

MAGYAR TESTNEVELÉSI ÉS SPORTTUDOMÁNYI EGYETEM

Adatvédelmi és adatbiztonsági Szabályzat

A Szenátus elfogadta a 14/2023. (III. 30.) számú határozatával.

2023

Tartalom

Adatvédelmi és adatbiztonsági Szabályzat.....	1
1. Általános rendelkezések.....	3
1.1.A szabályzatban használt rövidítések, fogalmak.....	3
1.2.A Szabályzat szerinti adatkezelő.....	5
1.3. A szabályzat célja.....	5
1.4. A szabályzat hatálya.....	5
2. Az általános adatkezelési szabályok.....	6
2.1. Az adatvédelem, az adatkezelés szervezeti kialakítása.....	6
2.2. A személyes adatok kezelésének alapelvei.....	10
2.2.1. Jogszerűség, tisztességes eljárás és átláthatóság alapelve.....	10
2.2.2. Célhoz kötöttség alapelve.....	11
2.2.3. Adattakarékosság alapelve.....	11
2.2.4. Pontosság alapelve.....	11
2.2.5. Korlátozott tárolhatóság alapelve.....	11
2.2.6.Integritás és bizalmas jelleg alapelve.....	12
2.2.7. Elszámoltathatóság alapelve.....	13
2.3. Adatvédelmi ismeretek oktatása és számonkérése.....	14
2.4. Közös adatkezelés és az adattovábbítás rendje.....	15
2.4.1. Közös adatkezelés.....	15
2.4.2. Az adattovábbítás szabályai.....	15
3. Adatvédelmi eljárásrendek és nyilvántartások.....	17
4. Az érintettek adatvédelmi jogai.....	17
5. Nyilvántartások vezetésének szabályai.....	17
6. Az adatvédelmi incidens.....	18
7. Az adatkezelésért való felelősség.....	18
7.1. Az Egyetem felelőssége.....	18
7.2. Az Egyetem által alkalmazott munkatársak és hallgatók felelőssége.....	18
8. Az adatvédelmi hatásvizsgálat.....	18
8.1. Adatvédelmi hatásvizsgálat végzési kötelezettség.....	18
8.2. Az adatvédelmi hatásvizsgálat elvégzése.....	19
8.3. Az adatvédelmi hatásvizsgálat folyamata.....	20
9. A szabályzat nyilvánossága.....	20
10. Záró rendelkezések.....	20

1. ÁLTALÁNOS RENDELKEZÉSEK

A Magyar Testnevelési és Sporttudományi Egyetem (a továbbiakban: Egyetem/adatkezelő) célja, hogy a tevékenységével összefüggésben felmerülő személyes adatok kezelésével járó folyamatait, eljárásait során biztosítsa a személyes adatok védelmének megfelelő szintjét az Európai Parlament és a Tanács (EU) 2016/679. számú a természetes személyeknek a személyes adatok kezelése az ilyen adatok áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről szóló rendelete (a továbbiakban : a Rendelet), valamint az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) szerint, ezért az alábbi adatvédelmi és adatbiztonsági szabályzatot a továbbiakban: **Szabályzat**) alkotja.

1.1.A szabályzatban használt rövidítések, fogalmak

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

„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;

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

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

„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;

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

„adatkezelő”: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza; ha az adatkezelés céljait és eszközeit az uniós vagy a tagállami jog határozza meg, az adatkezelőt vagy az adatkezelő kijelölésére vonatkozó különös szempontokat az uniós vagy a tagállami jog is meghatározhatja;

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

„címezett”: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, akivel vagy amellyel a személyes adatot közlik, függetlenül attól, hogy harmadik fél-e. Azon közhatalmi szervek, amelyek egy egyedi vizsgálat keretében az uniós vagy a tagállami joggal összhangban férhetnek hozzá személyes adatokhoz, nem minősülnek címezettnek; az említett adatok e közhatalmi szervek általi

kezelése meg kell, hogy feleljen az adatkezelés céljainak megfelelően az alkalmazandó adatvédelmi szabályoknak;

„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;

„az érintett hozzájárulása”: 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;

„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;

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

„biometrikus adat”: egy természetes személy testi, fiziológiai vagy viselkedési jellemzőire vonatkozó minden olyan sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását, ilyen például az arckép vagy a daktiloszkópiai adat;

„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;

„felügyeleti hatóság”: egy tagállam által az 51. cikknek megfelelően létrehozott független közhatalmi szerv, a Magyarországon, a Nemzeti Adatvédelmi És Információszabadság Hatóság;

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

- a) az adatkezelő vagy az adatfeldolgozó az említett felügyeleti hatóság tagállamának területén rendelkezik tevékenységi hellyel;
- b) az adatkezelés jelentős mértékben érinti vagy valószínűsíthetően jelentős mértékben érinti a felügyeleti hatóság tagállamában lakóhellyel rendelkező érintetteket; vagy
- c) panaszt nyújtottak be az említett felügyeleti hatósághoz;

„személyes adatok határokon átnyúló adatkezelése”:

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

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

„nemzetközi szervezet”: a nemzetközi közjog hatálya alá tartozó szervezet vagy annak alárendelt szervei, vagy olyan egyéb szerv, amelyet két vagy több ország közötti megállapodás hozott létre vagy amely ilyen megállapodás alapján jött létre.

„**Rendelet**”: az Európai Parlament és a Tanács (EU) 2016/679. számú a természetes személyeknek a személyes adatok kezelése az ilyen adatok áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről szóló rendelete szerint (a továbbiakban: RENDELET)

„**Infotv**”: az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény.

„**Hatóság**”: a Nemzeti Adatvédelmi és Információszabadság Hatóság.

„**Szabályzat**”: jelen adatvédelmi és adatbiztonsági szabályzat.

„**Egyetem**”: A Magyar Testnevelési és Sporttudományi Egyetem.

A szabályzat további fogalmi megállapítás tekintetében megfelel a Rendelet 4. cikkében, illetve az Infotv. 3. §-ában meghatározottaknak.

1.2.A Szabályzat szerinti adatkezelő

1.2.1. Az Egyetem alapítványi fenntartású felsőoktatási intézmény, jogiszemély, amely a nemzeti felsőoktatási törvényben meghatározott jogosultságai alapján működik.

1.2.2. Adatkezelő adatai:

Adatkezelő megnevezése:	Magyar Testnevelési és Sporttudományi Egyetem
Intézményi azonosító szám:	FI89399
Adatkezelő székhelye:	1123 Budapest, Alkotás u. 42-48.
Adatkezelő postacíme:	1525 Pf. 69.
Adatkezelő elektronikus címe:	info@tf.hu
Adatkezelő képviselője:	Prof. Dr. Sterbenz Tamás rektor
Adatkezelő adatvédelmi tisztviselője:	BookPile Consulting Bt.
Adatvédelmi tisztviselő e-mail címe:	tf-adatvedelem@tf.hu

1.3. A szabályzat célja

1.3.1. Az Egyetem adatvédelmi és adatbiztonsági szabályzatának (a továbbiakban: a Szabályzat) célja, hogy ismertesse a személyes adatok kezelése során érvényesítendő szabályokat és eljárásokat mindazon személyekkel, akik az adatkezelő adatvagyonához hozzáférhetnek, az adatkezelővel munkavégzésre vagy adatfeldolgozásra irányuló jogviszonyban állnak. A Szabályzat meghatározza az adatkezelő által folytatott személyes adatkezelés működésének jogszerű rendjét, valamint biztosítja a Rendelet és az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: az Infotv.) követelményeinek érvényesülését.

1.3.2. Jelen Szabályzat megalkotása a Magyar Testnevelési és Sporttudományi Egyetem, mint adatkezelő által a RENDELET 24. cikk (1) bekezdése szerinti szervezési intézkedésnek tekintendő.

1.4. A szabályzat hatálya

1.4.1. A szabályzat hatálya az Infotv. 2. §-ának megfelelően kiterjed:

- 1) az Egyetemenél foglalkoztatott valamennyi munkavállalóra és a munkavégzésre irányuló egyéb jogviszonyban álló személyekre, (a továbbiakban: munkatársak),
- 2) az Egyetem teljeskörű feladatkörének ellátására, ideértve az Egyetem által létrehozott társulásokat és intézményeket,
- 3) az Egyetemenél nyilvántartott, valamint rendelkezésre álló adatokra, amely természetes személy adataira vonatkozik, vagy közérdekű adatot vagy közérdekből nyilvános adatot tartalmaz, függetlenül attól, hogy az adatkezelés vagy adatfeldolgozás teljesen vagy részben automatizált eszközzel, valamint manuális módon történik,

- 4) az adatfeldolgozási szerződésekben rögzítettek szerint, az adatfeldolgozási szerződést aláírt külső szervezetek mindazon alkalmazottjaira, akik az adatkezelő informatikai rendszereit használják, üzemeltetik, működtetik vagy fejlesztik – azaz mindazon személyekre, akik az adatkezelő adatvagyonához hozzáférhetnek,
- 5) az adatkezelés során felhasznált tárgyi, informatikai eszközökre, függetlenül annak üzemeltetési helyétől,
- 6) a minősített adatok kezelésére vonatkozó jogszabály eltérő rendelkezésének hiányában a minősített adathordozóban szerepeltetett személyes adatok kezelése során.

1.4.2. A szabályzat módosítására az adatkezelő bármely dolgozója javaslatot tehet a rektornak megküldött, de az adatvédelmi tisztviselőnek címzett írásbeli megkeresésben.

- a) A megkeresésnek tartalmaznia kell a dolgozó nevét, aláírását, elérhetőségét, a javasolt módosítást röviden összefoglalva, továbbá a módosítás szükségességét alátámasztó indokokat.
- b) A megkeresés iktatás után kiszignálásra kerül az adatvédelmi tisztviselőhöz, aki megvizsgálja a javasolt módosításokat, elkészíti ajánlását a javasolt módosítás tekintetében.
- c) A megkeresés az ajánlással együtt megküldésre kerül az érintett szakmai vezetőnek, illetve a rektornak, aki jóváhagyja a módosítás előkészítését.
- d) Az adatvédelmi tisztviselő előkészíti a módosítás tervezetét és megküldi az érintett szakmai vezetőnek, a rektornak egyeztetésre.
- e) A módosítási eljárás szabályait a szakmai vezető, illetve a rektor megkeresése alapján indított módosítási eljárás esetében is megfelelően alkalmazni kell.

2. AZ ÁLTALÁNOS ADATKEZELÉSI SZABÁLYOK

2.1. Az adatvédelem, az adatkezelés szervezeti kialakítása

2.1.1. A személyes adatok védelmével kapcsolatos feladat- és szerepkörök:

- a) az elektronikus informatikai rendszerhez kapcsolódó adatok, adatbázisok, illetve adatkezelés esetén az Információ Biztonsági Szabályzatban meghatározott szerepkörök,
- b) a nem elektronikus információrendszerben tárolt, kezelt adatok, adatbázisok, illetve adatkezelés esetén:
 - 1) a rektor,
 - 2) az adatvédelmi tisztviselő,
 - 3) a Rektori Hivatal vezetője,
 - 4) a szervezeti egységek vezetői,
 - 5) az adatkezelő, munkatárs.

2.1.2. A rektor, a nemzeti felsőoktatásról szóló 2011. évi CCIV. törvény 13. § (1) bekezdése értelmében a felsőoktatási intézmény első számú felelős vezetője és képviselője. A rektor a felelős az Egyetem adatkezeléseinek jogszerűségéért. A rektor:

- jóváhagyja a személyes és különleges adatokat tartalmazó, adatszolgáltatási, adattovábbítási, valamint az adatvédelemmel és adatkezeléssel kapcsolatos nyilvántartásokat,
- engedélyezi a nyilvántartási rendszerekhez a hozzáférési jogosultságot,
- szükség esetén gondoskodik az adatvédelmi ismeretek oktatásáról az Egyetem foglalkoztatottjai részére,
- a tudomására jutott visszaállítás esetén utasítja az érintett foglalkoztatottat a jogszerűtlen adatkezelés megszüntetésére, szükség esetén fegyelmi eljárást kezdeményez a foglalkoztatottal szemben,

- felelős a személyes adatok védelméért és az adatkezelő tevékenységére vonatkozó közérdekű adatok nyilvánosságára vonatkozó törvényi előírások érvényesítésért,
- a rektor az adatvédelemmel és az információ szabadsággal kapcsolatos feladatát a közvetlen irányítása alatt álló, Adatvédelmi Tisztviselő (a továbbiakban adatvédelmi tisztviselő) útján látja el. A rektor az Egyetem által kezelt személyes adatok védelmére és az Egyetem tevékenységére vonatkozó közérdekű adatok nyilvánosságára vonatkozó törvényi előírások érvényesítése érdekében feladatai ellátására adatvédelmi tisztviselőt bíz meg.

2.1.3. A rektor feladatai az adatvédelem területén:

- a helyi adatvédelmi, és adatkezeléssel összefüggő belső szabályzatok alapján az adatok összehangolt kezelési rendjének kialakítása és működtetése,
- a személyes adatok védelmével kapcsolatos alapelvek betartása és Egyetemen belül betartatása,
- a személyes adatok kezelésével érintett személyek jogai gyakorlásának elősegítése,
- a hozzá beérkező adatkezeléssel kapcsolatos kérelmek adatvédelmi tisztviselőnek való továbbítása,
- részvétel az adatvédelemmel kapcsolatos kötelező tájékoztatásban,
- az adatvagyon leltár elkészítéséért adott területen felelős személyek kijelölése,
- együttműködés és kapcsolattartás a felügyeleti hatósággal,
- a szabályzatban meghatározott feladatok ellátása.

2.1.4. Az adatvédelmi tisztviselő

- Az adatkezelő folyamatosan biztosítja, hogy az adatvédelmi tisztviselő és az adatvédelem szervezete számára azokat az forrásokat, amelyek e feladatok végrehajtásához, a személyes adatokhoz és az adatkezelési műveletekhez való hozzáféréshez szükséges,
- az adatkezelő biztosítja, hogy az adatvédelmi tisztviselő a feladatai ellátásával kapcsolatban utasításokat senkitől ne fogadjon el,
- az adatvédelmi tisztviselőt feladatai teljesítésével kapcsolatban uniós vagy tagállami jogban meghatározott titoktartási kötelezettség vagy az adatok bizalmas kezelésére vonatkozó kötelezettség köti,
- az adatvédelmi tisztviselő a személyes adatok védelmével, a közérdekű adatok megismerésével és a kötelezően közzéteendő adatok nyilvánosságra hozatalával kapcsolatos szervezési és ellenőrzési feladatokat látja el,
- az adatvédelmi tisztviselő folyamatba építve vizsgálja az Infotv. és a RENDELET végrehajtásával összefüggő kötelezettségek teljesítését, majd a vizsgálat eredményéről az adatvédelmi tisztviselő évente legalább egy alkalommal átfogó jelentést készít a rektor részére,
- tájékoztat és szakmai tanácsot ad az adatkezelő vagy az adatfeldolgozó, továbbá az adatkezelést végző alkalmazottak részére az Infotv. és a RENDELET, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezések szerinti kötelezettségeikkel kapcsolatban, közreműködik, és segítséget nyújt az adatkezeléssel összefüggő döntések meghozatalában, valamint az érintettek jogainak biztosításában,
- kérésre szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomon követi a hatásvizsgálat elvégzését, konkrét ügyekben felmerülő igények alapján adatvédelmi kérdésekben 8 napon belül segítséget nyújt a szervezeti egységek munkatársai részére,
- ellenőrzi e szabályzatnak, valamint az uniós vagy tagállami adatvédelmi rendelkezéseknek, továbbá az adatkezelő vagy az adatfeldolgozó személyes adatok védelmével kapcsolatos belső szabályainak való megfelelést, ideértve a feladatkörök kijelölését, éves munkaterv alapján ellenőrzi az Egyetem szervezeti egységeinél az Infotv. és az adatkezelésre vonatkozó más jogszabályok, valamint a jelen szabályzat és a közérdekű adatok megismerésének, és a kötelezően közzéteendő adatok nyilvánosságra hozatalának rendjéről szóló rendelkezéseinek betartását,
- az ellenőrzésről jegyzőkönyvet készít, hiányosságok esetén 30 napos határidővel intézkedésre hívja fel az érintett szervezeti egység vezetőjét,
- az intézkedés teljesítésének ellenőrzésére 60 napon belül utóellenőrzést végez,

- az intézkedés elmaradása vagy nem megfelelő teljesítése esetén tájékoztatja a rektort és javaslatot tesz intézkedésre,
- javaslatot tesz a rektornak, amennyiben az adatbiztonság érdekében intézkedés meghozatalát látja szükségesnek,
- az érintettek a személyes adataik kezeléséhez és az e rendelet szerinti jogaik gyakorlásához kapcsolódó valamennyi kérdésben az adatvédelmi tisztviselőhöz fordulhatnak, kivizsgálja és intézi a hozzá érkező bejelentéseket, a bejelentések kivizsgálására, az Infotv. VI. fejezetében foglaltakat kell megfelelő eltéréssel alkalmazni,
- elkészíti és évente, a tárgyévet követő év január 31. napjáig felülvizsgálja az adatvédelmi szabályzatot, jogszabályváltozás miatt vagy más fontos okból gondoskodik annak módosításáról, kiegészítéséről,
- éves ellenőrzési ütemterv alapján ellenőrzi a kezelt adatok nyilvántartásáról és védelméről, a közérdekű adatok nyilvánosságáról szóló jogszabályok végrehajtását,
- a közérdekű adatok nyilvánosságával kapcsolatban szükség szerint közreműködik ezen adatok megismerése iránti kérelmek teljesítésében,
- koordinálja az adatvédelmi tevékenységet segítő nyilvántartási rendszer kialakítását, módosításait,
- a szervezeti egységek munkatársai részére adatvédelmi oktatást, ismeretmegújítást tart, az adatvédelmi oktatással kapcsolatos feladatokat oktatási ütemterv alapján végzi,
- együttműködik a felügyeleti hatósággal; az adatkezeléssel összefüggő ügyekben – ideértve az előzetes konzultációt is – kapcsolattartó pontként szolgál a felügyeleti hatóság felé, valamint adott esetben bármely egyéb kérdésben konzultációt folytat vele;
- vezeti az adatvédelmi nyilvántartást,
- szervezi az adatkezelési műveletekben résztvevő személyzet tudatosság növelését és képzését, valamint a kapcsolódó auditokat is.

2.1.5. A Rektori Hivatal vezetője

- mint az Egyetem adatkezelésért felelős munkatársa koordinálja az adatkezelő szervezeti egységei és az adatvédelmi tisztviselő közötti kapcsolattartást, munkavégzése során segíti és támogatja az adatvédelmi tisztviselő munkavégzését,
- konkrét ügyekben felmerülő adatvédelmi kérdésekben segítséget nyújt a vezetők és az adatkezelők részére az adatvédelmi tisztviselő bevonásával,
- közreműködik, és segítséget nyújt az adatkezeléssel összefüggő döntések meghozatalában, valamint az érintettek jogainak biztosításában,
- a közérdekű adatok nyilvánosságával kapcsolatban koordinálja a közérdekű adatok közzétételéhez szükséges adatok megküldését,
- a közérdekű adatok nyilvánosságával kapcsolatban szükség szerint közreműködik ezen adatok megismerése iránti kérelmek teljesítésében,
- koordinálja az adatvédelmi tevékenységet segítő nyilvántartások kialakítását, módosításait,
- vezeti az adatvédelmi nyilvántartásokat és összesíti, majd a kitűzött határidőre továbbítja az adatvédelmi tisztviselőnek.

2.1.6. A szervezeti egység vezető

- köteles a Szabályzatban foglaltakat megismerni, munkája során alkalmazni, valamint gondoskodni arról, hogy azt a szervezeti egységének foglalkoztatottjai megismerjék, előírásait munkavégzésük során alkalmazzák,
- konkrét ügyekben felmerülő adatvédelmi kérdésekben segítséget nyújt az adatkezelők részére,
- javaslatot tehet a rektornak a Szabályzat módosítására, kiegészítésére,
- a hozzá érkező adatkezeléssel kapcsolatos panaszokat kivizsgálja, a kivizsgálásról feljegyzést készít, melyet továbbít a rektori hivatalvezető részére,
- a tudomására jutott visszaállásról tájékoztatja a Rektori Hivatalt.

Az Egyetem elsődleges adatkezelő szervezeti egységei:

- a) Rektori Hivatal;
- b) Campus Főigazgatóság;
- c) Gazdasági Főigazgatóság;
- d) intézetek, tanszékek, kutató központok, központok, Sportszaknyelvi Lektorátus, csoportok;
- e) Jogi Igazgatóság;
- f) Nemzetközi Kapcsolatok Igazgatósága;
- g) Műszaki és Ellátási Igazgatóság;
- h) Oktatási Igazgatóság;
- i) Pénzügyi és Számviteli Igazgatóság;
- j) Pályázati és Innovációs Központ;
- k) Sportvizsgaközpont;
- l) Technológia- és tudástranzfer Központ;
- m) Továbbképző Központ;
- n) Könyvtár és Levéltár;
- o) Tanulmányi Hivatal;
- p) Beszerzési és Közbeszerzési Osztály;
- q) HR Osztály;
- r) Kommunikációs és Rendezvényszervezési Osztály;
- s) Minőségbiztosítási és Akkreditációs Iroda;
- t) Beruházási Programiroda;
- u) Sport Iroda;
- v) Tudományos Iroda;
- w) Doktori Iskola;
- x) kollégium, szakkollégium;
- y) Hallgatói Önkormányzat,
- z) a Szenátus által létrehozott bizottságok;
- aa) az Egyetem fenntartásában működő köznevelési intézmény.

2.1.7. Az adatkezelő (munkatárs)

- köteles az adatvédelemmel kapcsolatos jogszabályokat és a Szabályzatot megismerni és maradéktalanul betartani,
- köteles tájékoztatni közvetlen felettesét, szükség esetén a rektort, a feladatkörében felmerült bármely adatvédelmi problémáról, észrevételeiről, a számítástechnikai eszközök bármilyen meghibásodásáról, az adatállomány kezelhetőségében bekövetkezett problémáról, jogosulatlan hozzáférésről,
- köteles a tudomására jutott, az adatkezeléssel kapcsolatosan feltárt visszásságot haladéktalanul megszüntetni,
- vezeti a munkakörébe tartozó adat-, adatszolgáltatási és adattovábbítási nyilvántartást,
- gondoskodik arról, hogy az általa vezetett nyilvántartás adataihoz illetéktelen személy ne férhessen hozzá, ügyel a nyilvántartás biztonságos tárolására,
- elvégzi a kezelésében lévő adatok biztonsági mentését, gondoskodik azok biztonságos tárolásáról,
- a jogszabály által felhatalmazott személynek vagy szervezetnek adatot szolgáltat, adatot továbbít,
- fegyelmi és kártérítési felelősséggel tartozik azért, hogy tevékenységét az adatkezelésre és az adatok védelemére vonatkozó jogszabályoknak, valamint a Szabályzatnak, az adatkezelést elrendelő jogszabály hiányában pedig az érintett hozzájárulásának megfelelően végezze
- kötelezettsége, hogy az 1. 2. f) pont szerinti éves adatvédelmi jelentéshez vezetője útján adatot szolgáltatson.
- kötelezettsége, hogy részt vegyen az adatvédelmi oktatáson.

2.1.9. Kiemelt szakmai együttműködés szükséges az adatvédelmi tisztviselő, és az információbiztonsággal összefüggő feladatkört ellátók között.

2.1.10. Az adatvédelemmel érintett munkakört ellátóknak a tevékenységük során folyamatos tájékoztatási, együttműködési és tevékenység harmonizációs kötelezettségük van.

2.2. A személyes adatok kezelésének alapelvei

2.2.1. Jogszerűség, tisztességes eljárás és átláthatóság alapelve

2.2.1.1. A személyes adatok kezelését jogszerűen és tisztességesen, az érintett számára átlátható módon kell végezni. A személyes adatok kezelésekor a természetes személyek számára átláthatóvá kell tenni a rájuk vonatkozó személyes adataik gyűjtésének és felhasználásának módját, mikéntjét, az adatok kezelésének mértékét, továbbá az azokba való betekintés lehetőségét és módját. Az átláthatóság elve megköveteli, hogy a személyes adatok kezelésével összefüggő tájékoztatás, illetve kommunikáció könnyen hozzáférhető és közérthető legyen, valamint, hogy azt világosan és egyszerű nyelvezettel fogalmazzák meg.

2.2.1.2. Az érintettel az adat felvétele előtt közölni kell az adatkezelés célját, és az adatszolgáltatás önkéntes vagy kötelező jellegét. Kötelező adatszolgáltatás esetén meg kell jelölni az adatkezelést elrendelő jogszabályt, illetve az elrendelést megállapító jogszabályi rendelkezés jogszabályhely szerinti megjelölését.

2.2.1.3. A hozzájáruláson alapuló adatkezeléséhez az érintett hozzájárulását kell kikérni, kivéve, ha hozzájárulását, különleges adatát írásbeli beadványban maga az érintett közölte. Különleges adatot az érintett kifejezett és írásos hozzájárulása szerint szabad felvenni. Különleges adatok kezelésével járó ügyekben – a jogszabályokban és jelen szabályzatban foglaltakon túl is – fokozott gondossággal kell eljárni.

2.2.1.4. Személyes adat kezelésének minősül az érintettől készített fotó, videofelvétel abban az esetben is, ha a fotón, videofelvételen nem szerepel az érintett neve vagy más adata. Személyes adatkezelésnek minősül a felvétel elkészítése abban az esetben is, ha az felhasználásra nem kerül. Az ilyen adatkezelés csak hozzájáruláson alapulhat.

2.2.1.5. A hozzájárulás beszerzéséért a szervezeti egység vezetője felelős. Amennyiben az adat nem az érintettől származik, csak akkor kezelhető, ha az adat közlője az adatkezelő rendelkezésére bocsátja az érintett felhasználási célra vonatkozó hozzájárulását. Személyes adat közzétételéhez az adatkezelőnek rendelkeznie kell az érintettnek a közzétételre való hozzájárulásával is. A hozzájárulást a felvételek elkészítése előtt kell beszerezni. A rendezvényeken való felvételkészítés során, a rendezvényeken résztvevőket előzetesen – a meghívón vagy a rendezvényen való adatkezelési tájékoztató tábla elhelyezésével – a felvétel készítéséről és annak felhasználásáról tájékoztatni kell. Az adatkezelési tájékoztatás megtörténtéről jegyzőkönyvet kell felvenni.

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

- a) az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez;
- b) az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél, vagy az a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges;
- c) az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges;
- d) az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges;
- e) az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges;
- f) az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető

jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé, különösen, ha az érintett gyermek.

Az f) pont nem alkalmazható a közhatalmi szervek által feladataik ellátása során végzett adatkezelésre. (Rendelet 6. cikk (1).)

2.2.1.7. Személyes adat kezelhető akkor is, ha az érintett hozzájárulásának beszerzése lehetetlen vagy aránytalan költségekkel járna, és a személyes adat kezelése az adatkezelőre vonatkozó jogi kötelezettség teljesítése céljából szükséges, vagy az adatkezelő vagy harmadik személy jogos érdekének érvényesítése céljából szükséges, és ezen érdek érvényesítése céljából szükséges, és ezen érdek érvényesítése a személyes adatok védelméhez fűződő jog korlátozásával arányban áll. (Infotv. 6. § (1) bekezdés)

2.2.2. Célhoz kötöttség alapelve

2.2.2.1. A személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történhet. A személyes adatok nem kezelhetők ezekkel a célokkal össze nem egyeztethető módon. 2.2.2.2. Az ügyintézés során csak azokat a személyes, vagy különleges adatokat szabad felvenni és kezelni, amelyek az ügy szempontjából feltétlenül szükségesek, és amelyeknek a célhoz kötöttsége igazolható. A felvett adatokat csak az adott ügy intézése érdekében szabad felhasználni, más eljárásokkal és adatokkal – törvény eltérő rendelkezése hiányában – nem kapcsolhatók össze.

2.2.3. Adattakarékosság alapelve

2.2.3.1. A személyes adatoknak az adatkezelés céljai szempontjából megfelelőnek és relevánsnak kell lenniük, valamint csak a szükséges adatra szabad korlátozódniuk.

2.2.4. Pontosság alapelve

2.2.4.1. A személyes adatoknak pontosnak és szükség esetén naprakésznek kell lenniük, azaz minden észszerű intézkedést meg kell tenni annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul töröljék vagy helyesbítsék.

2.2.4.2. Az adatminőség biztosítása céljából személyes adatot csak az érintett személyének azonosítására alkalmas és érvényes hatósági igazolványból szabad felvenni. Az adatfelvétel és a további adatkezelés folyamán ügyelni kell a személyes adatok pontosságára, teljességére és időszerűségére, hogy emiatt az érintettek jogai ne sérülhessenek.

2.2.5. Korlátozott tárolhatóság alapelve

2.2.5.1. A személyes adatok tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé; a személyes adatok ennél hosszabb ideig történő tárolására csak akkor kerülhet sor, amennyiben a személyes adatok kezelése ezt követően is igazolhatóan szükséges.

2.2.5.2. Annak biztosítása érdekében, hogy a személyes adatok tárolása a szükséges időtartamra korlátozódjon, az adatkezelő minden adatkezelése tekintetében adattörlési határidőt állapít meg az iratkezelési szabályzatában, ezt a határidőt pedig az adatkezelési nyilvántartásában felvezeti.

2.2.5.3. A célhoz már nem kötődő és olyan adatokat, amelyekre nézve az adatkezelés célja megszűnt vagy módosult – az iratkezelési szabályzatban foglaltakkal összhangban – haladéktalanul, vagy az előírt megőrzési határidő leteltével meg kell semmisíteni. A személyes adatokat tartalmazó egyéb iratanyagok megsemmisítéséről szintén a szükséges biztonsági intézkedések mellett kell gondoskodni. A számítógépen rögzített adatokat, amennyiben céljukat betöltötték – további felhasználásuk megakadályozása érdekében – felismerhetetlenné kell tenni.

2.2.5.4. A személyes adatok akkor továbbíthatóak, valamint a különböző adatkezelések akkor kapcsolhatók össze, ha az érintett ahhoz hozzájárult, vagy törvény azt megengedi, és ha az adatkezelés feltételei minden egyes személyes adatra nézve teljesülnek. Személyes adat (beleértve a különleges adatot is) az országból – adathordozótól vagy adatátvitel módjától függetlenül - harmadik országban lévő

adatkezelő vagy adatfeldolgozó részére akkor továbbítható, ha az Infotv 10.§-ában foglalt feltételek teljesülnek.

2.2.5.5. A hatósági ügyek során hozott iratok nem tartalmazhatják az értesítendő személyek nevét és címét. Annak érdekében, hogy a kézbesítés ellenőrizhető legyen, a köztisztviselő köteles az irattári példányon rögzíteni az értesítendőkhöz jegyzékét, arról tájékoztatást adni azonban csak a vonatkozó jogszabályok és jelen szabályzat figyelembevételével lehet.

2.2.6. Integritás és bizalmas jelleg alapelve

2.2.6.1. A személyes adatok kezelését oly módon kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve.

2.2.6.2. Az ügyiratba nem kerülő, papíralapú feljegyzésben rögzített, személyes és különleges adatokat – további felhasználásuk megakadályozása érdekében – azonosításra alkalmatlanná kell tenni vagy azonnal törölni kell.

2.2.6.3. A számítástechnikai eljárás során keletkezett munkapéldánnyal, illetőleg rontott vagy egyéb okból feleslegessé vált példányokkal a 2.2.6.2. pont szerint kell eljárni.

2.2.6.4. Az ügyintézőnél vagy az irattárban lévő iratba az ügyintézőn kívül más személy csak akkor tekinthet be, amennyiben ezt törvény lehetővé, vagy az adatkezelői tevékenységével összefüggő feladatellátás szükségessé teszi.

2.2.6.5. Az érintett vagy képviselője betekintési jogának gyakorlása során úgy kell eljárni, hogy ezáltal mások jogai ne sérülhessenek (a más személyre vonatkozó személyes, vagy védett adatokat adott esetben ki kell takarni vagy más módon felismerhetetlenné tenni). Ugyanígy kell eljárni a másolat, kivonat készítésekor is.

2.2.6.6. Az adatvédelmi tisztviselő különösen az adatvédelmi feladatok végrehajtásának ellenőrzése során, e feladatához kötődően és szükséges körben, jogosult az adatkezelő által kezelt valamennyi adat – ideértve valamennyi személyes adat, minősített adat, vagy üzleti titok – megismerésére.

2.2.6.7. Az egyéb szempontokon túl adatvédelmi megfontolásból azokat a helyiségeket, ahol közös használatú nyomtató vagy másológép üzemel, az adatbiztonsági követelmények figyelembevételével kell használni.

2.2.6.8. Az egyéb szempontokon túl adatvédelmi megfontolásból azokat a szobákat, helyiségeket, ahol számítógép, munkaállomás üzemel, úgy kell használni, hogy az megfeleljen az adatvédelmi, tűzrendészeti és informatikai biztonsági követelményeknek. Az ügyintéző köteles a számítógépet és az ahhoz alkalmazott adathordozókat úgy kezelni, tárolni, hogy a védelmet igénylő adatokat illetéktelen személy ne ismerhesse meg.

2.2.6.9. Személyes adatokat is tartalmazó iratot az adatkezelő hivatalos helyiségéből kivinni – munkaköri feladat ellátásának kivételével – csak a közvetlen felettes vezető engedélyével lehet. Az ügyintéző ez esetben is köteles gondoskodni arról, hogy az ne vesszen el, ne rongálódjon vagy semmisüljön meg, és tartalma illetéktelen személy tudomására ne jusson.

2.2.6.10. Az iratok telefaxon, az adatok telefonon, és egyéb elektronikus úton csak kellő körültekintéssel és kizárólag az adatkezelő technikai eszközeinek igénybevételével továbbíthatók.

2.2.6.11. Az adatkezelő adatfeldolgozó igénybevétele esetén gondoskodik arról, hogy a kiválasztott adatfeldolgozó a személyes adatok védelme érdekében megtegye a szükséges intézkedéseket, valamint kövesse Az adatkezelő szabályzatait és egyedi utasításait. A kiválasztás során az adatkezelő törekszik arra, hogy csakis olyan adatfeldolgozó kerüljön igénybevétele, amely megfelelő garanciákat nyújt – különösen szakértelem, megbízhatóság és erőforrások tekintetében – arra vonatkozóan, hogy az

adatvédelmi követelmények teljesülését biztosító technikai és szervezési intézkedéseket végrehajtja, ideértve az adatkezelés biztonságát is.

2.2.6.12. A szabályzat hatálybalépését követően kötött adatfeldolgozói szerződésekben legalább a Rendelet 28. cikkében rögzített feltételekről rendelkezni szükséges.

2.2.7. Elszámoltathatóság *alapelve*

2.2.7.1. Az adatkezelő az adatkezeléssel kapcsolatos valamennyi iratát a tanúsított iktatási rendszerben iktatja, helyreállítható formátumban. Az egyes adatkezeléssel kapcsolatos iratokat a szervezeti egységek őrzik papír alapú és elektronikus dokumentumban.

2.2.7.2. A személyes adatok védelméért, az adatkezelés jogszerűségéért az adatkezelő szervezeti egységek vezetői és az adatkezelést végző munkatársak felelősek. Az adatkezelő által kezelt személyes adatok védelméről, az adatvédelemmel kapcsolatos szabályok, foglalkoztatottak általi megismeréséről és betartásáról az adatkezelő szervezeti egységek vezetői gondoskodnak. Az egyes nyilvántartások, adatkezelések tekintetében a hozzáférési jogosultságot a szervezeti egység vezetőjének személyre, munkaköri feladatra lebontottan meg kell határoznia és az időszerű állapotnak megfelelő nyilvántartásokról gondoskodnia kell. E jogosultságokat a munkaköri leírásokban meg kell jeleníteni.

2.2.7.3. A 2.2.7.1. pontban szereplő adatokról a szervezeti egységeknek a nyilvántartás leíró adataival adatleltárt kell vezetnie. Az adatleltár leíró adatait, a felvételt követő 8 napon belül, az adatvédelmi tisztviselőnek meg kell küldeni.

2.2.7.4. Az e szabályzat által előírt nyilvántartásokat és dokumentumokat (adatleltárt, adatkezelési nyilvántartást, adatkezelési tájékoztatókat, adattovábbítási nyilvántartást, adatszolgáltatási nyilvántartást az érintetti jogok gyakorlásának nyilvántartását, a felülvizsgálati jegyzőkönyveket és azok nyilvántartását) a szervezeti egységek vezetik az adatvédelmi tisztviselő közreműködésével. A dokumentumok elkészítéséért és a nyilvántartások vezetéséért, annak teljes körűségéért, az abban feltüntetett adatok valóságáért és naprakészségéért a szervezeti egység vezetője felelős.

2.2.7.5. Az adatkezelő adatleltárát – a szervezeti egységek adatleltára alapján – az adatvédelmi tisztviselő vezeti.

2.2.7.6. A személyes adatokat továbbítani, vagy adatszolgáltatást teljesíteni, és a különböző adatkezeléseket összekapcsolni csak akkor lehet, amennyiben ahhoz az érintett hozzájárult, vagy törvény ezt előírja, vagy megengedi és az adatkezelés feltételei minden egyes személyes adatra nézve teljesülnek. A harmadik országba történő adattovábbítás esetén az Infotv. 8. §-nak valamint a RENDELET V. fejezetének rendelkezéseit kell alapul venni.

2.2.7.7. Az adattovábbítást teljes adattartalomra kiterjedően regisztrálni (naplózni) kell (adattovábbítási nyilvántartás), annak érdekében, hogy megállapítható legyen, milyen adat, kinek, milyen felhatalmazás alapján, mikor került továbbításra vagy kiszolgáltatásra (pl. belföldi jogsegély).

2.2.7.8. Amennyiben a szervezeti egység vonatkozásában a szakmai irányító szerv az előző pontban foglaltakhoz képest tágabb körben határozta meg a vonatkozó nyilvántartás kötelezően vezetendő adattartalmát, úgy a nyilvántartást a szakmai irányító szerv által meghatározottak szerint kell vezetni.

2.2.7.9. A 2.2.7.7. - 2.2.7.8. pontok szerinti nyilvántartást szervezeti egységenként kell vezetni. A nyilvántartás egy másolati példányát – a tárgyévet követő év január 15. napjáig – az adatvédelmi tisztviselő részére át kell adni. Az Infotv. értelmében az adattovábbításról vezetett nyilvántartást – eltérő jogszabályi rendelkezés hiányában – személyes adatok esetében minimum 5 évig, különleges adatok vonatkozásában pedig minimum 20 évig kell megőrizni.

2.2.7.11. Az adattovábbítás feltételeit – kétség esetén – szervezeti egység vezetője mérlegeli és bírálja el, az általa továbbított adatokért az érintettel szemben felelősséggel tartozik.

2.2.7.12. Amennyiben az adattovábbítást nem lehet jogszerűen teljesíteni, vagy az igény elbírálásához szükséges információkat az igénylő a felkérést követően sem jelölte meg, az adattovábbítást meg kell tagadni.

2.2.7.13. Az adattovábbítás megtagadásáról – annak indokolásával együtt – írásban kell értesíteni az igénylőt.

2.2.7.14. A 2.2.7.8-2.2.7.13. pontok rendelkezéseit nem kell alkalmazni az összesített, és a statisztikai adatokra vonatkozó adatkérés esetén, amennyiben az adatfeldolgozás eredményeként az adatok elvesztik egyedi jellegüket.

2.2.7.15. Az érintettet a kérelmére indult eljárásban az adattovábbításra vonatkozó törvényi felhatalmazás hiányában nyilatkoztatni kell – különleges adatai tekintetében írásban és kifejezetten –, hogy hozzájárul-e személyes adatainak továbbításához, amennyiben ügye elintézéséhez más szerv megkeresése szükséges.

2.2.7.16. Amennyiben az érintett nem járul hozzá az adatai más szerv részére történő továbbításához, tájékoztatni kell arról, hogy kérelme ez esetben nem teljesíthető.

2.2.7.17. Az érintettet a Rendelet 12. cikk és az Infotv. 14. §-a szerint megilleti az a jog, hogy személyes adatai kezeléséről tájékoztatást kérjen, továbbá kérheti személyes adatainak helyesbítését, vagy – a kötelező adatkezelés kivételével – azok törlését vagy zárolását. Az adatkezelésről szóló tájékoztatásra vonatkozó kérelmeket – a jogszabályi feltételek fennállása esetén – az Infotv. alapján legfeljebb 25 napon belül, lehetőség szerint azonban soron kívül teljesíteni kell. Az elutasított kérelmekről az Egyetem adatvédelmi tisztviselőjét közvetlenül tájékoztatni kell.

2.3. Adatvédelmi ismeretek oktatása és számonkérése

2.3.1. Az adatkezelő állományába újonnan került személyeket az adatvédelmi tisztviselő - az adatkezelő személyzeti feladatot ellátó szervezeti egységének tájékoztatása alapján - köteles az állományba vételt követő két hónapon belül adatvédelmi oktatásban részesíteni. Az oktatásra kötelezett részére a szükséges jogszabályokat, közjogi szervezetszabályozó eszközöket, belső normákat és egyéb segédanyagokat rendelkezésre kell bocsátani, vagy ezek tekintetében az elektronikus hozzáférés lehetőségét és módját ismertetni kell.

2.3.2. Az oktatást követően 30 napon belül az adatkezelőnél foglalkoztatottaknak az adatvédelmi ismeretekből vizsgát kell tenni, amelyről szóló igazolást az érintett személyi anyagában kell elhelyezni. adatkezelőnél foglalkoztatottak szükség szerint évente, de legalább két évente részt kell venniük az adatvédelmi tisztviselő által szervezett adatvédelmi oktatáson vagy tájékoztatón, melyet aláírásukkal kell igazolniuk.

2.3.3. Az adatvédelmi tisztviselő az adatkezelő személyes adatok kezelését végző munkavállalóinak a bekövetkezett adatvédelmi tárgyú jogszabály- és normaváltozásokról köteles tájékoztatást adni, indokolt esetben - különösen a jelentősebb adatvédelmi tárgyú normaváltozásoknál vagy az ellenőrzés során feltárt visszatérő, vagy egyébként súlyos hiányosságoknál és súlyos adatvédelmi incidenst követően - az érintett szervezeti egységnél adatvédelmi oktatás tartani.

2.3.4. Az adatvédelmi tisztviselő rendkívüli oktatást tart az alábbi esetekben:

- a) adatvédelmi incidens megtörténte
- b) a Hatóság eljárása az Egyetemmel szemben
- c) adatvédelmi figyelmeztetés vagy bírság kiszabása bármely magyarországi felsőoktatási intézménnyel szemben.

2.4. Közös adatkezelés és az adattovábbítás rendje

2.4.1. Közös adatkezelés

2.4.1.1. Amennyiben az Egyetem a feladatkörébe tartozó adatkezelés céljait és eszközeit más adatkezelővel közösen határozza meg (a továbbiakban együttesen: „közös adatkezelők”), úgy az közös adatkezelésnek minősül. A közös adatkezelők a közös adatkezelés megkezdése előtt megállapodást kötnek, amelyben meghatározzák az adatvédelmi jogszabályok által előírt kötelezettségek teljesítéséért fennálló, feladataikkal összefüggő felelősségük megosztását, kivéve, ha a felelősség megosztása jogszabályban rendezett.

2.4.1.2. A megállapodásban rögzítik a közös adatkezelőknek az érintettekkel szembeni kötelezettségeit és feladatait, valamint a velük való kapcsolattartás módját. A közös adatkezelésre vonatkozó legfontosabb szempontokról az érintettet a megállapodásban foglaltak szerint tájékoztatják.

2.4.1.3. Az érintett mindegyik adatkezelő vonatkozásában és mindegyik adatkezelővel szemben gyakorolhatja az e rendelet szerinti jogait. A jogok biztosítása kapcsán a közös adatkezelők együttműködni kötelesek.

2.4.2. Az adattovábbítás szabályai

2.4.2.1. Adattovábbításnak minősül a személyes adat meghatározott harmadik személy számára történő hozzáférhetővé tétele. A harmadik személy az Egyetemen, az érintetten és az esetlegesen igénybe vett adatfeldolgozón kívül minden más személy és szervezet, aki önálló adatkezelőnek minősül és nem állnak fenn az adatkezelés tekintetében a közös adatkezelés feltételei

2.4.2.2. Az Egyetem ellenőrzi a kezelésében lévő személyes adat továbbítását megelőzően, hogy az adattovábbítás feltételei az adott személyes adat tekintetében fennállnak-e, így különösen, hogy az igényelt adat tekintetében adatkezelőnek minősül-e, hogy az adat továbbításra rendelkezik-e megfelelő joggal továbbá, hogy az a célhoz kötöttség elvének az adattovábbítás megfelel-e.

2.4.2.3. Az adattovábbítás feltételei fennállásának ellenőrzése az adattovábbítást végző foglalkoztatott kötelessége. Az adatfeldolgozásra irányuló adatátadás a fentiek értelmében nem minősül adattovábbításnak

2.4.2.4. A harmadik személy vagy szerv által benyújtott adattovábbítási kérelem elbírálása – a törvényben kötelezően előírt adattovábbítás esetét kivéve – a rektor hatáskörébe tartozik. Az adattovábbítási kérelem abban az esetben teljesíthető, ha az tartalmazza:

- a) az adattovábbítást kérő minden kétséget kizáró azonosításához szükséges adatokat;
- b) az adattovábbítás célját, jogalapját (az alapul szolgáló törvényi rendelkezés pontos megjelölését);
- c) a kért adatok körének pontos meghatározását;

az érintett személy azonosításához szükséges adatokat.

2.4.2.5. Az adattovábbítás történhet kérelem alapján egyedi adatszolgáltatással, illetőleg - törvény ilyen tartalmú rendelkezése vagy erre vonatkozó megállapodás alapján - közvetlen hozzáférés biztosításával.

2.4.3. Adattovábbítás szabályai harmadik országba

2.4.3.1. Olyan személyes adatok továbbítására – ideértve a személyes adatok harmadik országból egy további harmadik országba történő újbóli továbbítását is –, amelyeket harmadik országba vagy nemzetközi szervezet részére történő továbbításukat követően adatkezelésnek vetnek alá vagy szándékoznak alávetni, csak abban az esetben kerülhet sor, ha az Egyetem teljesíti – többek között – a Rendelet V. fejezetében rögzített alábbi feltételeket.

2.4.3.2. Adattovábbítás megfelelőségi határozat alapján: Az Egyetem elsőként azt vizsgálja meg, hogy az Európai Bizottság hozott-e megfelelőségi határozatot az adott ország vonatkozásában. Személyes adatok harmadik országba történő továbbítására további engedély beszerzése nélkül sor kerülhet, ha a Bizottság

megállapította, hogy a harmadik ország, a harmadik ország valamely területe, illetve egy, vagy több meghatározott ágazata megfelelő védelmi szintet biztosít.

2.4.3.3. Adattovábbítás megfelelő garanciák mellett: Amennyiben nincs megfelelőségi határozat, az adatok továbbíthatók, ha megfelelő garanciákat nyújt az Egyetem és az érintettek számára érvényesíthető jogok és hatékony jogorvoslati lehetőségek állnak rendelkezésre.

2.4.3.4. A felügyeleti hatóság külön engedélye nélkül megfelelő garanciákat az alábbiak jelenthetik:

- a) közhatalmi vagy egyéb, közfeladatot ellátó szervek közötti, jogilag kötelező erejű, kikényszeríthető jogi eszköz;
- b) kötelező erejű vállalati szabályok;
- c) vizsgálóbizottsági eljárással összhangban elfogadott általános adatvédelmi kikötések;
- d) jóváhagyott magatartási kódex a harmadik országbeli adatkezelő vagy adatfeldolgozó arra vonatkozó, kötelező erejű és kikényszeríthető kötelezettségvállalásával együtt, hogy alkalmazza a megfelelő – ideértve az érintettek jogaira vonatkozó – garanciákat;
- e) jóváhagyott tanúsítási mechanizmus a harmadik országbeli adatkezelő vagy adatfeldolgozó arra vonatkozó, kötelező erejű és kikényszeríthető kötelezettségvállalásával együtt, hogy alkalmazza a megfelelő garanciákat, ideértve az érintettek jogait illetően is.

2.4.3.5. Az Egyetem a fenti c) pont szerinti esetben mind adatkezelő-adatkezelő közötti, mind pedig adatkezelő-adatfeldolgozó közötti adattovábbítás esetén az Európai Unió illetékes szerve által meghatározott modellszerződések valamelyikének használatával továbbít személyes adatot.

2.4.3.6. Vállalkozáscsoporton vagy a közös gazdasági tevékenységet folytató vállalkozások ugyanazon csoportján belüli szervezetekhez irányuló nemzetközi adattovábbítások során lehetőség van a hatóság által jóváhagyott kötelező erejű vállalati szabályok alkalmazására, mely a fenti b) pont szerint megfelelő garanciát jelent az adattovábbításhoz.

2.4.3.7. A felügyeleti hatóság engedélyével megfelelő garanciákként különösen az alábbiak is szolgálhatnak:

- a) az adatkezelő vagy adatfeldolgozó és a harmadik országbeli vagy a nemzetközi szervezeten belüli adatkezelő, adatfeldolgozó vagy a személyes adatok címzettje között létrejött szerződéses rendelkezések; vagy
- b) közhatalmi vagy egyéb, közfeladatot ellátó szervek között létrejött, közigazgatási megállapodásba beillesztendő rendelkezések, köztük az érintettek érvényesíthető és tényleges jogaira vonatkozó rendelkezések.

2.4.3.8. Különös helyzetben biztosított eltérések: Megfelelőségi határozat, illetve megfelelő garanciák hiányában a személyes adatok harmadik ország vagy nemzetközi szervezet részére történő továbbítására, vagy többszöri továbbítására csak az alábbi feltételek legalább egyikének teljesülése esetén kerülhet sor:

- a) az érintett kifejezetten hozzájárulását adta a tervezett továbbításhoz azt követően, hogy tájékoztatták az adattovábbításból eredő – a megfelelőségi határozat és a megfelelő garanciák hiányából fakadó – esetleges kockázatokról;
- b) az adattovábbítás az érintett és az adatkezelő közötti szerződés teljesítéséhez, vagy az érintett kérésére hozott, szerződést megelőző intézkedések végrehajtásához szükséges;
- c) az adattovábbítás az adatkezelő 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.

3. ADATVÉDELMI ELJÁRÁSRENDEK ÉS NYILVÁNTARTÁSOK

3.1. Az Egyetem az alábbi adatvédelmi és adatbiztonsági eljárásrendeket és nyilvántartásokat vezeti.

Eljárásrendek:

- a) érintetti kérelem teljesítésére vonatkozó belső eljárásrend;
- b) adatvédelmi incidens bekövetkezése esetén követendő belső eljárásrend;
- c) adatvédelmi nyilvántartások elkészítésére vonatkozó belső eljárásrend.

Nyilvántartások:

- a) adatvagyon-leltár
- b) adatkezelések nyilvántartása
- c) az adatfeldolgozói nyilvántartása
- d) az adatfeldolgozóként végzett adatkezelésekről a nyilvántartása
- e) az érintettektől érkezett kérelmekről a nyilvántartás
- f) az adattovábbítások nyilvántartása
- g) az adatkezelési tájékoztatók nyilvántartása
- h) az adatvédelmi incidensek nyilvántartása.

4. AZ ÉRINTETTEK ADATVÉDELMI JOGAI

4.1. RENDELET 15-21. cikkei szerint az érintett a következő jogérvényesítési lehetőségekkel élhet az adatkezelővel szemben:

- az érintettek tájékoztatáshoz való joga
- az érintett hozzáféréshez való joga
- az érintett helyesbítéshez való joga
- az érintett törléshez való joga („az elfeledtetéshez való jog”)
- az adatkezelés korlátozásához való jog
- a tiltakozáshoz való jog
- az adatok hordozhatóságához való jog
- az egyedi ügyekben alkalmazott automatizált döntéshozatalról való döntés joga
- jogorvoslathoz való jog.

4.2. Az érintetteket megillető jogok és a jogok érvényesítésére alkalmazott belső eljárás részletesen külön mellékletben kerülnek ismertetésre.

4.3. Az érintett bármilyen, a személyes adatai kezelésével kapcsolatos kérdéssel, észrevétellel vagy panasszal az Egyetemhez fordulhat postai úton, emailben, illetve személyesen az Egyetem mindenkori székhelyén.

4.4. Az Egyetem az érintett beadványát megvizsgálja és az érintettet tájékoztatja a vizsgálat eredményéről 30 napon belül.

4.5. Amennyiben az Egyetem nem tesz intézkedést az érintett beadványa alapján, akkor tájékoztatja az érintettet, hogy mely hatóságnál és milyen feltételekkel élhet panasszal vagy jogorvoslati jogával.

5. NYILVÁNTARTÁSOK VEZETÉSÉNEK SZABÁLYAI

5.1. Az Egyetem a Rendelet 30. cikk szabályainak megfelelően vezeti az

- a) adatkezelések nyilvántartását
- b) az adatfeldolgozói nyilvántartást

- c) az adatfeldolgozóként végzett adatkezelésekről a nyilvántartást
- d) az érintettektől érkezett kérelmekről a nyilvántartást
- e) az adattovábbítások nyilvántartását
- f) az adatkezelési tájékoztatók nyilvántartását
- g) az adatvédelmi incidensek nyilvántartását.

5.2. A nyilvántartások valós tartalmáért a rektor felelős.

5.3. A nyilvántartások vezetése és naprakészen tartása a rektor által erre kijelölt foglalkoztatottak feladata.

5.4. A nyilvántartásokat a jelen szabályzatban meghatározott szabályok alapján papíralapon és/vagy elektronikus módon kell vezetni.

6. AZ ADATVÉDELMI INCIDENS

6.1. Az adatbiztonság sérülése, illetve az Egyetem által kezelt adatok véletlen vagy jogellenes megsemmisülése, elvesztése, módosulása, jogosulatlan továbbítása vagy nyilvánosságra hozatala, az adatokhoz való jogosulatlan hozzáférés bekövetkezése vagy ezeknek a gyanúja adatvédelmi incidens bekövetkezését jelenti.

6.2. Adatvédelmi incidens bekövetkezése esetén az adatokat bármely jogviszony alapján kezelő személy köteles a külön utasításban életbe léptetett vonatkozó belső eljárásrend szerint eljárni.

7. AZ ADATKEZELÉSÉRT VALÓ FELELŐSSÉG

7.1. Az Egyetem felelőssége

7.1.1 Az Egyetem felelősséggel tartozik a személyes adatok kezelésének jogszerűségéért.

7.1.2. A bírósági jogorvoslathoz való jogának érvényesítése érdekében az érintett az Egyetem, illetve – az adatfeldolgozó tevékenységi körébe tartozó adatkezelési műveletekkel összefüggésben – az adatfeldolgozó ellen az adatvédelmi hatósághoz, vagy bírósághoz fordulhat, ha megítélése szerint a személyes adatait a személyes adatok kezelésére vonatkozó, jogszabályban vagy az Európai Unió kötelező jogi aktusában meghatározott előírások megsértésével kezelik.

7.2. Az Egyetem által alkalmazott munkatársak és hallgatók felelőssége

7.2.1. Az Egyetem által foglalkoztatott személyek munkajogi, polgári jogi és büntetőjogi felelősséggel tartoznak a munkájuk során végzett adatkezelési műveletek jogszerűségéért és a jelen Szabályzatban foglaltak betartásáért.

7.2.2. Amennyiben az Egyetemmel hallgatói jogviszonyban álló személy az Egyetem, vagy bármely szervezeti egysége nevében vagy képviselőjében személyes adatot kezel – így különösen, de nem kizárólagosan, mint az Egyetemi Hallgatói Önkormányzat tagja, tisztviselője jár el –, úgy köteles a jelen Szabályzatban írtakat magára nézve kötelezően elfogadni, és a személyes adatok kezelését a jelen Szabályzat, valamint a vonatkozó jogszabályok szerint végezni. Az Egyetem munkatársaira vonatkozó kötelezettségek ilyen esetekben a hallgatói jogviszonyban álló személyeket is kötelezik.

7.2.3. Vétkes kötelezettségszegésnek minősül amennyiben a munkatárs vagy a hallgató nem tartja be a jelen Szabályzatban, illetve a személyes adatok kezelésére vonatkozó jogszabályokban foglalt kötelezettségeit.

8. AZ ADATVÉDELMI HATÁSVIZSGÁLAT

8.1. Adatvédelmi hatásvizsgálat végzési kötelezettség

8.1.1. Az adatvédelmi tisztviselő köteles eldönteni, hogy adott adatkezeléssel kapcsolatban kell-e hatásvizsgálatot végezni, vagy a hatásvizsgálat mellőzhető.

8.1.2. Az adatkezelő az adatkezelést megelőzően hatásvizsgálatot köteles végezni, ha az adatkezelés valószínűleg magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, így különösen az alábbi esetekben:

- a) a természetes személyekre vonatkozó egyes személyes jellemzők olyan módszeres és kiterjedt értékelése, amely automatizált adatkezelésen – ideértve a profilalkotást is – alapul, és amelyre a természetes személy tekintetében joghatással bíró vagy a természetes személyt hasonlóképpen jelentős mértékben érintő döntések épülnek,
- b) az érintett kifejezett hozzájárulása alapján kezelt személyes adatok különleges kategóriái, vagy a büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó személyes adatok nagy számban történő kezelése,
- c) a nyilvános helyek nagymértékű, módszeres figyelése.

8.1.3. A hatásvizsgálat célja annak megállapítása, hogy a tervezett adatkezelési műveletek milyen hatást gyakorolnak a személyes adatok védelmére.

8.1.4. A hatásvizsgálatnak olyannak kell lennie, amely kiterjed legalább:

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

8.1.5. Nem kell hatásvizsgálatot végezni, ha egyértelmű, hogy az adott adatkezelési művelet a természetes személyek jogaira és szabadságára nézve nem jár magas kockázattal. Az adatvédelmi tisztviselő az adatvédelmi hatásvizsgálat mellőzéséről adatkezelésenként külön-külön írásos jegyzőkönyvet készít, melyben rögzíti a hatásvizsgálat mellőzésének okait.

8.1.6. A mellőzés okai különösen:

- a) az adatkezelés valószínűsíthetően nem jár magas kockázattal,
- b) már készült hasonló adatvédelmi hatásvizsgálat, ahol az adatkezelés jellege, hatóköre, körülménye és célja egymáshoz nagyon hasonló,
- c) az adatkezelés szerepel abban a felügyeleti hatóság által kiadott jegyzékben, melyre vonatkozóan nem kell adatvédelmi hatásvizsgálatot végezni.

8.2. Az adatvédelmi hatásvizsgálat elvégzése

8.2.1. Az adatvédelmi hatásvizsgálatot az adatkezelés megkezdése előtt el kell végezni a tervezett adatkezelési folyamatok alapján. Az adatkezelés tervezett folyamatának változása esetén indokolt esetben az adatvédelmi hatásvizsgálat egyes lépéseit meg kell ismételni. Az ismétlések elvégzéséről az adatvédelmi tisztviselő dönt.

8.2.2. Az adatvédelmi hatásvizsgálat az adatvédelmi tisztségviselő irányításával történik, melyben részt vesz a tényleges adatkezelést végző, illetve, ha az adott adatkezelésben adatfeldolgozó is érintett, akkor az adatfeldolgozó is.

8.2.3. Az adatvédelmi tisztviselő dönt arról, hogy az adott ügyben az adatvédelmi hatásvizsgálattal érintettek, illetve a képviselőik véleményét ki kell-e kérni, vagy nem. Ha a vélemény kikérés mellett dönt, meghatározza azt, hogy a véleménykérés milyen módon, tartalommal és arányban történjen.

Amennyiben arról dönt, hogy nem kell az érintettek, illetve a képviselőik véleményét kikérni, írásban dokumentálja döntésének okát.

8.3. Az adatvédelmi hatásvizsgálat folyamata

8.3.1. Az adatvédelmi tisztviselő felelős azért, hogy az adatvédelmi hatásvizsgálat az alábbiak szerint – újra és újra – ismétlődő körforgásban megtörténjen az alábbiak tekintetében:

- a tervezett adatkezelés leírása,
- az adatkezelés szükségességének és arányosságának vizsgálata,
- már tervezett intézkedések,
- a természetes személyek adatvédelemmel kapcsolatos jogait és szabadságait érintő kockázatok vizsgálata,
- a kockázatok kezelésére irányuló intézkedések,
- a dokumentáció,
- a nyomon követés és felülvizsgálat.

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

8.3.3. Az adatvédelmi tisztviselő a hivatali adatkezelés tekintetében a rektorral egyetértésben dönt az adott adatvédelmi hatásvizsgálat nyilvánosságra hozataláról, ezen belül a nyilvánosságra hozatal módjáról, a mértékéről (teljes vagy részleges dokumentáció).

8.3.4. Ha az adatvédelmi hatásvizsgálat megállapítja, hogy az adatkezelés az adatkezelő által a kockázat mérséklése céljából tett intézkedések hiányában valószínűsíthetően magas kockázattal jár, a személyes adatok kezelését megelőzően az adatkezelő konzultál a felügyeleti hatósággal.

9. A SZABÁLYZAT NYILVÁNOSSÁGA

9.1. A szabályzat teljes felülvizsgálatát legalább évenként el kell végezni. A szabályzat egyes részterületeit a szabályzatban meghatározott időnként, az általános felülvizsgálati időtől függetlenül el kell végezni.

9.2. Az adatvédelmi tisztviselő a szabályzat teljes, illetve egyes részeinek felülvizsgálatát köteles kezdeményezni és a felülvizsgálatot előkészíteni, ha azt a körülmények indokolják. A módosítást a Szenátus határozatával hagyja jóvá.

9.3. A jóváhagyást követően ismét gondoskodni kell a szabályzat megismertetéséről, illetve a szabályzat védendő adatainak védelméről.

9.4. A szabályzatot az adatkezelő weboldalán közzéteszi.

10. ZÁRÓ RENDELKEZÉSEK

10.1. Jelen szabályzatot a Szenátus 14/2023. (III. 30.) számú határozatával elfogadta. Jelen szabályzat 2023. március 31. napján lép hatályba, ezzel egyidejűleg a Szenátus 4/2022. (I. 27.) számú határozatával elfogadott Adatvédelmi szabályzat hatályát veszti.

Budapest, 2023. március 30.

