SZÍNHÁZ- ÉS FILMMŰVÉSZETI EGYETEM

SZFE 1865

2/2024. (05.06.) számú rektori szabályzat

A Színház-és Filmművészeti Egyetem Adatvédelmi Szabályzata

Hatályos: 2024. május 07. napjától

Preambulum

A Színház- és Filmművészeti Egyetem (a továbbiakban: Egyetem) jelen szabályzatban (a továbbiakban: Szabályzat) határozza meg a természetes személyek személyes adatainak kezelésével és védelmével kapcsolatos irányelveket, valamint az Egyemet érintő adatvédelmi tevékenység ellátásában résztvevő szervezeti egységek és egyéb személyek feladatait és együttműködésük kereteit.

1.§
A Szabályzat hatálya

(1) A Szabályzat hatálya alá tartozó személyek kötelesek a tevékenységük során az Egyetem kezelésében lévő személyes adatokat a mindenkor hatályos jogszabályi rendelkezéseknek megfelelően, így különösen a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről szóló 2016/679/EU európai parlamenti és tanácsi rendelet (a továbbiakban: GDPR), az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) alkalmazandó rendelkezései, valamint az Egyetemre irányadó egyéb jogszabályok előírásai szerint kezelni.

(2) A Szabályzat hatálya alá tartozó személyek kötelesek az olyan tevékenységük során, amely szükségszerűen együtt jár személyes adatok kezelésével, az adott tevékenységre vonatkozó speciális szabályzatokban foglalt rendelkezések mellett a jelen Szabályzat előírásai szerint eljárni azzal, hogy amennyiben a speciális szabályzat a jelen Szabályzattal ellentétes rendelkezést tartalmaz, akkor jelen Szabályzat alkalmazandó.

(3) Jelen Szabályzat személyi hatálya kiterjed az Egyetemmel foglalkoztatási jogviszonyban állókra (a továbbiakban: foglalkoztatottak), továbbá azon természetes személyekre (a továbbiakban: érintett), akik személyes adatait a jelen Szabályzat hatálya alá tartozó adatkezelések (nyilvántartások) tartalmazzák, valamint azon érintettekre, akik jogait vagy jogos érdekeit az adatkezelés érinti. A jelen Szabályzat hatálya továbbá kiterjed mindazon személyekre, akikkel összefüggésben az Egyetem adatkezelést végez.

(4) Az Egyetem megbízásából személyes adatok kezelését vagy feldolgozását végzők esetén az erre a jogviszonyra az Egyetem által kötött szerződésben a GDPR 28. cikkének megfelelően rendelkezni kell arról, hogy az Egyetem által megbízott adatfeldolgozó a feladata ellátása során hogyan juttatja érvényre jelen Szabályzat rendelkezéseit.

(5) A Szabályzat tárgyi hatálya az Egyetem mindazon adatkezeléseire (nyilvántartásaira) kiterjed – függetlenül attól, hogy az adatkezelés elektronikusan vagy papíralapon történik – amelyek
   a) a felsőoktatási tevékenységhez kapcsolódó adatkezelést valósítanak meg;
   b) a felsőoktatási tevékenységen kívüli ügyfélkapcsolati jellegű adatkezelést valósítanak meg (az
   c) Egyetemmel kapcsolatba lépni szándékozó, kapcsolatban álló vagy kapcsolatban állt személyek, beleértve ezek meghatalmazottjait, képviselőit is; foglalkoztatási jogviszonyhoz kapcsolódó adatkezelést valósítanak meg, így az Egyetemmel munkaviszonyban vagy egyéb foglalkoztatási jogviszonyban (együtt: foglalkoztatási jogviszony) álló, állt, vagy foglalkoztatási jogviszonyba lépni szándékozó személyek);
   d) az Egyetemmel szerződéses kapcsolatban álló gazdasági társaságok vagy egyéb szervezetek képviselőinek, kapcsolattartóinak az adataira vonatkoznak.

2. §
Alapelvek

(1) Az Egyetem a személyes adatok kezelésével járó tevékenysége során érvényre juttatja a GDPR alapelveit, így különösen:

a) a jogszerűség, tisztességes eljárás és átláthatóság elve: a személyes adatok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni;

b) a célhoz kötöttség elve: a személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történik, és azokat az Egyetem nem kezeli ezekkel a célokkal össze nem egyeztethető módon;

c) az adattakarékosság elve: a kezelt személyes adatok az adatkezelés céljai szempontjából megfelelőek és relevánsak kell, hogy legyenek, és a szükségesre kell korlátozódniuk;

d) a pontosság elve: a kezelt személyes adatoknak pontosnak és szükség esetén naprakésznek kell lenniük; minden ésszerű intézkedést meg kell tenni annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul töröljék vagy helyesbítsék;

e) a korlátozott tárolhatóság elve: a személyes adatok tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé;

f) az integritás és bizalmas jelleg elve: 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;

g) a beépített adatvédelem elve: olyan megfelelő technikai és szervezési intézkedések végrehajtása, amelyek már az adatkezeléssel járó folyamatok tervezésétől (az adatkezelés módjának meghatározásától) kezdődően az adatkezelés megszüntetéséig terjedő időszakban azt célozzák, hogy az adatvédelmi elvek hatékony megvalósítása, illetve a GDPR-ban foglalt követelmények teljesítéséhez és az érintettek jogainak védelméhez szükséges garanciák beépüljenek az adatkezelés folyamatába;

h) az alapértelmezett adatvédelem elve: olyan technikai és szervezési intézkedések végrehajtása, amelyek biztosítják, hogy alapértelmezés szerint kizárólag olyan személyes adatok kezelésére kerüljön sor, amelyek az adott konkrét adatkezelési cél szempontjából szükségesek, továbbá, hogy a gyűjtött személyes adatok mennyisége, kezelésük mértéke, tárolásuk időtartama és hozzáférhetőségük is csak az adatkezelési cél szempontjából szükséges mértékre korlátozódjon. Különösen azt kell biztosítani, hogy a személyes adatok alapértelmezés szerint természetes személy beavatkozása nélkül arra illetéktelen személyek számára ne válhassanak hozzáférhetővé.

3.§
A Szabályzat célja

(1) A jelen Szabályzat célja, hogy biztosítsa az Egyetem tevékenysége során a személyes adatok védelméhez fűződő jog érvényesülését, továbbá, hogy az Egyetem által kezelt személyes adatok jogosulatlan felhasználásának megakadályozása érdekében meghatározza a személyes és különleges adatok kezelése során irányadó adatvédelmi és adatbiztonsági szabályokat.

(2) A Szabályzat célja továbbá, hogy meghatározza azokat a szervezési és technikai intézkedéseket, amelyek kialakításával az Egyetem gondoskodik a személyes adatok kezelése során a személyes adatok biztonságáról. Erre tekintettel a Szabályzat az Egyetem által folytatott adatkezelési

tevékenységek során figyelembe veendő és követendő elveket, rendelkezéseket tartalmaz. Ezeket az előírásokat minden egyes adatkezelési folyamat, tevékenység során, annak teljes tartama alatt figyelembe kell venni.

(3) A Szabályzat további célja, hogy meghatározza az Egyetem szervezeti egységeinél (ideértve a Hallgatói Önkormányzatot, a Doktorandusz Önkormányzatot, valamint az Egyetem Szervezeti és Működési Szabályzata szerinti testületeket, bizottságokat is) vezetett, személyes adatokat tartalmazó nyilvántartások vezetésének és működtetésének jogszerű rendjét, valamint biztosítsa a személyes adatok védelme elveinek és az adatbiztonság követelményeinek érvényesülését.

4. §
Dokumentálási kötelezettség

(1) Az Egyetem felelős a személyes adatok kezelésére vonatkozó alapelvek [GDPR 5. cikk (1) bekezdés] betartásáért. Az Egyetemnek képesnek kell lennie a személyes adatok kezelésére vonatkozó alapelvek betartásának igazolására [GDPR 5. cikk (2) bekezdés]. Az adatvédelmi alapelvek betartásának igazolása különösen az adatkezeléshez kapcsolódó döntéseket megalapozó körülmények és a döntések (pl. az adatkezelés feltételeit meghatározó döntéselőkészítő iratok), az érintetteknek szóló adatkezelési tájékoztatók, az érintettől származó nyilatkozatok (pl. hozzájáruló nyilatkozatok, az adatkezelési tájékoztató megismerését igazoló dokumentumok), továbbá a személyes adatokat tartalmazó (elektronikus vagy papír alapú) dokumentumok szervezeten belüli vagy azon kívüli mozgásának megfelelő dokumentálásával történik.

(2) Az Egyetem – a GDPR 30. cikkének megfelelően – nyilvántartást vezet az általa végzett adatkezelési tevékenységekről.

(3) Az adatkezelési alapelvek betartásának igazolása adatvédelmi incidens esetén különösen az incidenssel érintettek körének, az incidenssel érintett személyes adatok körének, az incidens kezelése során tett intézkedéseket megalapozó körülmények és a döntések dokumentálásával történik.

(4) Az Egyetem – a GDPR 33. cikkének megfelelően – nyilvántartást vezet a bekövetkezett adatvédelmi incidensekkel kapcsolatos tényekről és intézkedésekről.

5. §
Az adatvédelmi tevékenység ellátásában résztvevők

(1) Az Egyetem tevékenységi körébe tartozó feladatok ellátása során a személyes adatok adatkezelője az Egyetem, amely az adatkezelési tevékenységet az erre felhatalmazott szervezeti egységei (továbbiakban: adatkezelő szervezeti egység) útján végzi.

(2) Amennyiben az adatkezelés célja azt indokolja és az adatkezelés célját az Egyetem valamely szervezeti egysége önállóan határozza meg vagy törvény adatkezelőként az Egyetem valamely szervezeti egységét kifejezetten nevesíti, az Egyetem valamely szervezeti egysége (pl. az Egyetem által fenntartott intézmény vagy intézet) is adatkezelőnek minősülhet. Ahol e Szabályzat az Egyetemet adatkezelőként említi, és a szövegből egyértelműen más nem következik, ott az e szakasz alapján önálló adatkezelőnek minősülő szervezeti egységet is érteni kell.

(3) Az adatvédelmi tevékenység irányításában és ellátásában az Egyetem szervezeti egységei (ideértve a Hallgatói Önkormányzatot, a Doktorandusz Önkormányzatot, valamint az Egyetem Szervezeti és Működési Szabályzata szerinti testületeket és bizottságokat is) az Egyetem Szervezeti és Működési Szabályzatában meghatározott feladatkörükön belül a jelen Szabályzatban foglaltak szerint vesznek részt.

(4) A rektor felelős azért, hogy az Egyetem – mint adatkezelő, illetve adatfeldolgozó – működése az adatvédelmi szabályoknak megfeleljen. Ennek érdekében:

a) gondoskodik az adatvédelmi tevékenység irányításában és ellátásában résztvevő szervezeti egységek kijelöléséről, feladataik, az adatvédelmi tárgyú ügyekkel kapcsolatos döntési jogkörök meghatározásáról, az egyes adatkezelési döntési szintek kialakításáról;
b) biztosítja az adatvédelmi tevékenység irányításához és ellátásához, valamint az érintett jogai gyakorlásához szükséges személyi és tárgyi feltételeket;
c) felelős az adat- és titokvédelmi, valamint biztonsági és információbiztonsági szabályzatok kiadásáért és betartatásáért;
d) gondoskodik arról, hogy az adatvédelmi tevékenység során esetleg előforduló, feltárt hiányosságok megszűntetéséről, szükség szerint a felelősségre vonásról;
e) kinevezi az Egyetem adatvédelmi tisztviselőjét, és intézkedik, hogy az adatvédelmi tisztviselő neve és elérhetősége bejelentésre kerüljön a Nemzeti Adatvédelmi és Információszabadság Hatóság részére;
f) biztosítja az Egyetem adatvédelmi tisztviselője feladatainak ellátásához szükséges személyi és tárgyi feltételeket;
g) munkajogi értelemben vett közvetlen felettese az adatvédelmi tisztviselőnek.

(5) Az Egyetem szervezeti egységeinek vezetői az irányításuk alá tartozó szervezeti egység tekintetében:

a) betartják és betartatják az adat- és titokvédelmi, valamint a biztonsági és információbiztonsági előírásokat; az adatvédelmi tisztviselővel, a Jogi Osztállyal, továbbá az informatikáért felelős szakterülettel együttműködve gondoskodnak az adat- és titokvédelmi, valamint a biztonsági és információbiztonsági előírások, szabályzatok megismertetéséről, rendszeres oktatásáról;
b) kijelölik az irányításuk alá tartozó szervezeti egység adatkezelési megbízottját;
c) gondoskodnak arról, hogy az irányításuk alá tartozó szervezeti egységek felelősségi körébe tartozó nyilvántartások naprakészek, megbízhatóak legyenek;
d) gondoskodnak arról, hogy az irányításuk alatt álló személyek az adatkezelés meghatározott feltételeinek megfelelően járjanak el [GDPR 32. cikk (4) bekezdés];
e) az adatkezelési megbízott előterjesztésére – az Egyetem döntéselőkészítésre vonatkozó szabályainak megfelelően – döntenek a jelen Szabályzatban, illetve az adatkezeléssel járó folyamatot szabályozó egyéb belső szabályzatokban a feladat- és hatáskörébe utalt kérdésekben.

(6) A Kommunikáció és Marketing Igazgatóság

a) adatvédelmi incidens esetén közreműködik az érintettek tájékoztatásának módjáról és a tájékoztatás tartalmáról való döntés előkészítésében,
b) adatvédelmi incidens esetén – az adatvédelmi tisztviselő közreműködésével – szükség esetén sajtóközleményt bocsát ki és kizárólagos kapcsolatot tart a sajtó képviselőivel.

(7) Az adatvédelmi tisztviselő szükség szerinti közreműködésével ellátja az érintetti jogok gyakorlásával kapcsolatos beadványok megválaszolását a személyes adatok kezelését, illetve a GDPR szerinti jogaik gyakorlását érintő panaszok kivételével.

(8) Az Egyetem informatikáért felelős szakterülete az Egyetem Szervezeti és Működési Szabályzatában, valamint az Egyetem Informatikai Biztonsági Szabályzatában meghatározott feladatkörében:
   a) ellátja az informatikai biztonsággal kapcsolatos feladatokat a folyamatos üzemeltetési feladatok kivételével, különösen az Egyetem Informatikai Biztonsági Szabályzatában meghatározott feladatokat;
   b) ellátja az informatikai fejlesztéseknél és beszerzéseknél a beépített adatvédelem kontrolljai meglétének biztosításával, az adatminőség biztosításával, az informatikai biztonság kockázatarányos szintjét biztosító jogosultsági és naplózási rendszer kialakításával, a biztonságos szoftverfejlesztés alapelveinek érvényesítésével kapcsolatos feladatokat,
   c) az informatikai rendszerek üzemeltetése területén ellátja a személyes adatok kezelésével kapcsolatos technikai védelem megvalósítását, ellátja az Egyetem Informatikai Biztonsági Szabályzatában meghatározott, hatáskörébe tartozó információbiztonsági feladatokat, valamint a rendelkezésre állási kontrollok biztosítását, a tárolt és továbbított személyes adatok bizalmasságának védelmét, az incidensfelderítési és -kezelési tevékenység támogatását,
   d) az érintett szervezeti egységek vezetőivel együttműködve gondoskodik az információbiztonsági előírások, szabályzatok megismertetéséről, rendszeres oktatásáról.

(9) A Jogi Osztály
   a) szakmai támogatást nyújt az adatkezeléssel összefüggő, nem adatvédelmi jogszabályok értelmezésében,
   b) a szervezeti egység adatkezelési megbízottjától kapott információk alapján közreműködik a szervezeti egységgel kapcsolatos, az adatkezelőt terhelő döntések előkészítésében és az intézkedések végrehajtásában (pl. érdekmérlegelési teszt elvégzése, adatvédelmi hatásvizsgálat lefolytatása);
   c) az Egyetem Szervezeti és Működési Rendje szerint biztosítja, hogy az adatvédelmi tisztviselő véleményét kikérjék az Egyetem adatvédelmi tárgyú vagy adatvédelmi vonatkozású belső szabályzatainak előkészítése során,
   d) biztosítja az Egyetem képviseletét az érintett által az Egyetem ellen az érintett adatvédelmi jogainak megsértése miatt indított, illetve az Egyetem által a Nemzeti Adatvédelmi és Információszabadság Hatóság határozatainak felülvizsgálata iránt indított perekben, illetve egyéb eljárásokban.

(10) Adatkezelési megbízottat kell kijelölni az adatkezelési szempontból nagy jelentőséggel bíró szervezeti egységeknél. A Hallgatói Önkormányzat, Doktorandusz Önkormányzat és más érdekképviseleti szervek is kijelölhetnek olyan személyt, aki e szervezetek tevékenysége során a személyes adatok kezelésével kapcsolatban ellátja a jelen Szabályzat szerinti feladatokat vagy azok meghatározott részét.

(11) Adatkezelési megbízottnak olyan személyt kell kijelölni, aki az adott szervezeti egység tevékenységét, az ahhoz kapcsolódó adminisztratív folyamato(ka)t átlátja, illetve a szervezeti egység tevékenységét támogató informatikai rendszerekről kellő ismeretekkel bír. Egy adatkezelési megbízott hatáskörébe több szervezeti egység is tartozhat, illetve egy szervezeti egységnek több adatkezelési megbízottja is lehet. Az adatkezelési megbízotti kijelölést, hatáskört és a feladatokat írásba kell foglalni (pl. a munkaköri leírásban vagy a megbízásról szóló dokumentumban szerepeltetni kell).

(12) Az adatkezelési megbízott a felelősségi körébe tartozó szervezeti egység(ek) feladatkörén belül jelen Szabályzat és egyéb, a szervezeti egység tevékenységét érintő belső szabályozás szerint:
   a) figyelemmel kíséri az adott szervezeti egység tevékenységét adatkezelési szempontból, az adatkezeléssel kapcsolatos bárminemű változás vagy arra utaló szándék (pl. tervezett új

adatkezelés, adatkezelés megszüntetése, módosítása) egyeztetést kezdeményez az adatvédelmi tisztviselővel;
b) felelős azért, hogy az adott szervezeti egység a személyes adatokat az adatkezelésre vonatkozó belső szabályozásnak megfelelően kezelje;
c) napra készen tartja a szervezeti egység kezelésében lévő adatkezelések adatait az Adatkezelési Tevékenységek Nyilvántartásában;
d) adatvédelmi incidens gyanúja esetén az eseményt bejelenti az erre vonatkozó eljárásrend szerint vagy kétség esetén egyeztet az adatvédelmi tisztviselővel;
e) segíti a Jogi Osztály tevékenységét azzal, hogy információt szolgáltat a szervezeti egység tevékenységéről, és közreműködik a szervezeti egységgel kapcsolatos, az adatkezelőt terhelő döntések előkészítésében és az intézkedések végrehajtásában (pl. érdekmérlegelési teszt elvégzése, adatvédelmi hatásvizsgálat lefolytatása);
f) együttműködik az ugyanazon adatkezelésben érintett más adatkezelési megbízottakkal;
g) közreműködik az érintettek jogai gyakorlásának biztosításában;
h) közreműködik az adatvédelmi incidensek következményeinek elhárításában;
i) közreműködik az adatvédelmi tisztviselő vizsgálataiban.

6.§
Az adatvédelmi tisztviselő

(1) Az adatvédelmi tisztviselőt a rektor nevezi ki az olyan, az Egyetemmel foglalkoztatásra irányuló jogviszonyban álló természetes személyek közül, aki megfelelően ismeri az Egyetem működését, feladatait, munkafolyamatait és rendelkezik:
a) lehetőleg jogi végzettséggel vagy informatikai főiskolai (BSc) vagy egyetemi (MSc) szintű végzettséggel;
b) az európai és hazai adatvédelemmel kapcsolatos főbb jogszabályok, hatósági és bírósági határozatok, iránymutatások ismeretével;
c) alapvető adatkezelési és informatikai folyamatok ismeretével;

(2) Az adatvédelmi tisztviselő feladatai ellátására és/vagy adatvédelmi tanácsadási feladattal egyéb, jogi vagy természetes személy szakértőt is megbízhat, amennyiben eleget tesz a jelen Szabályzat 6.§ (1) bekezdésben meghatározott követelményeknek.

(3) Az adatvédelmi tisztviselő független, függetlensége biztosítása érdekében szakmai feladatai ellátása során utasítást nem fogadhat el, szakmai feladatai ellátásával összefüggésben nem bocsátható el. Jelen Szabályzatban foglalt tevékenysége ellátása során autonóm, szakmai ügyekben kizárólag a rektornak tartozik felelősséggel.

(4) Az Egyetem elősegíti az adatvédelmi tisztviselő megfelelő szakmai feladatellátását, ennek érdekében az Egyetem biztosítja különösen az adatvédelmi tisztviselő feladatai végrehajtásához, a személyes adatokhoz és az adatkezelési műveletekhez való hozzáférést, valamint a szakértői szintű ismereteinek fenntartásához szükséges forrást, elegendő időt a feladatai ellátásához, valamint az informatikáért és a biztonságért felelős szakterület együttműködése révén az adatvédelmi tisztviselő bevonását:
a) a megfelelő technikai-eljárási intézkedésekhez szükséges intézkedések és források meghatározása (költségvetési tervezés) során annak érdekében, hogy teljesüljenek az adatvédelem alapelvei a technikai vívmányok alkalmazása (beépített adatvédelem) és az adatvédelem-barát megoldások (alapértelmezett adatvédelem) révén;

b) a Hatósággal történő együttműködés során, amellyel az adatvédelmi tisztviselő – a Jogi Osztály és az ügy természetéből adódóan esetenként egyéb szakterület munkatársainak bevonásával – tartja a kapcsolatot.

(5) Az adatvédelmi tisztviselő véleményét – a Szervezeti és Működési Rend, valamint jelen Szabályzat rendelkezései szerint – előzetesen ki kell kérni az adatkezelést érintő döntések, szerződések és belső szabályzatok tervezetéről.

(6) Az adatvédelmi tisztviselőt tisztsége fennállása alatt és annak megszűnését követően titoktartási kötelezettség terheli a tevékenysége során tudomására jutott minden olyan információ tekintetében, amely nem minősül közérdekű vagy közérdekből nyilvános adatnak.

(7) Az Egyetemen nem lehet adatvédelmi tisztviselő az a természetes személy, aki az Egyetemen az adatkezelési tevékenység céljainak, kereteinek, eszközeinek meghatározásáról dönt, különösen a rektor és a gazdasági főigazgató, valamint helyetteseik, továbbá az adatkezelésért felelős szervezeti egység vezetője, a belső ellenőr, illetve az információbiztonsági felelős.

(8) Az adatvédelmi tisztviselő az adatvédelmi tisztviselői feladatokon kívül a rektordöntése alapján más munkakörhöz kötődő feladatokat is elláthat, amennyiben azok nem eredményeznek összeférhetetlenséget.

(9) Az adatvédelmi tisztviselő nevét és elérhetőségeit az Egyetem honlapján, székhelyén, telephelyén a nyilvánosság részére mindenkor elérhetővé kell tenni. Az Egyetem továbbá közli az adatvédelmi tisztviselő nevét és elérhetőségét a Nemzeti Adatvédelmi és Információszabadság Hatósággal.

(10) Az adatvédelmi tisztviselő feladatai:
a) közreműködik, illetve segítséget nyújt az adatkezeléssel összefüggő döntések meghozatalában, valamint az érintettek jogainak biztosításában;
b) ellenőrzi a GDPR, az Infotv. és az adatkezelésre vonatkozó más jogszabályok, valamint a jelen Szabályzat, továbbá az Egyetem egyéb belső szabályzatai rendelkezéseinek a megtartását, belső adatvédelmi ellenőrzési eljárást folytat le;
c) kivizsgálja – az érintett szakterületek a Jogi Osztály bevonásával – a neki címzett panaszokat, jogosulatlan adatkezelés észlelése esetén annak megszüntetésére hívja fel az adatkezelőt vagy az adatfeldolgozót;
d) a Jogi Osztállyal és az informatikáért felelős szakterülettel együttműködve elkészíti az adatvédelmi és incidenskezelési szabályzatot;
e) a Humán Erőforrás Irodával együttműködve gondoskodik az adatvédelmi ismeretek megfelelő oktatásáról;
f) a Jogi Osztállyal együttműködve tájékoztatást nyújt, tanácsot ad a személyes adatok kezelésére vonatkozó előírásokról;
g) személyes adatot is kezelő (új) informatikai rendszer fejlesztése során közreműködik a beépített adatvédelem alapelve érvényesülésének érdekében, vagy ha szükséges, az adatvédelmi hatásvizsgálat lefolytatásában;
h) az adatvédelmi incidenskezeléssel kapcsolatban ellátja a jelen Szabályzat szerinti feladatokat;
i) az Egyetem adatvédelmi helyzetéről éves összefoglaló jelentést készít a rektornak;
j) kapcsolatot tart és – a Jogi Osztállyal és az ügy természetéből adódóan esetenként egyéb szakterület munkatársainak bevonásával – együttműködik a Hatósággal.

7.§
Adatkezelés bevezetésével kapcsolatos feladatok

(1) Jogszabályban elrendelt vagy jogszabály rendelkezése miatt szükséges, vagy az Egyetem döntése alapján létrehozandó, személyes adatok kezelésével járó új nyilvántartás vagy nyilvántartási rendszer (a továbbiakban együtt: adatkezelés) bevezetése esetén, továbbá ha a meglévő adatkezelésben kezelt személyes adatok új célú felhasználását vagy még nem kezelt személyesadat-kategóriák felvételét, tárolását, harmadik személynek továbbítását tervezik (a továbbiakban együtt: új adatkezelés), az új adatkezelés bevezetése során a döntéselőkészítés rendjére vonatkozó belső szabályokat e fejezet rendelkezéseit figyelembe véve kell alkalmazni.

(2) Új adatkezelés bevezetése rektoriutasítással történik. A rektori utasítás – a belső szabályozók kötelező tartalmi és formai elemein túl – tartalmazza

a) az adatkezeléssel kapcsolatos fontosabb információkat (az adatkezelés célja, jogalapja, kezelt adatok köre stb.),

b) az adatkezelésért felelős szervezeti egység és egyéb szervezeti egységek új adatkezeléssel kapcsolatos feladatait, így különösen:

ba) a személyes adatok felvételének, módosításának, törlésének rendjét,

bb) adatszolgáltatási kötelezettségek meghatározását az adatok naprakészen tartása érdekében,

bc) a nyilvántartási rendszerből történő adattovábbítás, az ahhoz való hozzáférés rendjét;

bd) az adatkezelésre vonatkozó adatbiztonsági intézkedések meghatározását;

c) a GDPR-nak, az Infotv-nek és egyéb alkalmazandó jogszabálynak megfelelő adatkezelési tájékoztató kötelező és ajánlott tartalmi elemeit, az érdekmérlegelési tesztet, amennyiben az adatkezelés jogalapja az adatkezelő jogos érdeke,

d) az érintett hozzájárulásán alapuló adatkezelés esetén a hozzájáruló, illetve a hozzájárulás visszavonásáról szóló nyilatkozat mintáját, egyéb, az adatkezelési tevékenységhez szükséges dokumentumok (pl. űrlap) mintáját.

(3) Az adatkezelésért felelős szervezeti egység, illetve szükség szerint az informatikáért felelős szakterület adatkezelési megbízottját az új adatkezelés bevezetésére vonatkozó igény felmerülésétől kezdve be kell vonni az új adatkezelés feltételeinek kidolgozása folyamatába.

(4) Amennyiben az új adatkezelés bevezetése több szervezeti egységet érint, az adatkezelésért felelős valamennyi érintett szervezeti egység adatkezelési megbízottját be kell vonni az adatkezelés feltételeinek kidolgozása folyamatába. Az informatikáért felelős szakterület adatkezelési megbízottját minden esetben be kell vonni a folyamatba. Az adatkezelés fejlesztése iránti igényt megfogalmazó szervezeti egység vezetője az egyéb szakterületek adatkezelési megbízottjai bevonásának szükségességéről az érintett adatkezelési megbízottakat és az adatvédelmi tisztviselőt értesíti.

(5) Az új adatkezelés feltételeinek kidolgozásában érintett szakterületek/szervezeti egységek adatkezelési megbízottjai kötelesek egymással és az adatvédelmi tisztviselővel együttműködni. Az adatkezelés feltételeinek kidolgozásában érintett szakterületek/szervezeti egységek adatkezelési megbízottjai tevékenységének koordinálásáról az adatvédelmi tisztviselő gondoskodik.

(6) Az új adatkezelés bevezetésével, az adatkezelés feltételeinek meghatározásával kapcsolatban az adatkezelési megbízott a Jogi Osztály közreműködésével és a leendő adatkezelésért annak tárgya szerint felelős szakterület/szervezeti egység(ek) adatkezelési megbízottjával együttműködve:

a) meghatározza az adatkezelés célját, az adatkezelés jogalapját, a kezelendő adatok körét, az adatkezelés egyéb feltételeit, és erről írásbeli javaslatot készít a döntésre jogosultnak (GDPR 4. cikk 7. és 16. pont);
b) tájékoztatja a döntésre jogosultat arról, hogy a meglévő adatkezelés eltérő, új célja összeegyeztethető-e az adatkezelés eredeti céljával, és így hatással van-e a tervezett adatkezelés jogalapjára [GDPR 6. cikk (4) bek.];
c) amennyiben az új adatkezelés jogalapja a jogos érdek lehet [GDPR 6. cikk (1) bek. f) pont] elkészíti az érdekmérlegelési teszt tervezetét;
d) az adatvédelmi tisztviselő véleményének kikérése után dokumentálja az adatvédelmi hatásvizsgálat el nem végzésének indokait, vagy javaslatot tesz a döntésre jogosultnak az adatvédelmi hatásvizsgálat elvégzésére ; a döntésre jogosult erre vonatkozó pozitív döntése esetén – az informatikáért felelős szakterület adatkezelési megbízottja(i) közreműködésével – elvégzi az adatvédelmi hatásvizsgálatot, elkészíti ennek dokumentumát, és kikéri róla az adatvédelmi tisztviselő, valamint – ha alkalmazható – az érintettek vagy képviselőik véleményét [GDPR 35. cikk (1)-(2) és (9) bekezdés]
e) előterjesztést tesz a döntésre jogosultnak arról, hogy az adatkezelést közös adatkezelésként indokolt-e ellátni, illetve indokolt-e adatfeldolgozót bevonni;
f) javaslatot tesz automatizált döntéshozatali módszer, illetve profilalkotási módszer alkalmazására [GDPR 22. cikk (1) bekezdés];
g) megszövegezi az esetleg szükséges hozzájáruló nyilatkozatot [GDPR 7. cikk (2) bekezdés], továbbá ha közös adatkezelés vagy adatfeldolgozó bevonása miatt szükséges, a megfelelő szerződéses rendelkezéseket;
h) megfogalmazza az új adatkezelésre, vagy a meglévő adatkezelés módosítására, illetve információkkal kiegészíti az adatkezelési tájékoztatót (GDPR 13-14. cikk);
i) az új adatkezelés bevezetéséről szóló döntést követően az informatikáért felelős szakterület közreműködésével gondoskodik az új adatkezelésről szóló új vagy módosított tájékoztatás könnyen hozzáférhető módon való közzétételéről [GDPR 12. cikk (1) bekezdés];
j) az új adatkezelés bevezetéséről szóló döntést követően az Adatkezelési Tevékenységek Nyilvántartásában rögzíti az új adatkezelés adatait, illetve átvezeti a már nyilvántartott adatokban bekövetkezett valamennyi változást [GDPR 30. cikk (1) bekezdés]
k) amennyiben ennek szükségessége felmerül, egyedi esetben előterjesztést tesz a döntésre jogosultnak az érintett vagy harmadik személy létfontosságú érdeke fennállásáról [GDPR 6. cikk (1) bekezdés d) pont, 9. cikk (2) bekezdés d) pont] mint az adatkezelés lehetséges jogcíméről;
l) amennyiben ennek szükségessége felmerül, egyedi esetben előterjesztést tesz a döntésre jogosultnak arról, hogy személyes adatok harmadik országba továbbíthatók-e egyedi ügyekben [GDPR 49. cikk (1) bekezdés];
m) az informatikáért felelős szakterület adatkezelési megbízottja a személyes adatot kezelő rendszer fejlesztése és beszerzése során közreműködik:
   ma) a célhoz kötött adatkezelés és az adattakarékosság elvének megfelelően gyűjtött adatokra vonatkozóan a beépített és alapértelmezett adatvédelem elveinek dokumentált érvényesüléséről;
   mb) annak biztosításában, hogy az adathordozhatóság, adattörlés és adattisztítás célú módosítások szabályozott és dokumentált módon valósuljanak meg;
   mc) annak biztosításában, hogy az adatvédelmi tájékoztatók és nyilatkozatok könnyen elérhetők legyenek bárki számára,
   md) annak biztosításában, hogy az adatkezeléssel kapcsolatos ügyfélrendelkezéseket (pl. hozzájáruló nyilatkozatokat vagy azok visszavonását) visszakereshető formában tárolják;

me) az adatok sértetlenségével, bizalmasságuk megőrzésével és az üzletmenet-folytonossággal kapcsolatos kontrollok (pl. változáskezelés, magas rendelkezésre állás, jogosultságkezelés, adatrejtő eljárások, incidenskezelés támogatása) tervezéskori érvényesítésében, illetve dokumentált meglétében;
mf) az adott adatkezelés különös (az Egyetem Informatikai Biztonsági Szabályzatától eltérő) adatbiztonsági intézkedések meghatározásában; döntések előkészítésében.

(7) Döntésre jogosultnak minősül az személy, aki az Egyetem Szervezeti és Működési Szabályzata szerint az adatkezelés alapjául szolgáló tevékenységgel kapcsolatban döntésre jogosult, illetve – amennyiben a döntés testületi hatáskörbe tartozik – a testületi döntés előkészítéséért felelős.

(8) A döntések, javaslatok véglegesítése előtt ki kell kérni az adatvédelmi tisztviselő véleményét úgy, hogy az adatvédelmi tisztviselőnek legalább 10 munkanapja legyen a vélemény adására.

(9) Az adatvédelmi tisztviselő véleményének kikéréséhez olyan dokumentumokat (leírást) kell benyújtani, amely kellő részletességgel meghatározza az adatkezelés célját, az adatkezelés jogalapját, a kezelendő adatok körét, az adatkezelés egyéb feltételeit, illetve az egyéb döntési javaslatokat.

(10) Az adatvédelmi tisztviselő adatvédelmi jogi támogatást nyújt az adatkezelési megbízott által előkészített, adatkezeléshez kapcsolódó dokumentumok elkészítéséhez, és közreműködik azok véglegesítésében.

(11) A végleges dokumentumok szakmai megfelelőségéért az új adatkezelésért felelős szervezeti egység adatkezelési megbízottja, az adatvédelmi megfelelőségéért az adatvédelmi tisztviselő, az informatikai, információbiztonsági megfelelőségért pedig az informatikáért felelős szakterület tartozik felelősséggel. Abban az esetben, ha bármely szakterület/szervezeti egység eltér a megfogalmazott szakmai, adatvédelmi vagy információbiztonsági állásfoglalásoktól, az eltérésért, illetve a végleges dokumentumért az adatvédelmi tisztviselő vagy az információbiztonsági szakterület semmilyen felelősséggel nem tartozik.

(12) A szervezeti egységek a véleményüket az adatvédelmi tisztviselőnek küldik meg az adatvédelmi tisztviselő által meghatározott határidőben, amely nem lehet kevesebb 5 munkanapnál. A véleményeket az adatvédelmi tisztviselő – szükség esetén az adatkezelési megbízottakkal és a véleményezőkkel való konzultáció után – összesíti és véglegesíti.

(13) Amennyiben az új adatkezelés feltételei kidolgozásában részt vevő adatkezelési megbízottak között véleményeltérés van, illetve a Jogi Osztály vagy az informatikáért felelős szakterület kifogást fogalmaz meg, az adatvédelmi tisztviselő – szükség esetén az adatkezelési megbízottakkal és a véleményezőkkel való konzultáció után – javaslatot tesz a lehetséges megoldásra.

(14) Az adatvédelmi tisztviselő véleményét az új adatkezelés bevezetéséről való döntés alapjául szolgáló előterjesztésben (javaslatban) ismertetni kell. Az adatvédelmi tisztviselő véleményétől való esetleges eltérést az előterjesztésben részletesen meg kell indokolni.

(15) Az új adatkezelésről szóló döntést dokumentálni kell, amelyet az előterjesztéssel együtt kell kezelni. A döntéshozatalt követően a jelen Szabályzatban meghatározottak szerint kell eljárni az új adatkezeléssel kapcsolatban.

8. §
Az adatkezelési megbízott feladatai az adatkezelés során

(1) Az adatkezelés során az adatkezelésért felelős szervezeti egység adatkezelési megbízottja az adatkezelésért felelős szervezeti egység feladatkörébe tartozó kérdésekben:
   a) eltérő utasítás hiányában képviseli az adatkezelőt az adatfeldolgozó vagy közös adatkezelés esetén a többi adatkezelő felé;
   b) figyelemmel kíséri az adatkezelés feltételeinek folyamatos fennállását (beleértve az adatkezelés jogszerűségéhez szükséges tájékoztatások megadását, nyilatkozatok beszerzését, valamint az Infotv. 5. § (5) bekezdése szerinti felülvizsgálatot stb.), és szükség esetén intézkedik (beleértve az intézkedés kezdeményezését is) az adatkezelés feltételeinek módosítására;
   c) szükség esetén összeállítja és napra készen tartja a meglévő adatkezelésekre vonatkozódokumentációt, illetve kezdeményezi belső rendelkezés kiadását, módosítását vagy az adatkezelés megszüntetése esetén annak hatályon kívül helyezését;
   d) amennyiben az adatkezelés az érintett hozzájárulásán alapul, ellenőrzi, hogy az érintett hozzájárulását szabályosan szerezték-e be [GDPR 7. cikk (1) bekezdés];
   e) gondoskodik arról, hogy legalább az érintettel való első kapcsolatfelvételkor felhívják a figyelmét az adatkezelő vagy harmadik személy jogos érdeke, illetve közérdekű feladat vagy közfeladat ellátása jogalapon (ideértve az említett jogalapokon alapuló profilalkotást is) történő adatkezeléssel szembeni tiltakozási jogra, és hogy az erről szóló tájékoztatást egyértelműen és más információtól elkülönítve jelenítsék meg [GDPR 21. cikk (4) bekezdés];
   f) rendszeres időközönként, de legalább évente áttekinti az adatvédelmi hatásvizsgálatban azonosított kockázatok alakulását, szükség esetén dokumentálja, illetve jelzi az adatvédelmi tisztviselőnek az adatkezeléssel járó kockázatok változását és az azok csökkentését célzó intézkedéseket, elvégzi, illetve közreműködik az adatvédelmi hatásvizsgálatok utóellenőrzésében és annak dokumentálásában [GDPR 35. cikk (11) bekezdés].

(2) Az adatkezelés során (informatikai rendszerben kezelt személyes adatok esetén az informatikai rendszer üzemeltetési szakaszában) az informatikáért felelős szakterület adatkezelési megbízottja – a feladatkörébe tartozó kérdésekben – gondoskodik arról, hogy az adatkezelés adatbiztonsági kontrolljainak működtetése az erre vonatkozó szabályozásoknak és az informatikáért felelős szakterület által meghatározott elvárásoknak megfelelően történjék, ezen belül gondoskodva különösen:
   a) a fizikai és logikai hozzáférés-védelem kontrolljairól,
   b) a rendkívüli esemény-kezelési eljárásokról (adatvédelmi incidensek feladatkörükbe tartozó kezelése, kedvezőtlen külső vagy belső behatásokkal szembeni ellenállási képesség biztosítása stb.),
   c) a jogosultságkezelésről és
   d) az adatminőséggel, illetve adatrejtéssel kapcsolatos intézkedések végrehajtásáról.

(3) Amennyiben az adatkezelési tevékenység során szükségessé válik az érintett személyazonosságának vagy bármely más, rá vonatkozó tény (pl. iskolai végzettség) okmánnyal/okirattal való igazolása, akkor az igazolásként bemutatott okmányról és/vagy okiratról kizárólag abban az esetben lehet fénymásolatot készíteni, ha ezt jogszabály kifejezetten elrendeli. Erről szóló jogszabályi rendelkezés hiányában az érintett személyazonosságának vagy bármely más, rá vonatkozó tény igazolása céljából történt okmány- vagy okiratbemutatásról és az Egyetem foglalkoztatottja által történt megtekintésről jegyzőkönyvet kell felvenni.

9.§
Adatkezelés megszüntetésével kapcsolatos feladatok

(1) Amennyiben a kezelt személyes adatokra a továbbiakban nincs szükség (az adatkezelési cél megvalósult vagy a kezelt adatokra vonatkozó megőrzési idő letelt), vagy jogszabályi változások miatt, vagy a Hatóság vagy bíróság döntése értelmében a személyes adatok kezelését meg kell szüntetni, az adatkezelési megbízott – az adatvédelmi tisztviselő és rajta keresztül a Jogi Osztály és az informatikáért felelős szakterület véleményének kikérése után – javaslatot tesz a döntésre jogosultnak:
   a) az adatkezelés egészének vagy egyes adatfajták nyilvántartásának megszüntetésére (a személyes adatok archiválására a megőrzési idő leteltéig),
   b) a nyilvántartás egészének vagy a nyilvántartási rendszerben kezelt egyes adatfajták, illetve a személyes adatok törlésére.

(2) Az Adatkezelés megszüntetése esetén:

   a) az Adatkezelési Tevékenységek Nyilvántartásából az adatkezelést vagy az egyes adatfajtákat törölni kell,
   b) az adatokat
      ba) az informatikai rendszerekben archiválni kell, illetve
      bb) az informatikai rendszerekből törölni kell, a papír alapú nyilvántartásban kezelt adatokat pedig – az Egyetem Iratkezelési Szabályzata szerint – selejtezni kell.

10.§
Az érdekmérlegelési teszt elvégzésének módszertana

(1) Amennyiben az Egyetem valamely adatkezelésének az Egyetem vagy harmadik személy jogos érdeke a jogalapja [GDPR 6. cikk (1) bekezdés f) pont], érdekmérlegelési tesztet kell elvégezni és azt dokumentálni. Jogos érdek az a törvényes, kellően pontosan megfogalmazott, valós és fennálló, illetve elérhető előny, amelyet az adatkezelő származtat – vagy a harmadik személy származtathat – az adatkezelésből.

(2) Az érdekmérlegelési tesztet a tervezett adatkezelésért felelős szervezeti egység adatkezelési megbízottja végzi el. Az érdekmérlegelési tesztet írásba kell foglalni. Az elkészült dokumentumot az adatvédelmi tisztviselőnek kell megküldeni, aki azt szakmai szempontból véleményezi. A jogos érdeken alapuló adatkezelés kizárólag az érdekmérlegelési teszt elvégzését és az adatvédelmi tisztviselő véleményének beszerzését követően kezdhető meg.

(3) Az érdekmérlegelési teszt módszertanát, a megválaszolandó kérdéseket minden esetben a tervezett adatkezelés figyelembevételével kell megválasztani, az alábbi kérdések köre csak orientáló, a tervezett adatkezelés szempontjából releváns egyéb kérdésekkel bővíthető. Abból kell kiindulni, hogy bármilyen adatkezelés beavatkozás az érintett magánszférájába, és e beavatkozás jogosságát, szükségességét és arányosságát kell bizonyítani a mérlegelés során.

(4) Az érdekmérlegelési teszt részei:
   a) a tervezett adatkezelés leírása és az annak keretében kezelni tervezett személyes adatok (körének vagy típusának) meghatározása,
   b) az adatkezelő vagy azon harmadik fél jogos érdekének azonosítása, akinek az adatkezelés érdekében áll (Miért szükséges az adatkezelés?),

c) az érintett érdekeinek, jogainak azonosítása (Arányban van-e az adatkezelés az érintett magánszférájának korlátozásával?),
d) az adatkezelő (vagy harmadik fél) és az érintettek érdekeinek összevetése,
e) a személyes adatok védelme biztosítékainak leírása,
f) az érdekmérlegelési teszt eredménye.

11.§
Az adatvédelmi hatásvizsgálat elvégzésének módszertana

(1) Ha az adatkezelés valamely, különösen az új technológiákat alkalmazó típusa valószínűsíthetően magas kockázattal jár a természetes személyek jogaira nézve, az adatkezelést megelőzően adatvédelmi hatásvizsgálatot kell végezni. Olyan, egymással hasonló típusú adatkezelési műveletek, amelyek egymáshoz hasonló kockázatokkal járnak, egyetlen adatvédelmi hatásvizsgálat (továbbiakban: hatásvizsgálat) keretei között is értékelhetők.

(2) A hatásvizsgálat elvégzésének szükségességéről a tervezett adatkezelésért felelős szervezeti egység adatkezelési megbízottja szükség esetén kikéri az adatvédelmi tisztviselő véleményét.

(3) A hatásvizsgálat elvégzését a tervezett adatkezelésért felelős szervezeti egység adatkezelési megbízottja koordinálja. A hatásvizsgálat megállapításait írásban kell rögzíteni. Az elkészült hatásvizsgálati dokumentációt az adatvédelmi tisztviselőnek kell megküldeni, amely azt 8 munkanapon belül szakmai szempontból véleményezi, és beszerzi az információbiztonsági szakterület véleményét is. Ha az adatkezelési megbízott úgy ítéli meg, hogy az adatkezelés nem jár magas kockázattal a természetes személyek jogaira, úgy ezt meg kell indokolnia és – ha ez lehetséges – dokumentumokkal igazolnia a mellőzés okait. A bevezetendő adatkezelés kizárólag a hatásvizsgálat elvégzését követően kezdhető meg.

(4) Adatvédelmi hatásvizsgálatot a GDPR 35. cikk (3) bekezdésében, illetve a Nemzeti Adatvédelmi és Információszabadság Hatóság által közzétett jegyzékben (**https://www.naih.hu/files/GDPR_35_4_lista_HU_mod.pdf**) szereplő adatkezelések, adatkezelési műveletek esetén kell végezni.

(5) A fenti eseteken túl minden olyan bevezetésre kerülő – különösen az új technológiákat alkalmazó – adatkezelés esetén is hatásvizsgálatot kell végezni, mely adatkezelés az ügyfélre tekintettel jelentős joghatással bír/az ügyfelet (jogait) jelentős mértékben érinti.

(6) A hatásvizsgálat módszertanát minden esetben a tervezett adatkezelés figyelembevételével kell megválasztani. A hatásvizsgálat lefolytatásához szüksége adatvédelmi hatásvizsgálati szoftver („PIA software”) megtalálható a Nemzeti Adatvédelmi és Információszabadság Hatóság honlapján (**https://naih.hu/adatvedelmi-hatasvizsgalati-szoftver.html**).

(7) A hatásvizsgálat első részében összefoglalóan le kell írni a tervezett adatkezelést, különösen:
a) az adatkezelésért felelős szervezeti egységet és a tervezett közös adatkezelő vagy adatfeldolgozó megjelölését;
b) az adatkezelés célját és jogalapját, az adatkezeléstől várt előnyöket, az adatkezelés szükségességét, az adatkezelés terjedelmét (időben és a kezelt adatok volumenében);
c) az adatkezeléssel érintettek körét, a kezelendő adatok körét, az adatok megőrzésének tervezett idejét,

d) azon adatkezelők megjelölését, akiknek az adatot továbbítani tervezik, és különösen, ha harmadik országba vagy nemzetközi szervezet felé tervezik az adattovábbítást (ideértve az adatfeldolgozás céljából történő adatküldést is);
e) az adatkezelésre vonatkozó követelmények (jogszabályi követelmények vagy magatartási kódexből, szabványból eredő követelmények);
f) az adatkezelés folyamatának a leírását.

(8) A hatásvizsgálat második részében ki kell fejteni és meg kell indokolni:
a) az adatkezelés szükségességének és arányosságának biztosítékait,
b) az érintett jogait biztosító garanciák érvényesülését.

(9) A hatásvizsgálat harmadik részében azonosítani és értékelni kell az adatkezelés potenciális kockázatait és a kockázatok enyhítésére tervezett, elfogadott intézkedéseket, megoldásokat.

(10) A hatásvizsgálat negyedik része tartalmazza a tervezett adatkezelés értékelését:
a) a meghatározott szempontok értékelését a tekintetben, hogy azok egyenként megfelelőek, további intézkedésekkel megfelelőek lehetnek, illetve nem megfelelőek;
b) a tervezett kiegészítő intézkedések végrehajtásának ütemtervét;
c) annak egyértelmű rögzítését, hogy a tervezett adatkezelés valószínűsíthetően magas kockázattal jár-e a természetes személyek jogaira nézve és ennek alapján az adatkezelés megkezdhető-e, illetve szükség van-e az adatvédelmi felügyeleti hatósággal való konzultációra.

(11) A hatásvizsgálat megállapításait az adatkezelési tevékenységbe vissza kell csatolni és ennek megfelelően kell kialakítani az adatkezelést.

(12) A hatásvizsgálatot legalább évente, dokumentáltan felül kell vizsgálni, szükség esetén újra el kell végezni.

12. §
Az adatkezelési tevékenység nyilvánossága

(1) Az Egyetem a honlapján egy olyan, „Adatvédelem” nevű aloldalt tart fenn, amely bármely oldalról közvetlenül elérhető. Az „Adatvédelem” oldalon közzé kell tenni:
a) az Egyetem általános adatkezelési tájékoztatóját;
b) az Egyetem egyes adatkezelési tevékenységeihez kapcsolódó különös adatkezelési tájékoztatókat (a munkavállalók, egyéb jogviszonyban foglalkoztatottak adatainak kezelésére vonatkozó tájékoztatók kivételével);
c) közös adatkezelés esetén a közös adatkezelésben résztvevők közötti megállapodás lényegét, ha azt a különös adatkezelési tájékoztatók nem tartalmazzák;
d) tájékoztatást arról, hogy az érintett kihez fordulhat az adatkezelést érintő kérdéseivel, panaszaival (az adatkezelő és az adatvédelmi tisztviselő elérhetősége, a Hatóság elérhetősége);
e) tájékoztatást az elektronikus ügyintézés lehetőségéről és az azzal kapcsolatos információkról (pl. e-Papír szolgáltatás, az Egyetem biztonságos kézbesítési szolgáltatási címe vagy kormányrendeletben meghatározott egyéb típusú elektronikus elérhetősége, azon adatvédelmi beadvány típusok felsorolása, amelyeket az Egyetem az e-Papír szolgáltatás útján is fogad).

(2) Az Egyetem honlapjának olyan aloldalain, amelyek személyes adatok kezelésével járó egyes tevékenységekről tájékoztatnak (pl. egyes képzési formák igénybevételének feltételeit tartalmazzák), el kell helyezni legalább az adott tevékenységhez kapcsolódó
   a) adatkezelési tájékoztatóra mutató hivatkozást;
   b) egyéb releváns dokumentumokat (pl. hallgatóknak szóló tájékoztatókat, formanyomtatványokat).

(3) Az Egyetem szervezeti egységeinek vezetői gondoskodnak arról, hogy a szervezeti egység tevékenységének helyszínein az Egyetem általános adatkezelési tájékoztatóján kívül az adott szervezeti egység tevékenységi körébe tartozó adatkezelésekről szóló különös adatkezelési tájékoztatók kinyomtatott formában is rendelkezésre álljanak.

(4) Az Egyetem kezelésében lévő közérdekű adatok és közérdekből nyilvános adatok közzétételéről, illetve rendelkezésre bocsátásáról külön szabályzat rendelkezik.

13.§
Korlátozottan cselekvőképes személyek tájékoztatáshoz való jogának biztosítása

Az Egyetem szervezeti egységeinek vezetői az adatkezelési megbízottak közreműködésével gondoskodnak arról, hogy az Egyetemmel kapcsolatba kerülő, korlátozottan cselekvőképes személyek törvényes képviselői, illetve – állapotuktól függően – a korlátozottan cselekvőképes személyek is megfelelő tájékoztatást kapjanak a személyes adatok kezeléséről. A törvényes képviselőt írásban nyilatkoztatni kell, hogy az adatkezelésre vonatkozó tájékoztatást közli a gondnoksága alatt álló érintettel.

14. §
Korlátozottan cselekvőképes személyek személyes adatainak kezelése hozzájáruló nyilatkozat alapján

(1) Az Egyetem szervezeti egységeinek vezetői az adatkezelési megbízottak közreműködésével gondoskodnak arról, hogy az Egyetemmel kapcsolatba kerülő korlátozottan cselekvőképes személyek tekintetében – amennyiben az adatkezelés az érintett hozzájárulásán alapul – a személyes adatok kezeléséhez való hozzájárulást törvényes képviselőjük adja meg.

(2) A hozzájáruló nyilatkozatnak tartalmaznia kell a törvényes képviselőnek arra vonatkozó nyilatkozatát, hogy jogosult az érintett helyett a jognyilatkozat megtételére.

(3) Amennyiben az érintett törvényes képviselői (pl.: szülői felügyelet gyakorlására jogosult szülők) egymástól eltérő nyilatkozatot tesznek az adatkezeléshez való hozzájárulásról, úgy az adatkezeléshez való hozzájárulást meg nem adottnak kell tekinteni.

15.§
Az adatvédelmi beadványok típusai

(1) Az érintettől a következő, személyes adatai Egyetem általi kezelését érintő beadványok érkezhetnek:
   a) bejelentheti az Egyetem által nyilvántartott adatok megváltozását;
   b) tájékoztatást kérhet személyes adatai kezeléséről (milyen személyes adato(ka)t, milyen célból, milyen jogalapon, milyen forrásból szerezve, meddig kezeli az Egyetem, alkalmaz-e

automatizált döntéshozatalt és/vagy profilalkotást az adatkezelés során, a személyes adatokat kinek, milyen jogalapon továbbítja) – hozzáféréshez való jog (GDPR 15. cikk);

c) kérheti a pontatlanul vagy hiányosan nyilvántartott személyes adatai helyesbítését, illetve vitathatja a nyilvántartott személyes adatok pontosságát – helyesbítéshez való jog (GDPR 16. cikk);
d) kérheti a nyilvántartott személyes adatai törlését – törléshez való jog (GDPR 17. cikk);
e) kérheti a személyes adatai kezelésének korlátozását (a pontatlan adat helyesbítéséig terjedő időre; a jogellenesen kezelt személyes adatok törlése helyett; jogszerűen kezelt, de szükségtelenné vált adatok törlése helyett az érintett kérésére az érintett jogi igényének előterjesztéséhez, érvényesítéséhez vagy védelméhez; jogos érdeken alapuló adatkezelés elleni tiltakozás elbírálásáig) – az adatkezelés korlátozásához való jog (GDPR 18. cikk);
f) kérheti, hogy a rá vonatkozó, általa az Egyetem rendelkezésére bocsátott és elektronikus adatbázisban a hozzájárulása, a személyes adatok különleges kategóriái esetén a kifejezett hozzájárulása, vagy a vele kötött szerződés teljesítése jogalappal, automatizált módon kezelt adatait tagolt, széles körben használt, géppel olvasható formátumban megkapja – adathordozhatósághoz való jog (GDPR 20. cikk);
g) tiltakozhat a személyes adatai kezelése ellen, ha az adatkezelés jogalapja az adatkezelő vagy harmadik személy jogos érdeke, illetve közérdekű feladat vagy közfeladat ellátása, beleértve mindkét esetben a profilalkotást is – tiltakozási jog gyakorlása (GDPR 21. cikk);
h) automatizált döntéshozatal alkalmazása esetén az adatkezelő részéről emberi beavatkozást kérhet, közölheti álláspontját (GDPR 22. cikk (3) bekezdés);
i) kifogást nyújthat be az automatizált döntéshozatal alkalmazásával meghozott döntéssel szemben (GDPR 22. cikk (3) bekezdés);
j) panaszt nyújthat be a személyes adatok kezelését, illetve a GDPR szerinti jogai gyakorlását érintően (GDPR 77. cikk, 38. cikk (4) bekezdés);
k) az elhunyt érintett életében tett meghatalmazottjaként vagy közeli hozzátartozójaként gyakorolni kívánja az érintett egyes jogait (Infotv. 25. §).

16. §
Az adatvédelmi beadványokkal kapcsolatos ügyintézés

(1) Az egyes belső szabályzatoknak az érintettek adatainak felvételére, módosítására vagy helyesbítésére, illetve törlésére vonatkozó rendelkezései alkalmazását jelen Szabályzat nem érinti, az adatvédelmi tisztviselő azonban bármely esetben – az érintett beadványának kivizsgálása, illetve saját ellenőrzése eredményeként, továbbá a Hatóság vagy bíróság döntése végrehajtásaként – az említett szabályzatokban meghatározott hatásköri és eljárási rendtől függetlenül kezdeményezheti személyes adat helyesbítését, törlését vagy az adatkezelés korlátozását (az adatok zárolását).

(2) Az Egyetemhez érkező beadványokat esetről esetre és a beadvány tárgyával összefüggő adatkezelési tevékenység figyelembevételével kell megítélni, továbbá az Egyetem Panaszkezelési Tájékoztatóban foglaltaknak megfelelően kell – a GDPR 12. cikkében írt határidők figyelembevételével – elintézni, az alábbi kiegészítésekkel és eltérésekkel:

a) a beadvány érkezése dátumát és időpontját pontosan rögzíteni kell;
b) a Szabályzat 16. § (1) bekezdés j) alpontban meghatározott panasz kivizsgálását az adatvédelmi tisztviselő végzi. A panasz kivizsgálása során az érintett szervezeti egységek kötelesek az adatvédelmi tisztviselővel együttműködni. A személyes adatok kezelését, illetve a GDPR szerinti jogok gyakorlását érintő panasz megalapozottsága esetén az adatvédelmi tisztviselő az

adatkezelésért felelős szervezeti egység(ek)nél intézkedést kezdeményez a panasz kiváltó okainak orvoslására, az érintett folyamatok felülvizsgálatára, valamint – szükség esetén – a személyi felelősség megállapítására,

c) az Egyetem bármely beadvány esetén kérheti az adatvédelmi tisztviselő véleményét a tekintetben, hogy az érintett kérte-e az adatkezelés korlátozását (zárolás, GDPR 18. cikk), és kérés esetén az adatvédelmi tisztviselő – az informatikáért felelős szakterület útján – intézkedik annak az informatikai rendszerekben történő megvalósításáról. Az adatkezelés korlátozásának (zárolásának) feloldásáról az adatvédelmi tisztviselő külön tájékoztatja az érintett informatikai rendszer(eke)t üzemeltető szervezet egység(ek)et,
d) az adatvédelmi tisztviselő dönt abban a kérdésben, hogy a beadvány egyértelműen megalapozatlan vagy túlzó-e,
e) az érintettnek saját adatai kezeléséről akár szóbeli (pl. telefonon történő), akár személyes megjelenés nélküli (pl. elektronikus levélben kért) tájékoztatás csak egyértelmű személyazonosítás után adható . Amennyiben a tájékoztatást kérő (beadványt előterjesztő) nem azonosítható, vagy kétség merül fel a beadványt előterjesztő személyazonosságát illetően, meg kell kísérelni a beadványt előterjesztő személyének azonosítását, beleértve a személyes megjelenés igénylését, vagy az e-Papír szolgáltatás igénybevételének ajánlását. Ilyen esetekben a GDPR 12. cikk (3) bekezdése szerinti határidő a beadványt előterjesztő sikeres azonosításakor kezdődik;
f) amennyiben a beadvány a GDPR hatálya alá tartozó beadványnak minősül, a beadványt előterjesztő a beadvány érkezését követő 8 napon belül értesíteni kell a beadvány érkezéséről, a megválaszolására nyitva álló határidőről, illetve arról, hol kaphat további felvilágosítást a beadványáról. Nem kell ilyen értesítést küldeni a beadványt előterjesztőnek, ha a beadványban kért intézkedést ezen időn belül teljesítik;
g) amennyiben a beadványt előreláthatóan nem lehet a GDPR 12. cikk (3) bekezdése szerinti határidőben megválaszolni, a beadványt előterjesztőt legkésőbb a beadvány érkezését követő 21. napon elküldött levélben vagy elektronikus üzenetben tájékoztatni kell a határidő meghosszabbításának szükségességéről, okairól és az új határidőről;
h) amennyiben a beadványt –a beadványt előterjesztő kérelme ellenére – nem lehet, vagy nem célszerű elektronikus úton megválaszolni (a kért dokumentumokat nem lehet vagy nem célszerű ilyen úton elküldeni), fel kell venni a kapcsolatot a beadványt előterjesztővel annak érdekében, hogy kölcsönösen elfogadható megoldást találjanak. Különösen indokolt a beadványt előterjesztővel a kapcsolatfelvétel, ha a beadványt előterjesztő különleges adat megküldését kéri nem biztonságos elektronikus úton. A kapcsolatfelvételre olyan időben kell sort keríteni, hogy a beadványt akkor is meg lehessen válaszolni a határidő betartásával, ha a beadványt előterjesztő ragaszkodik a nem biztonságos elektronikus úthoz vagy még nincs ügyfélkapu regisztrációja;
i) elektronikus úton személyes adat úgy küldhető, ha az adatok bizalmassága, integritása és rendelkezésre állása biztosítható (pl. jelszavas védelemmel ellátott titkosított állomány vagy hivatkozás küldése egy jelszóval védett tárhelyre) és a jelszót külön csatornán küldik el;
j) elektronikus úton titkosítás nélkül személyes adat csak a beadványt előterjesztő kifejezett kérésére vagy beleegyezésével és csak oly módon küldhető, ha előzőleg a beadványt előterjesztő figyelmét felhívták a kockázatokra, és a beadványt előterjesztő ezek után megerősíti a szándékát, egyúttal tudomásul véve az Egyetem felelősségkizáró nyilatkozatát, továbbá az
k) az Egyetem szervezeti egységei készített válaszlevél-tervezetét jóváhagyás végett bemutatják az adatvédelmi tisztviselőnek;
l) a beadvány határidőben megválaszoltnak minősül, ha a válaszadásra köteles szervezeti egység a választ a határidő utolsó napján postára adja vagy elektronikus üzenetet küld a beadványt előterjesztő a megtett intézkedésekről.

(3) Amennyiben az adott adatkezelési tevékenységről szóló belső szabályozás – figyelemmel az adatkezelés tárgyára – másként nem rendelkezik, a személyazonosítás
   a) személyes megjelenés során a személyazonosságot igazoló okmány (pl. személyazonosító igazolvány, útlevél) bemutatásával,
   b) személyes megjelenés hiányában pedig a természetes személyazonosító adatok (név, születési hely és idő, anyja neve), valamint legalább egy olyan adat (pl. Neptun kód) megadásával történik, amelyet mind az érintett, mind az Egyetem ismerhet, illetéktelen személy számára azonban nem hozzáférhető.

(4) A személyazonosítás során az Egyetem személyazonosítást végző munkavállalója köteles meggyőződni arról, hogy az érintett által bemutatott okmány adatai, vagy az érintett adatai azonosake az Egyetem nyilvántartásában szereplő adatokkal. A személyazonosítás elvégzéséről jegyzőkönyvet kell felvenni. Amennyiben a személyazonosítás nem egyértelmű (az érintett által bemutatott okmány vagy a személyes megjelenés nélkül megadott adatai és az Egyetem által nyilvántartott adatok között eltérés van), a beadvány elintézése mindaddig nem folytatható, amíg az érintett hitelt érdemlően nem igazolta magát.

(5) Ha az Egyetem rendelkezik biztonságos kézbesítési szolgáltatási címmel, akkor az általános célú elektronikus kérelem űrlap (e-Papír) szolgáltatás igénybevételével az Egyetemnek címzett adatvédelmi beadvány feladója azonosítottnak tekintendő, részére (értesítési tárhelyére) a válasz elektronikus úton megküldhető.

(6) Az adatvédelmi beadványokról olyan ügyiratnyilvántartást kell vezetni, amely segítségével bármikor egyértelműen azonosíthatók a beadványok, nyomon követhetők a beadványok elintézése során tett intézkedések, és a rendelkezésre álló adatokból bármikor statisztika készíthető a következő szempontok szerint:
   a) adott időszakban érkezett beadványok száma, típus szerinti bontásban is;
   b) a beadványok beérkezésének módja;
   c) a beadványok megválaszolásának átlagos időtartama;
   d) az elutasított beadványok száma, és azok okai;
   e) a válaszadás módja.

17. §
Más szervtől érkező megkeresés teljesítése, adattovábbítás

(1) Az Egyetem adatkezelőként dönt a más szervtől (minisztérium, nyomozó hatóság stb.) érkező, személyes adat vagy személyes adatot tartalmazó tárgy (pl. biztonsági kamera felvétele) szolgáltatását kérő megkeresések (a továbbiakban együtt: megkeresés) teljesítéséről. A megkeresés teljesítése előtt esetről esetre mérlegelni kell, hogy az adatkérés teljesítése kötelező (jogszabály írja elő) vagy mérlegelhető (jogos érdeken alapul), továbbá, hogy a megkeresés és a teljesítése megfelel-e a jogszabályi feltételeknek (az arra jogosult küldte-e a megkeresést, az Egyetemnek van-e jogalapja az adattovábbításhoz, a megkeresésben szereplő információk teljesek-e és elegendőek-e a megkeresés teljesítéséhez stb.).

(2) A megkeresésre adandó válasz összeállítása során törekedni kell arra, hogy kizárólag a megkeresés teljesítéséhez (az adatkérés céljához) elengedhetetlenül szükséges személyes adatok átadása valósuljon meg.

(3) A nem jogszerű adatkérés teljesítését el kell utasítani. Nem jogszerű a megkeresés, ha a tartalmi vagy alaki feltételek legalább egyike (pl. az adatkérés jogalapja) hiányzik vagy helytelen. Az elutasítással egyidejűleg a hiányzó/helytelen információk pótlását/javítását kell kérni a megkereső szervtől, amennyiben az Egyetem részéről a megkeresés teljesítése jogi kötelezettségen vagy jogos érdeken alapulhat. Ha az Egyetem részéről nincs helye az adatátadásnak sem jogi kötelezettség, sem jogos érdek alapján, a jogszerű megkeresést is el kell utasítani.

(4) Jogszerű az adatkérés, ha megfelel a tartalmi és alaki feltételeknek, azaz tartalmazza az alábbi információkat:
   a) megkereső szerv pontos megnevezése;
   b) a megkeresés azonosító adatai (pl. iktatószáma, megkeresés alapját képező eljárás száma);
   c) az adatkérés jogalapja (pl. jogszabály és jogszabályhely megjelölése) és feltételei,
   d) az adatkérés célja,
   e) az adatkérés teljesítéséhez, illetve az adatszolgáltatás tárgyának azonosításához szükséges adatok (pl. az érintett személy, tárgy vagy szolgáltatás adatai);
   f) a szolgáltatandó adatok köre és;
   g) az adatszolgáltatás teljesítésének módja és határideje.

(5) A nyomozó hatóság személyes adatot, illetve azt tartalmazó tárgyat (pl. irat, filmfelvétel) akkor foglalhat le, ha erről lefoglalási határozatot mutat be. A lefoglalási határozat teljesítését – a törvényesség érdekében – a Jogi Osztály közreműködésével kell végrehajtani. A lefoglalási határozatnak minimálisan az alábbi információkat kell tartalmaznia:
   a) a megkereső nyomozó hatóság pontos megnevezése;
   b) a büntetőeljárás száma;
   c) a lefoglalás tárgya.

(6) A szabálysértési eljárást folytató hatóság nem jogosult személyes adatot vagy azt tartalmazó tárgyat (pl. irat, filmfelvétel) lefoglalni.

(7) A jogos érdek alapján történő adatátadás csak érdekmérlegelést követően lehetséges. Az érdekmérlegelés keretében vizsgálni kell a büntető- vagy a szabálysértési eljárás sikeres lefolytatásához fűződő érdeket, amelyet szembe kell állítani az érintett adatvédelmi jogaival. Kizárólag abban az esetben lehet jogszerű az adatátadás, amennyiben a nyomozó vagy a szabálysértési eljárást folytató hatóság pontosan megjelöli az adatkérés célját és a kért adatkört, mivel ezek feltételei az érdekmérlegelés elvégzésének.

18.§
Az adatbiztonsági intézkedések (technikai és szervezési intézkedések) meghatározása és végrehajtása

(1) Az adatbiztonsági szabályok kialakítása során különös gondot kell fordítani a beépített és az alapértelmezett adatvédelem elveinek (GDPR 25. cikk) betartására, valamint arra, hogy az Egyetem által alkalmazott adatbiztonsági intézkedések megfeleljenek a GDPR 32. cikkében írt követelményeknek.

(2) Az Egyetem működése során betartandó adatbiztonsági szabályokat (GDPR 32. cikk) külön szabályzatok tartalmazzák, így különösen a mindenkor hatályos:

a) Informatikai Biztonsági Szabályzat,
b) Hozzáférésvédelmi Szabályzat,
c) Felhasználói Szabályzat,
d) Incidenskezelési Szabályzat,
e) Kamera Szabályzat,
f) Közérdekű Adatkezelésről szóló Szabályzat,
g) Iratkezelési Szabályzat, illetve
h) általános biztonsági előírásokat tartalmazó szabályzatok.

(3) Az adatbiztonsági szabályok tervezetének kialakításába – a véleményezésre vonatkozó egyéb szabályokat nem érintve – az adatvédelmi tisztviselőt be kell vonni.

(4) Az adatbiztonsági intézkedéseket érintően az adatkezelésért felelős szervezeti egység adatkezelési megbízottja:
a) a szakterületére vonatkozó információk szolgáltatásával közreműködik az érintett informatikai elemek védelmi osztályokba sorolásában;
b) a szakterületére vonatkozó információk szolgáltatásával közreműködik az adatkezelés biztonságát fenyegető kockázatok felmérésében és meghatározásában;
c) az informatikai rendszert üzemeltető szervezeti egységgel együttműködve közreműködik azon információbiztonságot érintő feladatok végrehajtásában, amelyek az adatbiztonsági követelmények megvalósulásához szükségesek;
d) figyelemmel kíséri a belső adatvédelmi szabályok érvényre juttatását a szakterületen belül, felhívja a szakterületen dolgozók figyelmét a szabályok betartására, jelzi a szabályok megsértését az érintett munkavállaló felettesének, közreműködik a szakterületen dolgozók adatvédelmi tudatosságának növelésében.

(5) Az adatbiztonság elveinek egy adatkezelés bevezetésének vagy személyes adatkezelést és/vagy -feldolgozást eredményező módosításának előkészítése során történő érvényesítése az informatikáért felelős szakterület adatkezelési megbízottjának (megbízottjainak) feladata, aki(ke)t az adatkezelési tevékenységet támogató nyilvántartási rendszerek fejlesztésének, módosításának folyamatába kötelezően be kell vonni.

(6) Az adatbiztonsági intézkedések mindennapi működés során történő betartására az Egyetem minden munkavállalója, valamint az Egyetem informatikai rendszereihez hozzáférő személy köteles.

(7) A jelen Szabályzat személyi hatálya alá tartozó személyek kötelesek a személyes adatokat tartalmazó, papíralapon kezelt iratokat a munkavégzés befejezését követően zárt szekrényben, fiókban tárolni. Ahol a tárolás előbb nevesített feltételei nem adottak, az irodahelyiség ajtajának kulcsra zárásával kell a személyes adatok védelmét biztosítani abban az esetben, ha az irodahelyiségben senki sem tartózkodik.

19.§
Közös adatkezelés

(1) Közös adatkezelésnek minősül, ha az adatkezelés céljait és eszközeit az Egyetem egy vagy több másik adatkezelővel közösen határozza meg (GDPR 26. cikk).

(2) A közös adatkezelésről szóló megállapodásban meg kell határozni különösen:

a) az adatkezelés célját, a kezelendő adatok körét, az adatkezelés időtartamát, az alkalmazandó adatbiztonsági intézkedéseket, az adatkezelés egyéb feltételeit,
b) azt, hogy a közös adatkezelésben érintett egyes adatkezelők:
ba) mely adatkezelési műveleteket (pl. hozzájáruló nyilatkozatok felvétele, adatok tárolása, adatok felhasználása stb.) végzik,
bb) az érintett tájékoztatását hogyan végzik (pl. melyik adatkezelő készíti el az adatkezelési tájékoztatót és bocsátja az érintettek rendelkezésére stb.),
bc) az érintett jogai gyakorlását hogyan biztosítják (pl. egyesített vagy elkülönített ügyfélszolgálat stb.),
bd) az esetleges jogellenes adatkezelés következményeit milyen arányban viselik;
c) az adatvédelmi incidens észlelése esetén követendő eljárást, különösen azt, hogy
ca) az adatvédelmi incidens tudomásra jutása esetén a másik adatkezelő adatvédelmi tisztviselőjét (adatvédelmi tisztviselő hiányában a kijelölt kapcsolattartót) haladéktalanul kötelesek értesíteni az adatvédelmi rendellenességről vagy incidensről,
cb) egymással kötelesek együttműködni az adatvédelmi rendellenesség vagy incidens okának kiderítésében és következményeinek felszámolásában,
d) az egyes adatkezelőket mely adatvédelmi incidensek tekintetében terheli a bejelentési kötelezettség;
e) kijelölnek-e kapcsolattartót az érintettek számára, és ha igen, a kapcsolattartó személyét és elérhetőségét naprakészen kell tartani,
f) a megállapodásról az érintett rendelkezésére bocsátandó összefoglalót, aminek – a GDPR 13-14. cikkeiben írtakon túl – tartalmaznia kell az adatkezelők által végzett adatkezelési műveleteket, és azt, hogy az érintett hogyan gyakorolhatja jogait a közös adatkezelés tekintetében.

(3) A közös adatkezelés szükségességét az adatkezelési megbízott az adatkezelés bevezetéséről való döntés előkészítése részeként vizsgálja meg. Ezt a szabályt kell alkalmazni akkor is, ha a közös adatkezelésről az adatkezelés folyamán születik döntés.

(4) Amennyiben a közös adatkezelésben érintett másik adatkezelő harmadik országbeli adatkezelő, először abban a kérdésben kell dönteni, hogy a harmadik országbeli adatkezelő képes-e a GDPR-nak megfelelő adatbiztonsági követelmények teljesítésére. Amennyiben a harmadik országbeli adatkezelő nem képes a GDPR által elvárt adatbiztonsági követelmények érvényesítésére, illetve nem tud a GDPR szerinti garanciákat nyújtani a személyes adatok kezelésére, az adatkezelővel nem köthető megállapodás közös adatkezelésre.

(5) Amennyiben döntés születik a közös adatkezelésről, az illetékes adatkezelési megbízott(ak) az adatvédelmi jogi megfelelőség biztosítása tekintetében az adatvédelmi tisztviselő, az egyéb jogszabályi követelményeknek való megfelelés szerződéses biztosítása tekintetében a Jogi Osztály közreműködésével, továbbá az informatikáért felelős szakterület véleményének kikérésével előkészíti a közös adatkezelésről szóló megállapodás tervezetét (benne a közös adatkezelőknek az érintettek számára kijelölendő kapcsolattartójának kijelölésével kapcsolatos döntést, valamint a közös adatkezelésre vonatkozó megállapodásnak az érintettek rendelkezésére bocsátható lényegi elemeit), és azt felterjeszti a szerződés megkötésére jogosult személynek.

(6) A szerződés megkötésére jogosult személy az, aki az Egyetem Szervezeti és Működési Szabályzata szerint az vonatkozó adatkezelés alapjául szolgáló tevékenységgel kapcsolatban döntésre jogosult,

illetve – amennyiben a döntés testületi hatáskörbe tartozik – a testületi döntés előkészítéséért felelős. E szabály nem érinti az együttes aláírásra vonatkozó szabályokat.

(7) Az adatkezelési megbízott a közös adatkezelői megállapodás megkötését követően – az adatkezelési tevékenységek nyilvántartására vonatkozó szabályok szerint – e tényt és a további adatkezelő(k) adatait (név és cím, kapcsolattartó neve és elérhetősége) rögzíti az Adatkezelési Tevékenységek Nyilvántartásában.

20.§
Adatfeldolgozói szerződések

(1) Amennyiben harmadik országbeli adatfeldolgozó igénybevétele merül fel, először abban a kérdésben kell dönteni, hogy a harmadik országbeli adatfeldolgozó képes-e a GDPR-nak megfelelő adatbiztonsági követelmények teljesítésére. Amennyiben a harmadik országbeli adatfeldolgozó nem képes a GDPR által elvárt adatbiztonsági követelmények érvényesítésére, illetve nem tud a GDPR szerinti garanciákat nyújtani a személyes adatok kezelésére, az adatfeldolgozóval nem köthető szerződés.

(2) Adatfeldolgozó igénybevétele esetén az adatfeldolgozóval kötendő szerződésnek tartalmaznia kell a GDPR 28. cikk (1)-(4) bekezdésében foglalt tartalmi elemeket a jelen Szabályzatban foglalt kiegészítések és pontosítások szerint.

(3) Az adatfeldolgozóval kötendő szerződésben
   a) kellő részletességgel (pl. szabályzatra vagy szabványokra utalással) meg kell határozni az adatfeldolgozó, vagy az adatfeldolgozó által igénybe veendő további adatfeldolgozó (al-adatfeldolgozó) által betartandó adatbiztonsági szabályokat, amelyek nem lehetnek kevésbé szigorúak, mint az Egyetem által alkalmazott adatbiztonsági intézkedések, valamint az adatfeldolgozónak az adatbiztonsági intézkedések végrehajtásával kapcsolatos feladatait;
   b) rögzíteni kell az adatfeldolgozónak az érintettől származó kérelmek, panaszok megválaszolásában való közreműködésének eljárásrendjét;
   c) rögzíteni kell az adatfeldolgozó kötelezettségeit adatvédelmi incidens észlelése esetén, így különösen az adatvédelmi incidens tudomásra jutása esetén az Egyetem adatvédelmi tisztviselőjét haladéktalanul köteles értesíteni az adatvédelmi incidensről,
   d) köteles együttműködni az Egyetem adatvédelmi tisztviselőjével és más közreműködő szervezeti egységgel az adatvédelmi incidens okának feltárásban és következményeinek felszámolásában,
   e) köteles együttműködni az adatvédelmi incidens bejelentésének teljesítésében,
   f) rögzíteni kell az adatfeldolgozó kötelezettségét az adatvédelmi hatásvizsgálat elvégzésében, illetve a hatásvizsgálatban azonosított kockázatok alakulásának figyelemmel kísérésében, az adatkezeléssel járó kockázatok változásának jelzésében, illetve az adatvédelmi hatásvizsgálatok utóellenőrzésben.

(4) Az adatfeldolgozó igénybevételének szükségességét az adatkezelési megbízott az adatkezelés bevezetéséről való döntés előkészítése részeként vizsgálja meg. Ezt a szabályt kell alkalmazni akkor is, ha az adatfeldolgozó igénybevételéről az adatkezelés folyamán születik döntés.

(5) Az adatbiztonsági intézkedések technikai megfelelőségének megítélése az informatikáért felelős szakterület hatáskörébe tartozik, beleértve azt is, hogy az adatfeldolgozó által egy magatartási

kódexhez vagy tanúsítási mechanizmushoz való csatlakozás elegendő garanciát jelent-e az adatbiztonsági szabályok megfelelőségére.

(6) Amennyiben döntés születik az adatfeldolgozó igénybevételéről, az adatkezelési megbízott az adatvédelmi jog megfelelőségének biztosítása tekintetében az adatvédelmi tisztviselő, az egyéb jogszabályi követelményeknek való megfelelés szerződéses biztosítása tekintetében a Jogi Osztály közreműködésével, továbbá az informatikáért felelős szakterület véleményének kikérésével előkészíti az adatfeldolgozóval kötendő szerződés tervezetét, és azt felterjeszti a szerződés megkötésére a jogosult személynek.

(7) Az adatkezelési megbízott az adatfeldolgozói szerződés megkötését követően – az adatkezelési tevékenységek nyilvántartására vonatkozó szabályok szerint – az adatfeldolgozó adatait (név és cím, kapcsolattartó neve és elérhetősége) rögzíti az Adatkezelési Nyilvántartásban.

(8) A jelen Szabályzat rendelkezéseit al-adatfeldolgozó igénybevétele esetén is megfelelően alkalmazni kell azzal, hogy az al-adatfeldolgozó igénybevételére vonatkozó hozzájáruló nyilatkozatnak az adatfeldolgozói szerződés megkötésre jogosult személy általi kiadása előtt az adatkezelési megbízott kikéri az adatvédelmi tisztviselő és rajta keresztül a Jogi Osztály, továbbá az informatikáért felelős szakterület véleményét is.

21.§
Az adatkezelési tevékenységek nyilvántartása

(1) Az Egyetem adatkezelői feladatainak segítése keretében az adatvédelmi tisztviselő – az adatkezelési megbízottak közreműködésével – vezeti az adatkezelési tevékenységek nyilvántartását (Adatkezelési Tevékenységek Nyilvántartása). Az Adatkezelési Tevékenységek Nyilvántartása valamennyi, az Egyetem általi adatkezelés esetén tartalmazza:

a) az adatkezelés célját,
b) az adatkezelés jogalapját,
c) az érintettek körét,
d) az érintettekre vonatkozó személyes adatok kategóriáit,
e) az adatok forrását (opcionális),
f) az adatok kezelésének időtartamát vagy az adattörlés ideje megállapításának szempontjait;
g) a továbbított adatok fajtáját, címzettjét és a továbbítás jogalapját, ideértve a harmadik országokba irányuló, valamint nemzetközi szervezethez történő adattovábbításokat és azok garanciáinak leírását is,
h) az adatfeldolgozó nevét és címét, a tényleges adatkezelés, illetve az adatfeldolgozás helyét és az adatfeldolgozónak az adatkezeléssel összefüggő tevékenységét,
i) az alkalmazott automatizált döntéshozatali logikákat (opcionális);
j) az adatkezelő, valamint közös adatkezelés esetén a közös adatkezelők megnevezését és elérhetőségét,
k) az adatkezelésért felelős szervezeti egység megnevezését és az adatkezelési megbízott nevét,
l) az adatvédelmi tisztviselő nevét és elérhetőségét,
m) az adatkezelés módszerét (manuális, számítógépes, vegyes),
n) ha lehetséges, az adatbiztonsági intézkedések általános leírását,
o) az archiválás módját, gyakoriságát (opcionális),
p) az érdekmérlegelési teszt és a hatásvizsgálati dokumentum elkészültének tényét.

(2) Az Adatkezelési Tevékenységek Nyilvántartása célja az Egyetem, mint adatkezelő adatkezelési tevékenysége átláthatóságának biztosítása, és ezzel az esetleges felesleges, párhuzamos adatkezelések elkerülése.

(3) Az Egyetem adatvédelmi tisztviselője az Adatkezelési Tevékenységek Nyilvántartásába való betekintést – a Hatóság képviselőin kívül – az Egyetem érintett szakterületei, továbbá a közös adatkezelést érintő rész tekintetében a közös adatkezelő részére biztosítja.

(4) A nyilvántartási célú adatállományt kezelő szervezeti egység vezetője az új adatállomány kialakítását a tevékenység megkezdése előtt 5 munkanappal bejelenti az adatvédelmi tisztviselőnek, aki azt Adatkezelési Tevékenységek Nyilvántartásába bejegyzi.

(5) Az Adatkezelési Tevékenységek Nyilvántartásába bejelentett adatok változását, vagy az adatkezelés megszűnését az adatkezelésért felelős szervezeti egység vezetője 5 munkanapon belül köteles bejelenteni az adatvédelmi tisztviselőnek, aki ennek megfelelően módosítja az Adatkezelési Tevékenységek Nyilvántartása adatait.

(6) Az Adatkezelési Tevékenységek Nyilvántartásával összefüggésben az adatvédelmi tisztviselő:

a) biztosítja, hogy az adatkezelések bevezetését megelőző döntéselőkészítés során az érintett szakterületek az Adatkezelési Tevékenységek Nyilvántartása adatait megismerhessék a felesleges, párhuzamos adatkezelések elkerülése, illetve az új adatkezelésnek a meglévő adatkezelésekhez való illeszkedése érdekében;
b) ellenőrzi az adatkezelések, közös adatkezelők, illetve adatfeldolgozók adatainak az Adatkezelési Tevékenységek Nyilvántartásába történő rögzítését, és jelzi az adatkezelésért felelős szervezeti egység vezetőjének a hiányos, hibás vagy valószínűleg megváltozott adatokat, információkat;
c) a Jogi Osztállyal együttműködve figyelemmel kíséri az adatkezelést érintő jogszabályok változását és a szükséges módosításokra felhívja az adatkezelési megbízottak figyelmét;
d) a Hatóság megkeresésére adatot szolgáltat az Adatkezelési Tevékenységek Nyilvántartásából.

22.§
Az adatvédelmi incidensek (rendkívüli esemény) bejelentése és kezelése

(1) Az a munkavállaló, aki az Egyetem által kezelt vagy feldolgozott személyes adatokkal kapcsolatban, vagy az Egyetem szerződéses partnere által kezelt vagy feldolgozott személyes adataival kapcsolatban rendkívüli eseményt (adatvédelmi incidenst vagy annak gyanúját) észleli, köteles azt haladéktalanul bejelenteni az adatvedelem@szfe.hu e-mail címen. A bejelentést az Egyetem Incidenskezelési Szabályzata szerinti, kitöltött űrlap megküldésével kell teljesíteni. Az előbbieken túli, egyéb bejelentő az Egyetem elektronikus elérhetőségén jelentheti be a rendkívüli eseményt, illetve az adatvédelmi incidenst vagy annak gyanúját.

(2) Amennyiben az adatvédelmi incidens bejelentése szóban (telefonon vagy személyesen) történik (beleértve az Egyetem telefonos elérhetőségein tett közérdekű bejelentéseket is), azt a szóbeli közlést követő legfeljebb 1 naptári napon belül írásban is meg kell erősíteni. Ilyen esetben a szóbeli közlés időpontját külön fel kell tüntetni.

(3) Ha a rendkívüli esemény felveti az adatvédelmi incidens gyanúját, akkor a bejelentésben ismertetni kell az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az adatvédelmi incidenssel érintett személyes adatok kategóriáit és hozzávetőleges számát, továbbá a bejelentő nevét és elérhetőségét.

(4) A rendkívüli esemény bejelentésével egyidejűleg meg kell tenni azokat a szükséges és haladéktalan intézkedéseket, amelyek a rendkívüli esemény jellegéből következnek (pl. áramtalanítás, katasztrófaelhárítók értesítése, terheléses támadás blokkolása), s a káros jelenség megszakítását, a lehetséges károk csökkentését célozzák. A haladéktalan intézkedéseket lehetőleg úgy kell megtenni, hogy a rendkívüli esemény kivizsgálásához szükséges bizonyítékok megmaradjanak.

23. §
Incidensprotokoll

(1) A rendkívüli eseményt az Egyetem Incidenskezelési Szabályzata szerinti előzetes kivizsgálás keretében kategóriába kell sorolni (adatvédelmi incidens, információbiztonsági incidens, általános biztonsági incidens).

(2) A Hatóságnak történő bejelentés határidejének számítása szempontjából az adatvédelmi incidensről tudomásszerzés időpontja az az időpont, amikor a rendkívüli eseményt az incidensvizsgáló bizottság adatvédelmi incidens kategóriába sorolja.

(3) Az Egyetem Incidenskezelési Szabályzata alapján végzett előzetes, illetve az adatvédelmi incidens (papíralapú és nem papíralapú adatokra vonatkozóan egyaránt) e Szabályzatnak megfelelő kivizsgálását és minősítését, valamint a haladéktalanul megteendő intézkedések meghatározását az incidensvizsgáló bizottság végzi.

(4) Az incidensvizsgáló bizottság állandó tagjai: az Egyetem adatvédelmi tisztviselője és információbiztonsági felelőse. Az incidensvizsgáló bizottság a rendkívüli esemény jellegének megfelelően további tagokkal bővíthető. Az incidensvizsgáló bizottság tagjainak – szükség esetén – munkaidőn kívül is rendelkezésre kell állniuk.

(5) Az incidensvizsgáló bizottság munkáját adatvédelmi incidens esetén az adatvédelmi tisztviselő koordinálja, és képviseli az Egyetem egyéb szervezeti egységei felé.

(6) Az adatvédelmi incidensről az adatvédelmi tisztviselő értesíti a rektort, valamint – szükség esetén – a Kommunikáció és Marketing Igazgatóságot.

(7) Az informatikáért felelős szakterület bevonásával a riasztásokban szereplő sérülékenység elhárításakor a következők szerint kell eljárni:
   a) figyelembe kell venni a különböző informatikai biztonsági szabályozásokban a sérülékenységek elhárítására vonatkozó rendelkezéseket;
   b) amennyiben a riasztás személyes adatot tartalmazó alkalmazás sérülékenységével kapcsolatban keletkezett, az adatvédelmi tisztviselőt haladéktalanul tájékoztatni kell;
   c) amennyiben az Egyetem rendelkezik automatizált módszerrel az adott sérülékenység elhárítására, akkor azt azzal az eszközzel azonnal el kell kezdeni;
   d) ha az Egyetem – a mindenkor hatályos Informatikai Biztonsági Szabályzatában, továbbá a Hozzáférésvédelmi Szabályzatában foglaltakkal összhangban – nem rendelkezik automatizált

módszerrel az adott sérülékenység elhárítására, akkor azt manuális módon kell azonnal elkezdeni;

e) amennyiben a sérülékenység elhárítása belső erőforrásból nem kivitelezhető, akkor külső szakértőket kell bevonni az elhárítás folyamatába.

(8) A nem papíralapon kezelt adattal kapcsolatos adatvédelmi incidensek kezelésére az Egyetem mindenkor hatályos Informatikai Biztonsági Szabályzatában, továbbá a Hozzáférésvédelmi Szabályzatában foglaltak is irányadóak.

(9) A közös adatkezelésről szóló szerződésben [GDPR 26. cikk], illetve az adatfeldolgozóval kötendő szerződésben [GDPR 28. cikk] egyértelműen rendelkezni kell a másik adatkezelő, illetve az adatfeldolgozó azon kötelezettségéről, hogy az adatvédelmi incidensről az Egyetem adatvédelmi tisztviselőjét köteles haladéktalanul, de legkésőbb az észlelést követő 24 órán belül értesíteni. A szerződésnek tartalmaznia kell továbbá a közös adatkezelő, illetve az adatfeldolgozó kötelezettségeit adatvédelmi incidens bejelentésében és kivizsgálásában.

(10) Az incidensvizsgáló bizottság üléseiről emlékeztetőt, döntéseiről indoklást is tartalmazó jegyzőkönyvet, vizsgálatairól pedig intézkedési javaslatokat is tartalmazó jelentést kell készíteni. Az incidensvizsgáló bizottság munkáját tartalmazó dokumentumok kezelésére az Egyetem mindenkori iratkezelési szabályai az irányadók. Az incidensvizsgáló bizottság korlátozhatja a munkájáról szóló dokumentumokba betekintők körét (ide nem értve a rektort).

(11) Az adatvédelmi incidensek vizsgálata során keletkezett, papíralapú és elektronikus, iktatott dokumentumokat az adatvédelmi tisztviselő az adatvédelmi incidens vizsgálatának lezárásától számított 10 évig őrzi meg, illetéktelenek számára hozzá nem férhető, zárt helyen.

24.§
Az adatvédelmi incidens minősítése

(1) Adatvédelmi incidens csak akkor következik be, ha az adatbiztonsági intézkedések – akár gondatlan, akár szándékos – megsértésének következtében bekövetkezik a személyes adatok véletlen vagy jogellenes megsemmisítése, elvesztése, megváltoztatása, jogosulatlan közlése vagy az azokhoz való jogosulatlan hozzáférés:

a) súlyos incidens: olyan incidens (pl. adatvesztés, adatsérülés), amely valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve (pl. a jogosulatlan hozzáférés során megismert adatok; olyan adatsérülés, adatvesztés, amelynél az adatok naplózott adatállományból, biztonsági mentésből nem állíthatóak helyre). Magas kockázatúnak minősül az az incidens, amely fizikai, vagyoni vagy nem vagyoni károkat okozhat az érintetteknek (pl. az érintett személyes adatai feletti rendelkezési jogának elvesztését vagy jogai korlátozását, hátrányos megkülönböztetést, személyazonosság-lopást vagy a személyazonosságával való visszaélést, pénzügyi veszteséget, jó hírnevének sérelmét, a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülését eredményezheti);

b) enyhe incidens: minden incidens, amely nem tartozik az a) pont alá (pl. átmeneti szolgáltatásleállás, - kiesés az Egyetem munkavállalói által használt belső rendszerekben, amely nem jár adatsérüléssel vagy adatvesztéssel).

(2) Az adatvédelmi incidensre vonatkozó szabályokat kell alkalmazni az Egyetem tulajdonát képező adathordozón, mobiltelefonon, laptopon, egyéb számítástechnikai eszközön tárolt személyes adatokra, továbbá az Egyetem munkavállalóinak olyan saját tulajdonú eszközein (adathordozó, mobiltelefon, laptop, egyéb számítástechnikai eszköz) tárolt személyes adatokra, amely eszközöket munkavégzéshez, munkaköri feladatok ellátásához, hivatalos célból használhat. Az adatvédelmi incidensre vonatkozó szabályokat az Egyetem birtokában lévő papíralapú adathordozón lévő személyes adatokra is alkalmazni kell.

(3) Az elektronikus információs rendszereket érintő (informatikai biztonsági vagy általános biztonsági) rendkívüli esemény egyúttal adatvédelmi incidensnek is minősül, amennyiben személyes adatokra nézve következik be. A jelen Szabályzat adatvédelmi incidens kezelésére vonatkozó rendelkezéseinek alkalmazása nem mentesít az elektronikus információs rendszereket érintő (informatikai biztonsági vagy általános biztonsági) rendkívüli események kezelésére (bejelentésére, kivizsgálására stb.) vonatkozó szabályok betartása alól, azaz az elektronikus információs rendszereket érintő (informatikai biztonsági vagy általános biztonsági) események kezelésére vonatkozó szabályokat jelen Szabályzat előírásaival párhuzamosan alkalmazni kell.

25.§
Az adatvédelmi incidens kivizsgálása

(1) A rendkívüli eseményről (adatvédelmi incidensről vagy annak gyanújáról) szóló bejelentés megvizsgálása során az alábbi szempontokat kell figyelembe venni:
   a) a bejelentés személyes adatot érint-e,
   b) amennyiben a bejelentés személyes adatot érint, megállapítható-e a személyes adatok köre,
   c) megállapítható-e az incidensben érintett személyek köre,
   d) a hatályos jogszabályok és belső szabályok alapján megállapítható-e, hogy személyes adat jogellenes kezelése vagy feldolgozása (beleértve a törlést/megsemmisítést is) történt,
   e) az incidens valószínűsíthetően magas kockázattal jár-e az érintettek jogaira és szabadságaira nézve,
   f) melyek az adatvédelmi incidensből eredő, valószínűsíthető következmények,
   g) az Egyetem által alkalmazott technikai és szervezési védelmi intézkedések az incidensben érintett személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik-e az adatokat.

(2) A bejelentőt – szükség esetén – további információk közlésére kell felkérni.

(3) Ha az incidensbejelentés előzetes megvizsgálása azzal az eredménnyel jár, hogy az elektronikus információs rendszereket érintő (informatikai biztonsági vagy általános biztonsági) rendkívüli esemény nem érintett személyes adatokat, akkor a vizsgálatot az Egyetem mindenkor hatályos Informatikai Biztonsági Szabályzatában, illetve Hozzáférésvédelmi Szabályzatában vagy az Egyetem Szervezeti és Működési Rendje szerint kell tovább folytatni.

(4) Az incidensvizsgáló bizottság – adatvédelmi incidens esetén az adatvédelmi tisztviselő útján – legkésőbb a rendkívüli esemény bejelentését vagy a rendkívüli esemény adatvédelmi incidens kategóriába sorolását (tudomásszerzés) követő 1 naptári napon belül tájékoztatja a következő személyeket a bejelentésben foglaltakról vagy az előzetes vizsgálat eredményéről, továbbá a GDPR 33. cikkében írt adatvédelmi felügyeleti hatóságnak történő bejelentés szükségességéről, valamint arról, hogy szükséges-e a rendkívüli esemény (adatvédelmi incidens) részletes vizsgálata:

a) az Egyetem rektorát;
b) Jogi Osztály vezetőjét;
c) informatikai rendszert is érintő rendkívüli esemény esetén az informatikáért felelős szakterület vezetőjét;
d) az incidenssel érintett, szakmailag illetékes szervezeti egység vezetőjét;
e) a Kommunikáció és Marketing Igazgatóság vezetőjét.

(5) Az incidensvizsgáló bizottság javaslata alapján a rektorlegkésőbb a bizottság javaslatának kézhezvételét követő 1 naptári napon belül dönt a GDPR 33. cikkében írt, a Hatóságnak történő bejelentés szükségességéről. A rektor döntéséről az adatvédelmi tisztviselő értesíti a meghatározott egyéb személyeket.

(6) Az adatvédelmi incidens részletes vizsgálatának szükségességéről az incidensvizsgáló bizottság dönt. A részletes vizsgálatot legkésőbb a döntést követő naptári napon meg kell kezdeni, s a vizsgálat megkezdésének napjától számított legfeljebb 15 munkanapon belül le kell zárni.

(7) Az adatvédelmi incidens részletes vizsgálata során elsősorban az alábbi módszerek alkalmazhatóak:
a) személyes megbeszélés az adatvédelmi incidenst észlelő személyekkel, valamint az érintett szervezeti egységek munkatársaival és vezetőivel,
b) írásbeli tájékoztatás kérése az érintett szervezeti egységektől,
c) dokumentumok vizsgálata,
d) informatikai rendszerek, hálózatok és eszközök vizsgálata.

(8) Amennyiben az incidensvizsgáló bizottság a részletes kivizsgálás eredményei alapján úgy ítéli meg, hogy azonnali intézkedések szükségesek annak biztosítására, hogy az adatvédelmi incidenssel azonos problémaforrásból eredő újabb incidens a jövőben ne valósuljon meg, úgy a szükséges intézkedések megtétele érdekében haladéktalanul tájékoztatja az érintett szervezeti egységek vezetőit.

(9) Az incidensvizsgáló bizottság a részletes vizsgálat megállapításairól, illetve a javasolt intézkedésekről a részletes vizsgálat befejezését követő 2 munkanapon belül vizsgálati jelentést készít. A vizsgálati jelentés tartalmazza az adatvédelmi incidens elhárításához és további incidens megelőzéséhez szükséges intézkedésekre vonatkozó, az illetékes vezető részére tett javaslato(ka)t is.

(10) A részletes vizsgálatról szóló jelentést a jelen Szabályzat 26. § (4) bekezdés a)-d) pontjaiban meghatározott vezetőknek kell megküldeni.

(11) A jelentés alapján a részletes vizsgálatban érintett szervezeti egységek vezetői 15 naptári napon belül, a megvalósításhoz szükséges határidőre tett javaslatot is tartalmazó intézkedési tervet készítenek, és azt megküldik az adatvédelmi tisztviselő útján az incidensvizsgáló bizottságnak.

(12) Az intézkedési tervet és a megvalósításhoz szükséges határidőt tartalmazó szakterületi javaslatot az incidensvizsgáló bizottság a kézhezvételtől számított 3 munkanapon belül véleményezi, majd jóváhagyásra megküldi a rektor részére.

(13) Az adatvédelmi incidens elhárítása, valamint a további adatvédelmi incidensek megelőzése céljából megtett egyes intézkedésekről az adatvédelmi incidenssel érintett szervezeti egység vezetője tájékoztatást küld az adatvédelmi tisztviselő részére.

(14) Az adatvédelmi tisztviselő az intézkedési tervben foglaltak végrehajtásáról időszaki tájékoztatást, továbbá az összes intézkedés befejezését követő 3 munkanapon belül összegző tájékoztatást küld a rektorrészére.

26.§
Az érintett tájékoztatása a súlyos adatvédelmi incidensről

(1) Súlyos adatvédelmi incidens esetén az Egyetem – az érintettel kapcsolatban rendelkezésére álló elérhetőségeken, ennek hiányában vagy alkalmazásuk lehetetlensége esetén (GDPR 34. cikk) az Egyetem honlapján közzétett közlemény útján – indokolatlan késedelem nélkül tájékoztatja az érintettet az adatvédelmi incidensről. A közlemény összeállításában a Kommunikáció és Marketing Igazgatóság közreműködhet.

(2) Az érintett részére adott tájékoztatásban egyértelműen és közérthetően ismertetni kell az adatvédelmi incidens jellegét, valamint közölni kell legalább az alábbi információkat és intézkedéseket:
   a) az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;
   b) az adatvédelmi incidensből eredő, valószínűsíthető következményeket;
   c) az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

(3) Az érintettet nem kell tájékoztatni, ha az adatvédelmi incidens nem jár magas kockázattal, és a következő feltételek bármelyike teljesül:
   a) az Egyetem megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre, és ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében alkalmazták, különösen azokat az intézkedéseket (pl. titkosítás alkalmazása), amelyek a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik az adatokat;
   b) az Egyetem az adatvédelmi incidenst követően olyan további intézkedéseket tett, amelyek biztosítják, hogy az érintett jogaira és szabadságaira jelentett, az említett magas kockázat a továbbiakban valószínűsíthetően nem áll fenn;
   c) a tájékoztatás aránytalan erőfeszítést tenne szükségessé. Ilyen esetekben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, vagy olyan intézkedést kell tenni, amely biztosítja az érintettek hasonlóan hatékony tájékoztatását.

(4) A rektordöntése alapján az Egyetem az érintetteket az Egyetem honlapján vagy országos lefedettségű sajtótermékben közzétett hirdetmény útján is értesítheti, amelynek összeállításában a Kommunikáció és Marketing Igazgatóság közreműködhet.

27.§
Az adatvédelmi incidens bejelentése a Hatóságnak

(1) Az adatvédelmi incidensről szóló bejelentést a Hatóság mindenkori kapcsolati pontjára kell eljuttatni.

(2) Az adatvédelmi incidens bejelentése összeállításának és beadásának felelőse az adatvédelmi tisztviselő. Az adatvédelmi incidensről szóló bejelentéshez szükséges információkat haladéktalanul az adatvédelmi tisztviselő rendelkezésére kell bocsátani.

(3) Az adatvédelmi incidensről szóló bejelentésben legalább:
   a) ismertetni kell az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát;
   b) közölni kell az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;
   c) ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket;
   d) ismertetni kell az Egyetem által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

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

28.§
Az Adatvédelmi Incidensek Nyilvántartása

(1) Az adatvédelmi incidensekről az adatvédelmi tisztviselő elektronikus nyilvántartást (Adatvédelmi Incidensek Nyilvántartása) vezet.

(2) Az Adatvédelmi Incidensek Nyilvántartásában rögzíteni kell:
   a) az adatvédelmi incidensben érintett személyes adatok körét és számát,
   b) az adatvédelmi incidenssel érintettek körét és számát,
   c) az adatvédelmi incidens észlelésének és tudomásszerzésének (adatvédelmi incidens kategóriába sorolásának) időpontját,
   d) az adatvédelmi incidens körülményeit, lehetséges és bekövetkezett hatásait,
   e) az adatvédelmi incidens elhárítására megtett intézkedéseket,
   f) az adatvédelmi incidenssel kapcsolatban adott tájékoztatások adatait,
   g) a Hatósághoz történt bejelentés adatait.

29.§
Harmadik országba irányuló adattovábbítás különös szabályai

(1) Amennyiben felmerül a személyes adat harmadik országba történő továbbításának szükségessége, az érintett szervezeti egység köteles az adatvédelmi tisztviselő véleményét kérni az adattovábbítás megengedhetőségéről, illetve az adattovábbítás lehetséges módjáról és feltételeiről.

(2) Az adatvédelmi tisztviselő – szükség esetén a Jogi Osztály és az informatikáért felelős szakterület véleményének kikérése után – javaslatot tesz az adattovábbítás módjára, az adatátadás során alkalmazandó biztosítékok körére.

30.§
Belső adatvédelmi ellenőrzési eljárás

(1) A belső adatvédelmi ellenőrzési eljárás célja, hogy az adatvédelmi tisztviselő meggyőződjön arról, hogy az Egyetem egyes szervezeti egységei az adatvédelemmel kapcsolatos jogszabályoknak és belső szabályzatoknak megfelelően kezelik-e a személyes adatokat.

(2) Az adatvédelmi tisztviselő éves ellenőrzési tervet készít. Az éves adatvédelmi ellenőrzési tervnek az ellenőrzés alá vont szervezeti egység nevét, az ellenőrzés várható időpontját és az ellenőrzés tárgykörét kell tartalmaznia. Az éves adatvédelmi ellenőrzési terveket úgy kell összeállítani, hogy négyéves időtartam alatt lehetőség szerint minden, adatkezelésért felelős szervezeti egység ellenőrzésére sor kerüljön. Az éves adatvédelmi ellenőrzési tervet legkésőbb az adott év február 28. napjáig kell elkészíteni, és az Egyetem rektora részére bemutatni.

(3) Az adatvédelmi tisztviselő a belső adatvédelmi ellenőrzés lefolytatásáról az érintett szervezeti egység adatkezelési megbízottját vagy vezetőjét az ellenőrzés kezdete előtt legalább 5 munkanappal tájékoztatja, melyben az eljárás kezdő időpontjára is javaslatot tesz. A szervezeti egység vezetője köteles gondoskodni arról, hogy az adatvédelmi tisztviselő a javasolt időpontban megkezdhesse a belső adatvédelmi ellenőrzést, illetve szükség esetén – az adatvédelmi tisztviselő által javasolt időponthoz képest legfeljebb tíz munkanapon belüli – új időpontra tesz javaslatot.

(4) A belső adatvédelmi ellenőrzés során az adatvédelmi tisztviselő a szervezeti egység irodahelységeibe beléphet, a szervezeti egység – a belső adatvédelmi ellenőrzés tárgyával összefüggésben kezelt – irataiba betekinthet, a szervezeti egység munkatársaitól tájékoztatást kérhet.

(5) Az adatvédelmi tisztviselő a belső adatvédelmi ellenőrzésről jegyzőkönyvet készít, melyet az ellenőrzött szervezeti egység vezetőjével együtt aláírnak. A jegyzőkönyv az ellenőrzött szervezeti egység megnevezését, a belső adatvédelmi ellenőrzés lefolytatásának tárgyát, időpontját és időtartamát, továbbá a belső adatvédelmi ellenőrzés során rögzített tényeket, megállapításokat, információkat tartalmazza.

(6) Az adatvédelmi tisztviselő a lefolytatott belső adatvédelmi ellenőrzés megállapításairól vizsgálati jelentést készít, amelynek mellékletét képezi a belső adatvédelmi ellenőrzésről készült jegyzőkönyv. A vizsgálati jelentés tartalmazza az adott szervezeti egységnél tapasztalt körülményeket, adatokat, valamint az adatvédelmi tisztviselő megállapításait. A vizsgálati jelentés tervezetére a szervezeti egység vezetője 5 munkanapon belül észrevételt tehet. A vizsgálati jelentéssel kapcsolatos észrevételek közlésének elmaradását úgy kell tekinteni, hogy a szervezeti egység vezetője a belső adatvédelmi ellenőrzésről szóló vizsgálati jelentés megállapításait elfogadja.

(7) Ha az adatvédelmi tisztviselő megállapítja, hogy az adatkezelés az ellenőrzés alá vont szervezeti egységnél nem a belső szabályzatoknak vagy jogszabályoknak megfelelően történik, javaslatot tesz a szabályszerű adatkezelés – meghatározott határidőn belüli – helyreállítására. Az adatvédelmi tisztviselő javaslata alapján megtett intézkedésekről a szervezeti egység vezetője az intézkedés megtételétől számított 3 munkanapon belül tájékoztatja az adatvédelmi tisztviselőt. Az adatvédelmi tisztviselő a megtett intézkedéseket, illetve azok betartását bármikor jogosult ellenőrizni (utóellenőrzés).

(8) Az adatvédelmi tisztviselő rendkívüli belső adatvédelmi ellenőrzést is lefolytathat, ha az adatvédelmi szempontból indokolt, különösen, ha a személyesadat-kezeléssel érintettek száma jelentős. Rendkívüli belső adatvédelmi ellenőrzésnek minősül az éves adatvédelmi ellenőrzési tervben nem szereplő belső adatvédelmi ellenőrzés. A rendkívüli belső adatvédelmi ellenőrzésről és annak indokairól a rektort tájékoztatni kell.

(9) Az adatvédelmi tisztviselő a belső adatvédelmi ellenőrzés (ideértve azutóellenőrzést is) lefolytatását követően tájékoztatja az Egyetem rektorát a belső adatvédelmi ellenőrzés adatairól és eredményeiről.

A rektor tájékoztatása történhet szóban vagy a vizsgált szervezeti egység vezetője által elfogadottvizsgálati jelentés megküldésével is.

(10) Az adatvédelmi tisztviselő jelen Szabályzat szerinti, az Egyetem adatvédelmi helyzetéről szóló éves jelentésnek tartalmaznia kell az adott évben lefolytatott belső adatvédelmi ellenőrzésekkel és utóellenőrzésekkel kapcsolatos összegző információkat és megállapításokat, valamint a vizsgált szervezeti egység által megtett intézkedéseket is.

31.§
Záró rendelkezések

(1) Jelen Szabályzat annak aláírását követő napon lép hatályba.

(2) A Jelen Szabályzat hatálybelépésével a 27/2021. (09.16.) számú rektori-kancellári közös utasítással elfogadott Adatvédelmi szabályzata hatályát veszti.

(3) Jelen Szabályzatot a Jogi osztály gondozza.

(4) A Jelen Szabályzat megtalálható és elérhető a www.szfe.hu oldalon.

Budapest, 2024. május 06.

...……..
Dr. Sepsi Enikő s.k.
rektor

Mellékletek:

1. számú melléklet: Értelmező rendelkezések

1. számú melléklet:
Értelmező rendelkezések

Jelen Szabályzat alkalmazása során a GDPR 4. cikkében és az Infotv. 3. § 3., 4., 6., 11., 12., 13., 16., 17., 21., 23-24. pontjában meghatározott fogalmakon kívül az alábbi fogalmakat kell alkalmazni:

adatbiztonság: a személyes adatok jogosulatlan kezelése, így különösen jogosulatlan megszerzése, feldolgozása, megváltoztatása és megsemmisítése elleni szervezési, technikai megoldások, valamint eljárási szabályok összessége; az adatkezelés azon állapota, amelyben az adatok sérülésének, illetéktelen felhasználásának, megsemmisülésének kockázati tényezőit – és ezáltal a fenyegetettséget – a szervezési, műszaki megoldások és intézkedések a minimálisra csökkentik,
Adatkezelési Tevékenységek Nyilvántartása: jelen utasítás 10. fejezetében meghatározott adattartalmú, folyamatosan karbantartott nyilvántartás;
adatkezelésért felelős szervezeti egység: az Egyetem azon szervezeti egysége, amelynek feladatkörébe tartozik az Egyetem kezelésében lévő valamely nyilvántartási rendszer létrehozása, fenntartása, illetve üzemeltetése,
adatvédelmi felügyeleti hatóság: a Nemzeti Adatvédelmi és Információszabadság Hatóság,
adatvédelmi hatásvizsgálat: olyan vizsgálat, amelyet az adatkezelésért felelős szervezeti egység kijelölt munkavállalója (adatkezelési megbízott) köteles elvégezni, amennyiben valamely tervezett adatkezelés – figyelemmel annak jellegére, hatókörére, körülményeire és céljaira, ideértve különösen az új technológiák alkalmazásának esetét – valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, és amelynek célja annak megállapítása, hogy a tervezett adatkezelés a személyes adatok védelmét hogyan érinti. Az adatvédelmi hatásvizsgálat egy olyan eljárás, amelynek során az adatkezelő a tervezett adatkezelési műveletet vagy műveleteket áttekinti, megvizsgálja az adatkezelés érintettekre gyakorolt esetleges hatását, felméri annak kockázatait, a kockázatok kezelésének módját, és mindezt megfelelően dokumentálja,
adatvédelmi incidens típusai: személyes adatok megsemmisülése, személyes adatok jogosulatlan megsemmisítése, személyes adatok rendelkezésre állásának sérülése, személyes adatok integritásának sérülése, személyes adatok elvesztése, személyes adatok jogosulatlan megváltoztatása, személyes adatok jogosulatlan közlése vagy jogellenes továbbítása, személyes adatokhoz történő jogosulatlan hozzáférés, személyes adatok bizalmasságának sérülése (pl. titoksértés) stb.
adatkezelési megbízott: az adatkezelésért felelős szervezeti egység azon, e feladatkör ellátására kijelölt munkavállalója, aki a jelen Szabályzatban, illetve az adatkezelésről szóló más belső szabályozó dokumentumokban meghatározottak szerint az adatkezelésért felelős szervezeti egység felelősségi körébe tartozó adatkezelések tekintetében, vagy adatkezeléseknek az adatkezelésért felelős szervezeti egység felelősségi körébe tartozó részében gondoskodik az adatkezelőt terhelő feladatok elvégzéséről,
adatvédelmi tisztviselő: az Egyetem szervezetében működő, a GDPR 39. cikkében meghatározott feladatokat az Egyetem jelen Szabályzatában foglaltak szerint ellátó, az Egyetemmel foglalkoztatási vagy megbízási jogviszonyban álló természetes személy,
álnevesítés (pszeudonimizálás): 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,
deperszonalizálás (anonimizálás): a nyilvántartási rendszerben tárolt személyes adatok közül a személyazonosításra alkalmas adatok eltávolítása olyan, visszafordíthatatlan módon, hogy a nyilvántartási rendszerben megmaradó adatok a továbbiakban semmilyen körülmények között nem teszik lehetővé egy természetes személy azonosítását,

érdekmérlegelési teszt: jogos érdeken [GDPR 6. cikk (1) bekezdés f) pont] alapuló adatkezelés tervezett bevezetése esetén annak írásbeli dokumentálása, hogy az adatkezelő számba vette az adatkezelést megalapozó érdekeket, érveket, valamint az érintettek személyes adataik védelméhez fűződő – a tervezett adatkezelés ellen ható – jogait és érdekeit, és ezen érdekek és érvek összevetésével megalapozza az adatkezelés bevezetését vagy a bevezetés elutasítását,

informatikáért felelős szakterület: az informatikai rendszerek üzemeltetéséért, az informatikai biztonság ellátásáért felelős szervezeti egység vagy egységek, ideértve az Egyetem információbiztonsági felelősét is,

titkosítás: az adatok olyan átalakítása, melynek során az adat értelmezhetetlenné válik a megfelelő kulcs ismerete nélkül,

törlés: az adat felismerhetetlenné tétele oly módon, hogy a helyreállítása a továbbiakban már nem lehetséges. A törlés célja megvalósítható deperszonalizálással (anonimizálással) [j/ pont] is,

ügyvitel: az Egyetem tevékenységére vonatkozó jogszabályokban az Egyetem részére meghatározott közfeladatok ellátásával összefüggő eljárás.