés során

Be kell mutatni, hogy milyen garanciális intézkedéseket alkalmaz az Adatkezelő annak érdekében, hogy csökkentse az érintettet érő negatív hatásait az adatkezelésnek. Ilyen intézkedések lehetnek például (az adatkezelés jellegéhez képest ezek közül lehet választani, vagy további intézkedéseket lehet alkalmazni):

- a kezelt személyes adatok körének a szükséges minimálisra szűkítése,*
- az adatkezelés időtartamának a lehető legrövidebb időre korlátozása,*
- az érintettek bármikor ki tudják kapcsolni az adatkezelést,*
- az adatok álnevesítése,*
- egy olyan felület létrehozása, amely alapján az érintett figyelemmel tudja követni, hogy milyen személyes adataira terjed ki az adatkezelés,*
- az érintett számára plusz tájékoztatás beiktatása (például az adatkezelési tájékoztatót és az érdekmérlegelési tesztet e-mailen is elküldik),*
- meghatározott személyi kör férhet hozzá a személyes adatokhoz, és a hozzáférés naplózása,*
- többfaktoros belépés az érintettek személyes adatait tartalmazó adatbázisba,*
- az adatbázis titkosítása vagy anonimizálása,*
- az alkalmazott ellenőrzése esetében a fokozatosság betartása (csak akkor kerül sor az alkalmazott ellenőrzésére, ha más módszerrel nem tárható fel valamely jogsértés) és az alkalmazott jelenlétének biztosítása az ellenőrzés során*

2. számú melléklet

Érdekmérlegelési teszt

[adatkezelés megnevezése] vonatkozásában

1. Az érdekmérlegelés jogalapja és az érdekmérlegelési teszt

A GDPR 6. cikk (1) bekezdés f) pontja alapján az adatkezelés jogszerűnek tekinthető abban az esetben is, ha "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."

Ezen jogalap alkalmazása esetén az adatkezeléshez nem szükséges az érintett hozzájárulása, hanem azt követeli meg, hogy a DE az érintettek számára igazolni tudja azt, hogy

- valósnak, tényleges jogos érdekekkel rendelkezik az adatkezeléshez,
- az adatkezelés milyen jogokat érint, milyen elvárásai lehetnek az érintettnek az adatkezeléssel összefüggésben.
- olyan garanciális intézkedéseket hozott, amelyek biztosítják azt, hogy a jogos érdeke alapján végzett adatkezelések arányosan korlátozzák az érintettek jogait, magánszféráját.

Ezen megfelelést az DE egy érdekmérlegelési tesztben foglalja össze, amelyben bemutatja, hogy az [adatkezelés megnevezése] esetében milyen jogos érdekei vannak, és az Ön jogai védelme érdekében milyen garanciális intézkedéseket hozott.

2. Jogos érdekek

Az adatkezeléssel összefüggésben az alábbi jogos érdeke(i) vannak:

- [miért előnyös az adatkezelőnek]
- [miért előnyös magának az érintettnek]
- [de az is ide tartozik, ha az adatkezelés valami más céggel kötött szerződéses kötelezettség teljesítéséhez szükséges]

3. Az érintetti elvárások és garanciális intézkedések

Vizsgálatunk alapján az adatkezelésünk az Ön személyes adatok védelméhez fűződő jogát érinti.

Emellett a vizsgálatunk alapján arra a következtetésre jutottunk, hogy az adatkezelésünk során biztosítani kell, hogy (a lehető legrövidebb ideig tartson az adatkezelés,

- csak az elengedhetetlenül szükséges adatok kezelésére terjedjen ki,
- csak olyan személyek férjenek hozzá a személyes adatokhoz, akiknek feladataik vagy munkakörük ellátása érdekében ez ténylegesen indokolt,
- megfelelő tájékoztatást kapjon az adatkezelésről,
- tiltakozása esetén az adatkezelést megszüntessük (ez csak néhány adatkezelés esetén jöhet szóba, pl. marketing célú adatkezeléseknél).

Annak érdekében, hogy az adatkezelés csak a szükséges mértékben korlátozza az adatkezelést, az alábbi garanciális intézkedéseket alkalmazzuk:

- Az adatkezelés a jogviszony keletkezésétől ... napig / évig tart. Ez azért indokolt, mert ...
- Az alábbi adatok szükségesek ezen adatkezelés esetében: (felsorolni a kezelt adatokat). Ezek közül például a név, születési hely és idő adat kezelése azért szükséges az adatkezeléshez, mert A ... és a ... személyes adatok kezelése azért fontos, mert ...
- A jogosultsági rendszerünk alapján a személyes adatokhoz csak ... munkakörben és a ... munkakörben dolgozó munkavállalók férnek hozzá. A ... személyes adatok nem kapják meg.
- Jelen érdekmérlegelési teszt többek között azt a célt is szolgálja, hogy Ön megfelelő információkkal rendelkezzen az adatkezelésről.
- Az Önt megillető jogokat és jogorvoslati lehetőségeket megtalálja az adatkezelési tájékoztatónkban, amelynek az alábbi linken keresztül érhető el (vagy letölthető): .

Keltezés, aláírás

3. számú melléklet

Adatkezelési tájékoztató

1. Az adatkezelő megnevezése és elérhetőségei

[adatkezelő neve]

Székhely: ...
Posta cím: ...
E-mail cím: ...
Telefonszám: ...

2. Adatkezelésre vonatkozó jogszabályok

Az [adatkezelő neve] adatkezelésére az alábbi jogszabályi rendelkezések vonatkoznak:

- A személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről szóló az Európai Parlament és a Tanács 2016. április 27-i (EU) 2016/679 rendelet (a továbbiakban: GDPR).
- A ... szóló ... törvény (a továbbiakban: ...).

3. Az adatkezelő által végzett adatkezelések

3.1. A..... összefüggő adatkezelés

3.1.1. *Az adatkezelés célja:* ...

3.1.2. *Kezelt adatok köre:* Az adatkezelés során az alábbi személyes adatokat kezeljük:

- ...
- ...

3.1.3. *Az adatkezelés jogalapja:* ... (pl. hozzájárulás) [a GDPR szerinti jogalap pontos megjelölése: GDPR 6. cikk (1) bekezdés a) pont].

3.1.4. *Az adatkezelés időtartama:* ...

3.1.5. *Hozzáfééréssel rendelkezők köre:* ...

3.2. A ... összefüggő adatkezelés

3.2.1. Az adatkezelés célja:

3.2.2. Kezelt adatok köre: ...:

- ...

3.2.3. Az adatkezelés jogalapja: ...

3.2.4. Az adatkezelés időtartama: ...

4. Az Ön jogai és a joggyakorlásra vonatkozó szabályok

4.1. Tájékoztatáshoz való jog

A GDPR 15. cikk (1) bekezdésének megfelelően, Ön tájékoztatást kérhet az [adatkezelő neve] által kezelt személyes adatokról. Ebben az esetben az [adatkezelő neve] az Ön által megjelölt elérhetőségére (e-mail cím, levelezési cím) továbbítja az alábbi információkat:

- milyen személyes adatokat kezelünk Önről;
- milyen adatkezelés célokból;
- kiknek továbbítjuk a személyes adatokat;
- az adatkezelés időtartama, illetve ezen időtartam meghatározásának szempontjai;
- Önt adatkezeléssel összefüggésben megillető jogokról;
- a Nemzeti Adatvédelmi és Információszabadság Hatóságnak címzett panasz benyújtásának jogáról.

4.2. Másolat kéréséhez való jog

A GDPR 15. cikk (3)-(4) bekezdése alapján Ön másolatot kérhet az [adatkezelő neve] által kezelt személyes adatokról. Ebben az esetben az [adatkezelő neve] az Ön által megjelölt elérhetőségére (e-mail cím, levelezési cím) továbbítja azokat a személyes adatokat, amelyeket Önről kezelünk.

4.3. Helyesbítéshez való jog

A GDPR 16. cikkének megfelelően, kérelmére az Ön kérésének megfelelően módosítjuk, pontosítjuk a személyes adatát.

4.4. Törléshez való jog

A 3.4. alpont szerinti adatkezelés esetében a GDPR 17. cikk (1) bekezdésével összhangban Ön kérheti, hogy töröljük a nyilvánosságra hozott személyes adatokat.

4.5. Korlátozáshoz való jog

Ön kérheti az adatkezelés korlátozását az alábbi esetekben:

- ha vitatja a személyes adatok pontosságát, akkor addig korlátozzuk az adatkezelést, amíg az [adatkezelő neve] ellenőrizi a személyes adatok pontosságát;
- az adatkezelés jogellenes, és Ön ellenzi az adatok törlését, és ehelyett kéri azok felhasználásának korlátozását;
- az [adatkezelő neve]-nek már nincs szüksége a személyes adatokra, de Ön igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez; vagy
- amennyiben a tiltakozás jogát gyakorolja, akkor arra az időtartamra korlátozzuk az adatkezelést, amíg a kérelmének jogszerűségét megvizsgáljuk.

Az adatkezelés korlátozására irányuló kérelmében esetében azt is meg kell jelölni, hogy melyik okból kéri a korlátozást.

Az [adatkezelő neve] az adatkezelés korlátozására irányuló kérelmét úgy teljesíti, hogy a személyes adatokat minden más személyes adattól elkülönítetten tárolja. Így például elektronikus adatállományok esetében külső adathordozóra kimentti, a papír alapú iratokat pedig külön mappában tárolja.

4.6. Tiltakozás

Ön jogosult arra, hogy a saját helyzetével kapcsolatos okokból tiltakozzon a jogos érdek mérlegelése alapján végzett adatkezelés ellen. Ebben az [adatkezelő neve] megvizsgálja az Ön vonatkozásában az érdekmérlegelés jogalapján végzett adatkezelését, és amennyiben megalapozottnak találja a kérelmét, töröljük a személyes adatait. A vizsgálatunkról Önt mindenképp tájékoztatni fogjuk.

4.7. A joggyakorlás közös szabályai

Az [adatkezelő neve] a kérelmét legfeljebb egy hónapon belül teljesíti, amely legfeljebb két hónappal meghosszabbítható.

A kérelem megtagadása esetén az [adatkezelő neve] a kérelem beérkezésétől számított egy hónapon belül tájékoztatja Önt a megtagadás indokairól, valamint arról, hogy panaszt nyújthat be a Hatóságnál, és élhet bírósági jogorvoslati jogával.

Az [adatkezelő neve] fenntartja magának azt a jogot, hogy ha megalapozott kétségei vannak a kérelmet benyújtó személy kilétét illetően, akkor az érintett személyazonosságának megerősítéséhez szükséges információk nyújtását kérje. Ilyen esetnek tekinthető különösen az, ha az érintett a másolat kéréséhez való jogával él, amely esetben indokolt, hogy az [adatkezelő neve] meggyőződjön arról, hogy a kérelem a jogosult személytől származik

5. Az Ön jogérvényesítési lehetőségei

Amennyiben az Ön megítélése szerint az [adatkezelő neve] adatkezelése nem felel meg a jogszabályi követelményeknek, akkor a Nemzeti Adatvédelmi és Információszabadság Hatóság (Postacím: 1363 Budapest, Pf. 9. e-mail cím: ugyfelszolgalat@naih.hu) eljárását kezdeményezheti, illetve bírósághoz fordulhat.

5. számú melléklet

Érintetti kérelem (ajánlottan alkalmazandó)

Bejelentő neve:

Azonosító okmány típusa és jelzése:

A bejelentő elérhetősége:

Adatkezelési igény típusa: Igény esetén aláhúzással jelölje

Tájékoztatás kérés kezelt adatokról (GDPR 13. és 14. cikk):

Személyes adatokhoz való hozzáférés (GDPR 15. cikk)

Személyes adatok módosítása (GDPR 16. cikk)

Személyes adatok törlése (GDPR 17. cikk)

Személyes adatok kezelésének korlátozása (GDPR 18. cikk):

Tiltakozási személyes adatok kezelése ellen (GDPR 21. cikk):

Alulírott az alábbi igénnyel fordulok a Debreceni Egyetemhez, mint adatkezelőhöz:

.....
.....
.....
.....
.....
.....
.....

Keltezés, aláírás

Informatikai biztonsági Intézkedések

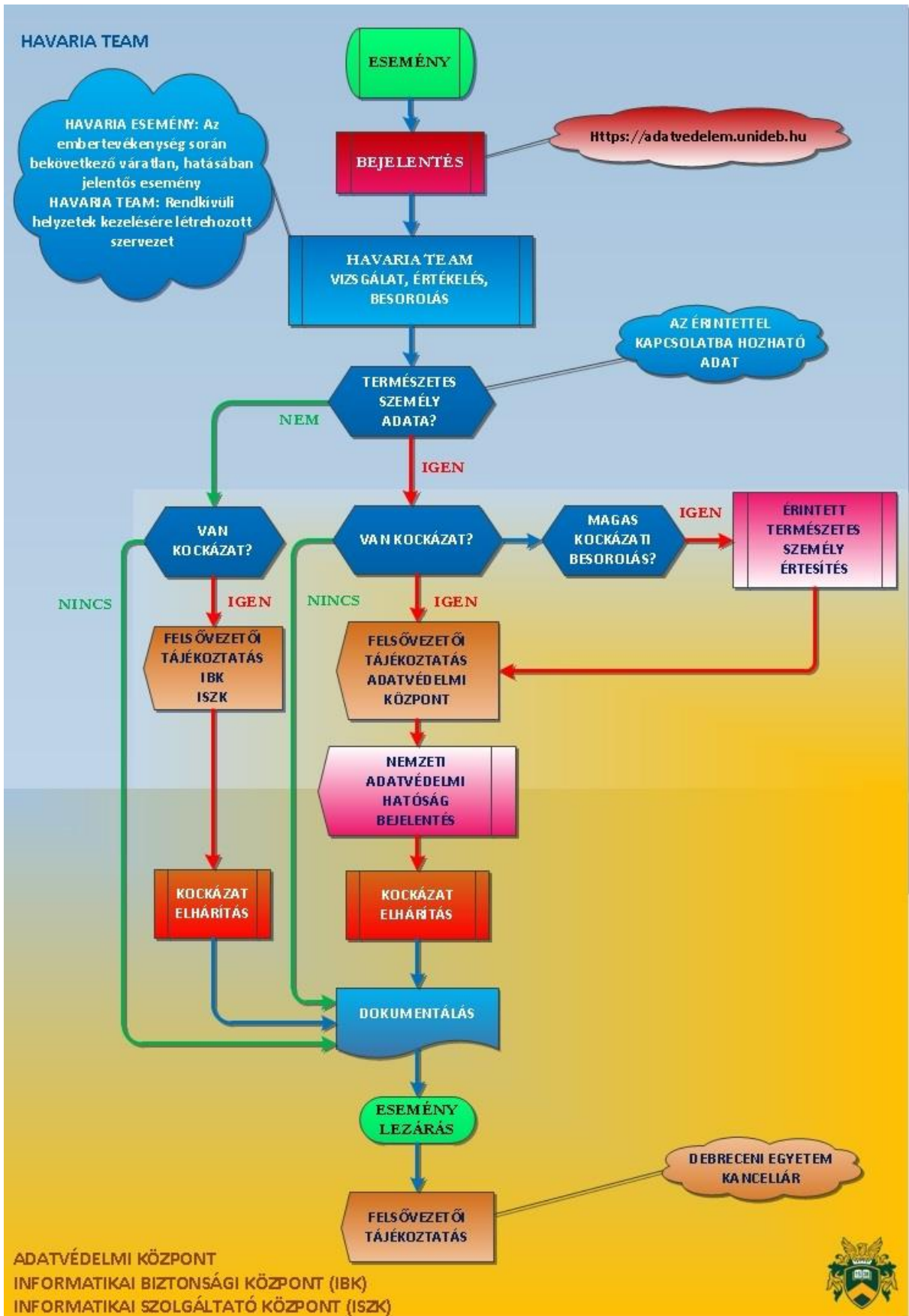
Informatikai biztonsági Intézkedés	Alkalmazott megoldás
Annak megakadályozása, hogy jogosulatlan személyek hozzáférést szerezzenek vagy belépjenek ezen rendszerekbe	
Megfelelő hozzáférési jogosultságok beállítása, illetve felhasználó nevet és a jelszót rendelnek hozzá az egyes jogosultságokhoz	
A jelszóhasználati előírások szabályozása (például a jelszó minimum hossza, használható karakterek, érvényesség időtartam, téves jelszóhasználatok száma a fiók zárolása előtt)	
Annak biztosítása, hogy a jogosultsággal rendelkező személyek a személyes adatokhoz csak a hozzáférési engedélyük keretein belül férhessenek hozzá	
Naplózás útján annak biztosítása, hogy ellenőrizhető legyen, mely felhasználó lépett be és milyen szoftverbe	
Annak biztosítása, hogy mely személyes adatokat mikor és ki vitte be, módosította vagy továbbította	
Annak biztosítása, hogy a személyes adatok engedély nélkül nem olvashatók, másolhatók, módosíthatók vagy tárolhatók el	
Az informatikai rendszerek folyamatos rendelkezésre állásának biztosítása	
Hálózatbiztonsággal összefüggő védelmi intézkedések	

Vírusvédelemmel, illetve a más rosszindulatú software-ek elleni védelemmel összefüggő intézkedések	
A munkaállomások védelmét biztosító intézkedések (például automatikus zárás, rendszeres frissítés)	
Az informatikai rendszerek folyamatos rendelkezésre állását biztosító intézkedések	
Fizikai vagy műszaki incidens esetén annak biztosítása, hogy a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását kellő időben vissza lehet állítani, az ilyen incidensekről jelentés készül, illetve az ilyen incidensek nem hatnak ki az adat integritására	
A személyes adatok titkosítása vagy álnevesítése (amennyiben ez az adott adatkezelés esetében indokolt)	
Annak biztosítása, hogy a különböző célből kezelt személyes adatokat (adatbázisokat) elkülönítve tárolják (amennyiben ez az adott adatkezelés esetében indokolt és lehetséges)	
Adatfeldolgozó igénybevétele esetén annak biztosítása, hogy megfelelő garanciák vonatkoznak az általuk végzett tevékenységre (például a személyes adatokat titkosítva adják át a számukra, jogosultságkezelés és hitelesítés)	

Dátum, keltezés

Aláírás

7. számú melléklet



8. számú melléklet

Adatvédelmi incidens nyilvántartás

Cím: [az adatvédelmi Incidens időpontja és az adatvédelmi Incidens jellege]

1. Az adatvédelmi Incidens bekövetkezése előtt alkalmazott intézkedések:

2. Az adatvédelmi Incidens jellege:

3. Az adatvédelmi Incidens oka:

4. Az adatvédelmi Incidenssel érintett személyes adatok típusa és mennyisége (legalább becsléssel):

5. Az érintettek száma:

6. Az érintettek kategóriái:

7. Az adatvédelmi Incidens lehetséges vagy már megtörtént következményei, illetve azok súlyossága az érintettekre nézve:

8. Amennyiben az Adatkezelő mellőzte az adatvédelmi Incidens bejelentést, akkor ennek oka:

9. Amennyiben nem volt szükséges az érintettek tájékoztatása, akkor ennek oka:

10. Amennyiben szükséges lett volna, de az Adatkezelő mellőzte az érintettek tájékoztatását, akkor ennek oka:

11. Az adatvédelmi Incidens orvoslására és az okainak megszüntetésére tett intézkedések:

9. számú melléklet

Adatvédelmi tisztviselő / területi adatvédelmi felelős által végzett feladatok nyilvántartása

Nyilvántartási szám/sorszám	Intézkedés dátuma	Intézkedés megnevezése	Intézkedés leírása	Intézkedés eredménye

10. számú melléklet

Jelenléti ív adatvédelmi oktatásra

Jelenléti ív

A Debreceni Egyetem, - az oktatás helyszíne, a szervezeti egység megnevezése, dátum, időponttól szervezett, az oktatás/előadás témájának leírása - témakörben megtartott előadáson megjelent személyekről.

Sorsz.	Résztevő neve /Nyomtatott betűvel/	Résztevő aláírása	Szervezeti egységének megnevezése
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			

11. számú melléklet

[Adatfeldolgozó neve]

[Adatfeldolgozó címe]

TÁRGY: A GDPR-nak való megfelelésről szóló nyilatkozat

Tisztelt [Kapcsolattartó neve]!

Amint azzal bizonyosan tisztában vannak, a **Debreceni Egyetem** (székhely: 4032 Debrecen, Egyetem tér 1.; a továbbiakban: **Adatkezelő**) részére nyújtott szolgáltatásai keretében az Adatkezelő által kezelt személyes adatokhoz férnek hozzá, így Önök az Adatkezelő adatfeldolgozójának minősülnek.

Az Európai Parlament és a Tanács 2016. április 27-i (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (a továbbiakban: GDPR) számos új kötelezettséget jelent az adatkezelők és az adatfeldolgozók számára.

A GDPR 28. cikk (1) bekezdése kifejezetten előírja az adatkezelők számára, hogy csak olyan adatfeldolgozókat vehetnek igénybe, amelyet teljesíteni tudják a GDPR elvárásait.

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

Ennek érdekében arra kérjük Önöket, hogy a GDPR 28. cikk (1) bekezdésének való megfelelés érdekében levelünkhöz mellékelt nyilatkozatot töltsék ki, és a nyilatkozat aláírását követően postai úton küldjék vissza a számunkra.

Köszönjük az együttműködésüket. Amennyiben kérdésük lenne állunk a rendelkezésükre.

[Dátum, keltezés]

Tisztelettel,
[Aláírás]

Adatfeldolgozó GDPR-nak való megfeleléssel kapcsolatos nyilatkozata

Alulírott, mint az **Adatfeldolgozó neve** (székhely, cégjegyzékszám, adószám) (továbbiakban: Társaság) képviselőjét ellátó személy, akinek jogosultsága van a jelen kötelezettségvállaló nyilatkozatot tenni, az alábbiak szerint nyilatkozom.

A Társaság kijelenti, hogy tudomással bír arról, hogy **Debreceni Egyetem** (székhely: 4032 Debrecen, Egyetem tér 1.; a továbbiakban: **Adatkezelő**) részére nyújtott szolgáltatásai során az Adatkezelő által kezelt személyes adatokhoz hozzáfér, adatfeldolgozóként közreműködünk az adatkezelés végrehajtásában.

A Társaság kijelenti, hogy a személyes adatokat kizárólag az Adatkezelő utasításai alapján kezeli, és az Adatkezelő által adott utasításokat végrehajtja. Amennyiben el kíván térni az Adatkezelő utasításától, vagy valamely jogszabályi rendelkezés felülírja az Adatkezelő által adott utasítást, akkor arról előzetesen tájékoztatnia kell az Adatkezelőt.

A Társaság vállalja, ha más céget vagy egyéni vállalkozót venne igénybe a Társaság és az Adatkezelő közötti szerződés teljesítéséhez, akkor erről előzetesen értesíti az Adatkezelőt. Ha az Adatkezelő elfogadja a cég vagy egyéni vállalkozó igénybevételét, akkor a Társaság gondoskodik arról, hogy ők is ugyanilyen tartalmú nyilatkozatot tegyenek a Társaság felé.

A Társaság biztosítja azt, hogy a munkavállalói - illetve más cég vagy egyéni vállalkozó közreműködése esetén, a cég munkavállalói vagy az egyéni vállalkozó - titoktartási kötelezettséget vállalnak vagy jogszabály alapján megfelelő titoktartási kötelezettség alatt állnak.

A Társaság garantálja a GDPR 32. cikk szerinti, az általa végzett tevékenységgel összhangban álló megfelelő szintű adatbiztonságot.

Adatvédelmi incidens esetén a Társaság az arról való tudomásszerzést követően 24 órán belül értesíti az Adatkezelőt. A Társaságnak kötelessége együttműködni az Adatkezelővel az adatvédelmi incidensnek a Nemzeti Adatvédelmi és Információszabadság Hatósághoz történő bejelentése, illetve az adatvédelmi incidens kivizsgálása során.

A Társaság vállalja, hogy az Adatkezelő és a Társaság közötti szerződés megszűnését követően az Adatkezelő utasításától függően minden személyes adatot töröl vagy visszajuttatja a személyes adatokat tartalmazó dokumentumot az Adatkezelőnek, és törli a meglévő másolatokat.

Ha a Társaság azt észleli, hogy az Adatkezelő utasítása sérti a GDPR vagy más jogszabályi rendelkezéseket, akkor a Társaság erre írásban felhívja az Adatkezelő figyelmét.

[Dátum, keltezés]

[Aláírás]

12. számú melléklet

Adatfeldolgozói Szerződés

amely létrejött egyrészről a Debreceni Egyetem (székhely: 4032 Debrecen, Egyetem tér 1., adószám: 19308667-4-09, csoport adóazonosító szám: 17782218-5-09, közösségi adószám: HU17782218, Intézményi azonosító: FI 17198, számlaszám:, képviseli: Prof. Dr. Bács Zoltán kancellár, jelen szerződés tekintetében az RH/..... sz. meghatalmazásnak megfelelően:, a továbbiakban: Adatkezelő),

másrészről a (partner adatai), a továbbiakban: Adatfeldolgozó) között az alábbi feltételekkel:

1. Alapfogalmak

1.1. adatvédelmi Incidens: a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, módosítását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi.

1.2. EGT-állam: az EGT tagállamokon (az EU tagállamai, illetve Izland, Liechtenstein és Norvégia) kívüli országok.

1.3. GDPR: Az Európai Parlament és a Tanács 2016. április 27-i (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK Irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet). A rendeletnek a gyakorlatban elterjedt rövidítése az angol elnevezéséből (General Data Protection Regulation) képzett GDPR mozaikszó.

1.4. NAIH: Nemzeti Adatvédelmi és Információszabadság Hatóság.

2. Adatfeldolgozó GDPR-nak való megfelelése

Az Adatfeldolgozó szavatolja, hogy szakértői szintű ismerettel, megbízhatósággal és erőforrásokkal rendelkezik ahhoz, hogy a GDPR követelményeinek teljesülését biztosító technikai és szervezési intézkedéseket – ideértve az adatkezelés biztonságát is – végrehajtsa.

3. Az adatfeldolgozás terjedelme

Az Adatkezelő az alábbi adatkezeléshez kapcsolódóan veszi Igénybe az Adatfeldolgozót:

- az adatkezelés tárgya: a napján tárgyban kötött szerződés szerinti személyes adatok kezelése
- az adatkezelés jellege és célja:
- az adatkezelés időtartama:
- a kezelt adatok köre:

4. Az Adatfeldolgozó általános kötelezettségei

4.1. A személyes adatok Adatfeldolgozó általi kezelése jelen szerződés keretében történik, és csak abban a mértékben, amelyben az Adatkezelő utasította az Adatfeldolgozót és kizárólag szolgáltatással kapcsolatban. Az Adatfeldolgozó az Adatkezelő nevében kezeli a személyes adatokat.

4.2. Amennyiben szolgáltatás ellátásához szükségessé válik a személyes adatok továbbítása (beleértve az adattovábbítás bármilyen formáját, de különösen harmadik országba történő továbbítást), akkor az Adatfeldolgozó ezt kizárólag az Adatkezelő előzetes jóváhagyásával teheti meg. A harmadik országba történő továbbításba bele értendő a felhőalapú adatkezelés is, ha a felhőalapú szolgáltatás nyújtója nem tudja megjelölni, illetve szavatolni, hogy a harmadik országon kívül nem végeznek adatkezelési műveletet a részére feldolgozási céllal átadott adatokkal kapcsolatban.

4.3. Az Adatfeldolgozó a szolgáltatások nyújtásához elvárt és szükséges mértéket meghaladóan a személyes adatokat semmilyen más célból nem kezelheti, illetve használhatja fel.

4.4. Az Adatfeldolgozó köteles a rá vonatkozó magyar és uniós jogszabályokat, illetve hatósági előírásokat betartani. Az Adatfeldolgozó köteles biztosítani az együttműködés, támogatás minden olyan formáját és megadni minden olyan információt, amelyet Adatkezelő Igényel annak érdekében, hogy igazolni tudja a vonatkozó jogszabályoknak való megfelelését és kötelezettségeinek teljesítését, valamint a NAIH-hal együttműködhessen és annak utasításait vagy döntéseit végrehajtsa úgy, hogy a NAIH vagy az eljárást folytató felügyeleti hatóság által előírt határidőt be tudja tartani.

4.5. Az Adatfeldolgozó a személyes adatokat kizárólag az Adatkezelő írásbeli utasításai alapján kezeli – beleértve a személyes adatoknak valamely harmadik ország vagy nemzetközi szervezet számára való továbbítását is –, kivéve akkor, ha az adatkezelést az Adatfeldolgozóra alkalmazandó uniós vagy tagállami jog írja elő. Ebben az esetben erről a jogi előírásról az Adatfeldolgozó az Adatkezelőt az adatkezelést megelőzően értesíti, kivéve, ha az ilyen értesítést az adott jogszabály fontos közérdekből tiltja.

Adatfeldolgozó Adatkezelő rendelkezésére bocsát minden olyan Információt, amely a GDPR 28. cikkében meghatározott kötelezettségek igazolásához szükséges, továbbá amely lehetővé teszi és elősegíti az Adatkezelő által vagy az általa megbízott más ellenőr által végzett auditokat, beleértve a helyszíni vizsgálatokat is.

4.6. Az Adatfeldolgozó szavatolja, hogy a személyes adatok kezelésére feljogosított személyek titoktartási kötelezettséget vállalnak vagy jogszabály alapján megfelelő titoktartási kötelezettség alatt állnak.

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

- a személyes adatok álnevesítését és titkosítását;
- a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítását, integritását, rendelkezésre állását és ellenálló képességét;
- fizikai vagy műszaki incidens esetén az arra való képességet, hogy a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását kellő időben vissza lehet állítani;
- az adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedések hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárást.

4.8. Az Adatfeldolgozó haladéktalanul tájékoztatja az Adatkezelőt, ha úgy véli, hogy valamely utasítás sérti az Irányadó jogot vagy más uniós vagy tagállami adatvédelmi rendelkezést.

4.9. Az Adatfeldolgozó az adatkezeléshez kapcsolódó szolgáltatás nyújtásának befejezését követően az adatkezelés jellegétől, valamint az Adatkezelő utasításától függően minden személyes adatot töröl vagy visszajuttat az Adatkezelőnek, és törli a meglévő másolatokat, kivéve, ha az uniós vagy a tagállami jog a személyes adatok tárolását írja elő. Amennyiben az Adatfeldolgozó részére az uniós vagy a tagállami jog a személyes adatok tárolását írja elő, akkor az Adatfeldolgozó haladéktalanul, de legkésőbb az erről való tudomásszerzést követő 5 munkanapon belül az ezt alátámasztó megfelelő dokumentum Adatkezelő részére történő megküldésével igazolni köteles az Adatkezelő számára az Adatkezelő által kezelt személyes adatok további tárolását.

5. További adatfeldolgozók igénybevétele

5.1. Az Adatfeldolgozó az Adatkezelő előzetes kifejezett felhatalmazása nélkül más adatfeldolgozót nem vehet igénybe.

5.2. Amennyiben az Adatfeldolgozó – az Adatkezelő előzetes kifejezett felhatalmazásával – bizonyos, az Adatkezelő nevében végzett konkrét adatkezelési tevékenységekhez további adatfeldolgozót is igénybe vesz, szerződés útján erre a további adatfeldolgozóra is ugyanazokat az adatvédelmi kötelezettségeket kell telepíteni, mint amelyeket a jelen szerződésben is kijelöltek, különösen úgy, hogy elegendő garanciát nyújtson a megfelelő technikai és szervezési intézkedések végrehajtására oly módon, hogy az adatkezelés megfeleljen az Irányadó jog követelményeinek.

5.3. Csak olyan további adatfeldolgozó javasolható, akinek/amelynek az alkalmasságát az Adatfeldolgozó megfelelően alátámasztotta, vagy akinek/amelynek az alkalmasságáért szavatosságot vállalt.

5.4. Adatkezelő bármikor visszavonhatja a további adatfeldolgozó igénybevételére szóló hozzájárulását, ha olyan információ birtokába kerül, amely kétségessé teszi az alkalmasságát.

6. Kapcsolattartás és utasítások rendje

6.1. Az Adatkezelő vállalja, hogy a jelen szerződés megkötése napjától számított 1 munkanapon belül tájékoztatja az Adatfeldolgozót az Adatkezelő kapcsolattartójának (vagy kapcsolattartóinak) nevéről, e-mail címéről és telefonszámáról. Az Adatkezelő részéről Adatkezelő kapcsolattartója (vagy kapcsolattartói) jogosult(ak) az adatkezeléssel kapcsolatosan utasítást adni, illetve az Adatfeldolgozó ezen kapcsolattartót (vagy kapcsolattartókat) köteles az észrevételeivel megkeresni. Az Adatkezelő vállalja, hogy ezen adatok változásról a változást követő egy munkanapon belül tájékoztatást ad az Adatfeldolgozó számára.

6.2. Az Adatfeldolgozó vállalja, hogy a jelen szerződés megkötése napjától számított 1 munkanapon belül tájékoztatja az Adatkezelőt az Adatfeldolgozó kapcsolattartójának (vagy kapcsolattartóinak) nevéről, e-mail címéről és telefonszámáról. Az Adatkezelőnek jelen szerződéssel kapcsolatos utasításait az Adatfeldolgozó kapcsolattartójának (vagy kapcsolattartóinak) kell címeznie. Az Adatfeldolgozó vállalja, hogy ezen adatok változásról a változást követő 1 munkanapon belül tájékoztatást ad az Adatkezelő számára.

7. Az adatvédelmi incidens bejelentése

7.1. Adatvédelmi Incidens esetén az Adatfeldolgozó az arról való tudomásszerzést követően indokolatlan késedelem nélkül, és nem később, mint 24 órán belül köteles bejelenteni az adatvédelmi Incidenszt az Adatkezelőnek és együttműködni az Adatkezelővel az illetékes felügyeleti hatóság értesítése során.

7.2. Az Adatfeldolgozó 24 órán belüli értesítésében köteles kitérni az alábbiakra:

- az adatvédelmi Incidens jellege (a személyes adatok véletlen vagy jogellenes megsemmisítése, elveszítése, módosítása, jogosulatlan közlése vagy az azokhoz való jogosulatlan hozzáférés)
- az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó neve és elérhetőségei;

7.3. Amennyiben az Adatfeldolgozó nem értesíti az Adatkezelőt 24 órán belül, az Adatfeldolgozó köteles az Adatkezelőt a késedelem okairól tájékoztatni.

7.4. Az Adatfeldolgozó köteles az adatvédelmi Incidenssel kapcsolatosan azonnal tájékoztatni az Adatkezelőt az alábbiakról, amint azok adott körülményei tisztázódnak:

- adatvédelmi Incidens részletes leírása;
- az adatvédelmi Incidens jellege, beleértve, ha lehetséges, az érintettek kategóriáit és hozzávetőleges számát, valamint az érintett személyes adatok típusát, kategóriáit és hozzávetőleges számát;
- minden egyes érintett személy megnevezése (vagy amennyiben ez nem lehetséges az érintettek és a személyes adatokat tartalmazó nyilvántartások/adatbázisok száma);
- az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó neve és elérhetőségei;
- az adatvédelmi Incidens valószínűsíthető következményei;
- az Adatfeldolgozó által az adatvédelmi Incidens orvoslására tett vagy tervezett intézkedések, beleértve adott esetben annak esetleges hátrányos következményei enyhítését célzó intézkedéseket.

8. Az érintett joggyakorlás teljesítésében való közreműködése

8.1. Az Adatfeldolgozó aktívan támogatja az Adatkezelőt azon kötelezettsége teljesítésében, hogy megerősítse, hogy bizonyos érintettre vonatkozó személyes adatok kezelése folyamatban van-e vagy sem, és amennyiben ez az eset áll fenn, hozzáférést biztosítson az érintett számára a személyes adatokhoz és információkhoz.

8.2. Az Adatfeldolgozó aktívan támogatja az Adatkezelőt azon kötelezettsége teljesítésében, hogy indokolatlan késedelem nélkül:

- helyesbítse a pontatlan személyes adatokat;
- kiegészítse a hiányos személyes adatokat;
- törölje a személyes adatokat,
- korlátozza az adatkezelést, ha az alábbiak valamelyike teljesül.

8.3. Amennyiben az Adatkezelőhöz a GDPR 18. cikk (1) bekezdés a) pontja szerinti érintetti kérelem érkezik, akkor az Adatkezelő utasítására, az abban megjelölt időtartamig az Adatfeldolgozó korlátozza a rendszerben az adatkezelést, így különösen átmenetileg megszünteti valamennyi hozzáférési jogosultságot, kivéve azok esetében, akik az Adatkezelő vagy az Adatfeldolgozó részéről részt vesznek az érintetti kérelem elintézésben.

8.4. Amennyiben az Adatkezelőhöz a GDPR 18. cikk (1) bekezdés b)-d) pontja szerinti érintetti kérelem érkezik, akkor az Adatkezelő utasítására az Adatfeldolgozó az Adatkezelő által biztosított adathordozóra másolja az Adatkezelő utasításában megjelölt személyes adatokat, és azokat az Adatfeldolgozó törli a rendszerében.

8.5. Abban az esetben, ha az Adatfeldolgozó közvetlenül az érintettől kap érintetti joggyakorlással kapcsolatos megkereséseket, az Adatfeldolgozó ezen megkereséseket köteles haladéktalanul továbbítani az Adatkezelőnek és az érintettnek kizárólag Adatkezelő írásos hozzájárulása esetén adhat választ a megkeresésre.

9. Felelősség

9.1. Az Adatfeldolgozó felelősséggel tartozik minden kárért, amely a jelen szerződés szerinti kötelezettségek vagy az Irányadó jog megsértéséből származnak.

9.2. Az Adatfeldolgozó garantálja, hogy megtérít az Adatkezelőnek minden kárt, amely a jelen szerződés szerinti kötelezettségek vagy az Irányadó jog megsértéséből származnak.

Kelt:

Adatkezelő képviselőjében:

Adatfeldolgozó képviselőjében:

.....

<képviselőre jogosult neve>
<képviselőre jogosult titulusa>
Debreceni Egyetem

.....

<képviselőre jogosult neve>
<képviselőre jogosult titulusa>
<cégnév – ha céggel kötjük>

Jogi ellenjegyző:

.....

13. számú melléklet

Adatkezelői Megállapodás

-

(székhely: - a továbbiakban: **Adatkezelő 1.**),
és

-

(székhely: -, a továbbiakban **Adatkezelő 2.**),

(a továbbiakban: együttesen: Felek vagy Adatkezelő) [év, hó, nap] megbízási // vállalkozási // más szerződést kötött egymással. Ezen szerződés alapján a **Felek** közösen végeznek olyan tevékenységet, amely személyes adatok kezelését is magában foglalja, így a Felek közös adatkezelőnek minősülnek.

Az Európai Parlament és a Tanács 2016. április 27-i (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (a továbbiakban: GDPR) számos új kötelezettséget jelent a közös adatkezelők számára, így például a GDPR 26. cikke alapján megállapodást kell kötniük egymással. Erre tekintettel a Felek egymás jogait és kötelezettségeit szabályozó adatkezelői megállapodást kötnek egymással.

1. A GDPR-nak való megfelelés

Felek szavatolják, hogy szakértői szintű ismerettel, megbízhatósággal és erőforrásokkal rendelkeznek ahhoz, hogy a GDPR követelményeinek teljesülését biztosító technikai és szervezési intézkedéseket - ideértve az adatkezelés biztonságát is - végrehajtsák.

2. A közös adatkezelés bemutatása

2.1. A Felek az alábbi adatkezelést végzik közösen:

- a) **az adatkezelés megnevezése:** -
- b) **az adatkezelés célja:** -
- c) **adatkezelés időtartam:** -
- d) **a kezelt adatok köre:** a személyes adatokat Adatkezelő 1. által üzemeltetett szerveren tárolják;

2.2. A 2.1. alponton túlmenően a Felek az alábbi adatkezelést is közösen végzik:

- a) **adatkezelés megnevezése:**
- b) **az adatkezelés célja:**
- c) **adatkezelés időtartam:**
- d) **kezelt adatok köre:** a személyes adatokat Adatkezelő 1. által üzemeltetett szerveren tárolják;

3. Az előzetes tájékoztatással összefüggő kötelezettség teljesítése

3.1. A GDPR 13. vagy 14. cikk szerinti adatkezelési tájékoztató elkészítése Adatkezelő 1. kötelezettsége, azonban az adatkezelési tájékoztató véglegesítése előtt Adatkezelő 2. jóváhagyását be kell szereznie.

3.2. Az adatkezelési tájékoztatót az Adatkezelők kötelesek nyilvánosságra hozni a honlap főoldalán.

4. Az érintetti joggyakorlás teljesítése

4.1. Adatkezelő 1. kötelessége teljesíteni a GDPR 15-22. cikke szerinti érintetti joggyakorlás során érkező kérelmeket.

4.2. Adatkezelő 1. kérelmére Adatkezelő 2. köteles közreműködni az érintetti joggyakorlás teljesítésében

4.3. Az érintett a kérelmét bármelyik Adatkezelő részére elküldheti. Felek kötelesek 3 munkanapon belül továbbítani egymásnak az érintetti kérelmet.

5. Kapcsolattartás rendje

Felek vállalják, hogy a jelen szerződés megkötése napjától számított 1 munkanapon belül tájékoztatják egymást kapcsolattartójuk nevéről, e-mail címéről és telefonszámáról. Felek vállalják, hogy ezen adatok változásáról a változást követő egy munkanapon belül tájékoztatást adnak egymásnak.

6. Adatvédelmi incidens bejelentése

Az adatvédelmi incidenst az észlelő fél haladéktalanul köteles a másik fél felé jelezni, majd közös egyeztetés után a szükséges intézkedést megtenni.

7. Felelősség

7.1. A Felek megállapodnak abban, hogy nem jogosultak olyan költségek megtérítésére, amelyek a másik fél oldalán merülnek fel, és amelyek jelen szerződésből, illetve az uniós vagy tagállami jogszabályokból eredő kötelezettségek teljesítéséből származnak.

7.2. Felek felelősséggel tartoznak egymás irányában minden kárért, amely a jelen szerződés szerinti kötelezettségeik, illetve az uniós vagy tagállami jogszabályok megsértéséből származnak. Felek vállalják, hogy megtérítenek egymásnak minden olyan kárt, amely a jelen szerződés szerinti kötelezettségeik, illetve az uniós vagy tagállami jogszabályok megsértéséből származik.

[Dátum, keltezés]

[Aláírás]

14. számú melléklet

Adattovábbítási nyilvántartás

sorszám	Az adatszolgáltatást teljesítő szervezeti egység megnevezése (adatkezelő)	Személyes adatok továbbításának időpontja/gyakorlatossága, módja	Az adattovábbítás jogalapja	Az adattovábbítás címzettje	A továbbított személyes adatok körének meghatározása	Az érintettek köre	Az adatkezelést előíró jogszabályban meghatározott egyéb adatok (megkereső szerv/személy neve és címe; adatkérés célja/jogalapja /időpontja	Az adattovábbítás során alkalmazott biztonsági intézkedések	Bejegyző neve, bejegyzés dátuma