BUDAPESTI CORVINUS EGYETEM	**ELNÖKI TESTÜLETI RENDELKEZÉS**	**13/2023.** Verziószám: **00.**

AZ ADATKEZELÉS RENDJÉRŐL

Szakmai felelős:	**Bíró Barbara**	jogi vezető
Szakmai ellenőrző:	**Locsmándi Balázs**	adatvédelmi tisztviselő
Jogi ellenőrző:	**Bíró Barbara**	jogi vezető
Döntéshozó:	**Elnöki Testület**	
Szerkesztésért és közzétételért felelős:	**Erős Anikó**	felsőoktatási szakértő

Verziószám	Közzététel dátuma	Hatálybalépés dátuma	Verziókövetés
00.	2023. 06. 13.	2023. 08. 01.	**Közzététel** ET-68/2023. (IV. 27.) sz. határozat

Tartalomjegyzék

A rendelkezés célja és hatálya

1. §

(1) A Rendelkezés célja az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (a továbbiakban adatvédelmi rendelet vagy GDPR) alapján a Rendelkezés célja annak biztosítása, hogy a Budapesti Corvinus Egyetem (a továbbiakban: az Egyetem) mint adatkezelő jogi személy a működése során maradéktalanul megfeleljen a GDPR, valamint minden más ágazati adatvédelmi szabályozásnak.

(2) A Rendelkezés hatálya kiterjed az Egyetem székhelyén és valamennyi telephelyén folyó valamennyi, az Egyetem által folytatott adatkezelésre.

(3) A Rendelkezés személyi hatálya kiterjed az Egyetem valamennyi szervezeti egységére, minden munkavállalójára, valamint az Egyetem számára egyéb foglalkoztatási jogviszony keretében munkát végző, vagy az Egyetemmel egyéb kapcsolatban álló személyes adatkezelést végző személyekre.

(4) A Rendelkezés tárgyi hatálya kiterjed az Egyetem bármely szervezeti egysége által kezelt valamennyi személyes adatra, a rajtuk végzett adatkezelési műveletek teljes körére keletkezésük, kezelésük, feldolgozásuk helyétől, valamint megjelenési formájuktól függetlenül.

Kapcsolódó dokumentumok

2. §

(1) Kapcsolódó jogszabályok:

a) Magyarország Alaptörvénye;

b) az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) – a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet, GDPR);

c) 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (Infotv.).

Fogalmak

3. §

(1) Jelen paragrafus vonatkozásában:

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

vagy több tényező alapján azonosítható (pl.: név, születési hely, Neptun azonosító, fogyatékosságra vonatkozó adat, az a tény, hogy egy adott személy az Egyetem hallgatója, hogy a hallgató milyen szakra jár, az a tény, hogy egy hallgató önköltséges képzésen vagy Corvinus Ösztöndíjas képzésen vesz részt, az a tény, hogy egy hallgató bármilyen ösztöndíjra pályázatot adott be, ösztöndíjat nyert el, az, hogy egy hallgató mely vizsgára jelentkezett vagy ott milyen értékelést kapott, az, hogy ha egy hallgató TDK-n vesz részt, ott milyen eredményt ért el, ellene fegyelmi eljárás indult vagy annak eredménye, adott vizsgára jelentkezés ténye; egy munkavállaló neve, lakcíme, anyja neve, az, hogy milyen munkakörben dolgozik, mennyi ideje dolgozik az Egyetemen, a munkavállaló munkabére, egyéb juttatásai, az a tény, hogy egy munkavállaló valamilyen tisztséget, bizottsági tagságot tölt be, az a tény, hogy egy munkavállaló a teljesítményértékeléssel szemben panaszt emelt, az, hogyha egy munkavállaló díjazásban, kitüntetésben részesült, vagy vele szemben munkajogi intézkedést foganatosítottak);

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

c) *adatkezelő:* az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, aki/amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza. Jelen Rendelkezésben adatkezelő jogi személy az Egyetem, azonban ennek keretében adatkezelőnek minősül minden, a Szervezeti és Működési Rend szerinti szervezeti egység, aki személyes adatot kezel és aki a személyes adatok kezelésének céljait, a kezelt adatok körét, valamint az adatkezelés eszközeit meghatározza (a továbbiakban: Adatkezelő). Adatkezelő például a Hallgatói Szolgáltatások, a HR, a Pénzügy, a CIAS, a Könyvtár, de adatkezelő lehet egy intézet, kutatóintézet is;

d) *adatfeldolgozó:* az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, aki/amely az adatkezelő nevében személyes adatokat kezel, így adatfeldolgozónak minősül pl. egy külső IT üzemeltető és/vagy fejlesztő cég, amely a szerződéses feladatai ellátása keretében hozzáférhet a rendszerben tárolt személyes adatokhoz, de azokkal semmit nem tehet az adatkezelő hozzájárulása vagy utasítása nélkül;

e) *adatvédelmi incidens:* a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi;

f) *az adatkezelés korlátozása:* a tárolt személyes adatok megjelölése jövőbeli kezelésük korlátozása céljából;

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

h) *álnevesítés:* a személyes adatok olyan módon történő kezelése, amelynek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik, feltéve, hogy az ilyen további információt külön tárolják, és technikai és szervezési intézkedések megtételével biztosított, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni;

i) *nyilvántartási rendszer:* a személyes adatok bármely módon – centralizált, decentralizált, funkcionális vagy földrajzi szempontok szerint – tagolt állománya, amely meghatározott ismérvek alapján hozzáférhető;

j) *címzett:* az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, akivel vagy amellyel a személyes adatot közlik, függetlenül attól, hogy harmadik fél-e. Azon közhatalmi szervek, amelyek egy egyedi vizsgálat keretében az uniós vagy a tagállami joggal összhangban férhetnek hozzá személyes adatokhoz, nem minősülnek címzettnek; az említett adatok e közhatalmi szervek általi kezelése meg kell, hogy feleljen az adatkezelés céljainak megfelelően az alkalmazandó adatvédelmi szabályoknak;

k) *harmadik fél:* az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, aki/amely nem azonos az érintettel, az adatkezelővel, az adatfeldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére felhatalmazást kaptak, pl. a fenntartó, ágazati minisztérium, Egyetem tanácsadói, informatikai rendszereket üzemeltető cégek;

l) *az érintett hozzájárulása:* az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez;

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

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

o) *egészségügyi adat:* egy természetes személy testi vagy pszichikai egészségi állapotára vonatkozó személyes adat, ideértve a természetes személy számára nyújtott egészségügyi szolgáltatásokra vonatkozó olyan adatot is, amely információt hordoz a természetes személy egészségi állapotáról;

p) *adatvédelmi tisztviselő:* a GDPR-nak történő megfelelést, az érintettek kontrolljogainak a gyakorlását elősegítő, a GDPR 37–39. cikkei szerint eljáró, a CORVINUS által kijelölt személy;

q) *adatok törlése:* személyes adatok fizikai megsemmisítése vagy álnevesítése;

r) *adatvédelmi kapcsolattartó:* az adatkezelést végző vezető által kijelölt munkavállaló, vagy a munkavégzésre irányuló egyéb jogviszonyban az Egyetem számára feladatot teljesítő természetes személy, aki az Egyetem, adatvédelmi tisztviselőjével és/vagy a Jog, Igazgatás, Szabályozás vezetőjével (a továbbiakban: jogi vezető) az adatvédelmi jellegű ügyekben kapcsolatot tart, és/vagy ezen személyek felé az ilyen ügyekben az adatkezelést végző szervezeti egységet képviseli.

Alapelvek

4. §

(1) Az Adatkezelő minden szervezeti egysége eljárásának meg kell felelnie az érintetti jogok gyakorlása során az adatkezelés alapelveinek, különösen az alábbiaknak:

a) *Jogszerűség, tisztességes eljárás és átláthatóság:* A személyes adatok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni. Az átláthatóság elve az előreláthatóságot jelenti és az érintett adatai feletti rendelkezést biztosítja. Ez az elv garantálja, hogy az érintett tudomással bírjon arról, hogy adatai milyen formában, hogyan kerülnek kezelésre.

b) *Pontosság:* A 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.

c) *Elszámoltathatóság:* Az elszámoltathatóság elve egyrészt az Adatkezelő azon kötelezettségét jelenti, amely szerint ki kell alakítania azokat a belső szabályokat, folyamatokat, mechanizmusokat, amelyek az általános adatvédelmi rendeletből fakadó kötelezettségek teljesítéséhez szükségesek, másrészt a megfelelés bemutatásának képességét várja el.

d) *Beépített adatvédelem elve:* Az Adatkezelő az érintett jogainak gyakorlása érdekében köteles figyelembe venni a tudomány és a technológia állását, a megvalósítás költségeit, az adatkezelés jellegét, hatókörét, körülményeit és céljait. A beépített adatvédelem elvének érvényesüléséhez szükséges, hogy az Adatkezelő mérlegelést végezzen, amelynek során a természetes személyek jogaira jelentett kockázatokat kell azonosítania és elemeznie. A fentiek alapján határozható meg, hogy az adott

szervezeten belül, az adott adatkezelést a feltárt körülmények között miként lehet a beépített adatvédelem elvárásának megfelelően alakítani.

I. AZ EGYETEM ADATVÉDELMI SZERVEZETE

Adatvédelmi szerepkörök, felelősségek

5. §

(1) Általános munkavállalói felelősség: Az adatvédelmi előírások betartásával kapcsolatos jogi felelősség egyaránt terheli az Egyetem valamennyi munkavállalóját, ideértve a vezetőket, valamint az Egyetem számára egyéb foglalkoztatási jogviszony keretében munkát végző személyeket. Ez minden, a GDPR-ból és a nemzeti adatvédelmi jogszabályokból eredő kötelezettségre, és különösen az alábbiakra érvényes:

a) az adatvédelmi alapelvek betartása, úgymint célhoz kötöttség, adattakarékosság, jogszerűség (GDPR 5. cikk);

b) személyes adatok törlése vagy anonimizálása (GDPR 5., 6. és 17. cikk);

c) megfelelő technikai és szervezési intézkedések megtétele (GDPR 32. cikk).

(2) Felsővezetői felelősség: Az Elnöki Testület elkötelezett a GDPR-nak történő maradéktalan megfelelés iránt.
Az elnök felelős azért, hogy az Egyetem működése minden tekintetben megfeleljen a GDPR és a nemzeti adatvédelmi jogszabályok követelményeinek. Ennek keretében biztosítja a megfeleléshez szükséges anyagi és emberi erőforrásokat, előterjeszti a jelen Rendelkezést, valamint az általa meghatározottak szerint rendszeres időközönként meggyőződik a jelen Rendelkezésnek megfelelő működésről.

(3) Vezetői felelősség: Az egyes szervezeti egységek vezetői a fentieken túl felelnek még:

a) érintetti jogok teljesítésében (GDPR 15. cikk);

b) adatfeldolgozói szerződések megkötésében (GDPR 28. cikk (3) bek);

c) jogi vezető felelősségi körébe tartozó adatkezelési nyilvántartás összeállításában és naprakészen tartásában (GDPR 30. cikk) való közreműködésért.

(4) A Szervezeti és Működési Rend szerinti vezetőknek (a továbbiakban: vezetők) felügyeleti és szervezési kötelezettsége is van (vezetői felelősség). Minden vezető felelősséggel tartozik azért, hogy az illetékességi területén történő adatkezelések adatvédelmi jogszabályoknak való megfelelősége biztosított legyen. Azt, hogy a vezetők miként tesznek eleget a feladatkörükbe tartozó feladatoknak – az adatkezelések és a szervezési keretfeltételek szigorú figyelembevételével –, nekik maguknak kell meghatározniuk. Megfelelő szervezési intézkedéseknek minősül többek között a munkautasítások kiadása, a GDPR-konform adatkezelés felügyelete, támogató intézkedések (pl. dolgozói oktatások és online tesztek) szükségességének felmérése, folyamatok kialakítása új adatkezelések bevezetésére, technikai és szervezési adatvédelmi intézkedések meghatározása, intézkedések megtétele, beleértve a fegyelmi szankciókat és egyéb munkajogi intézkedéseket is. Azzal kapcsolatban, hogy egy, a jelen bekezdés szerinti vezetői intézkedés megfelelő-e, a vezetők

igénybe vehetik a jogi vezető, valamint az Egyetem adatvédelmi tisztségviselőjének segítségét.

(5) A vezetők felelősségi körébe így beletartozik különösen:

a) a vezetésük alatt álló és/vagy az irányításukkal működő területeken végzett adatkezelések naprakész nyilvántartása legalább a jelen Rendelkezés 1. melléklete szerinti adatkörrel;

b) a vezetésük alatt álló és/vagy az irányításukkal működő területeken észlelt adatvédelmi incidensek jelentése a jelen Rendelkezés szerint;

c) azon adatvédelmi intézkedések nyilvántartása, amelyet a vezetésük alatt álló és/vagy az irányításukkal működő szervezeti egység akár a saját döntése, akár más szervezeti egység vagy vezető (pl.: HR, Vállalati és Intézményi Kapcsolatok, Hallgatói Szolgáltatások, elnök, rektor, kancellár) kezdeményezése alapján tett (így különösen a munkavállalók tájékoztatása a személyes adataik kezeléséről, adott esetben a munkavállalótól hozzájárulás kérése a személyes adatai kezeléséhez, adatvédelmi tárgyú belső szabályozás kiadása) a jelen Rendelkezés szerint;

d) az adatvédelmi hatásvizsgálat előkészítése a jelen Rendelkezés szerint;

e) új adatkezelések bevezetésének előkészítése;

f) a vezetésük alatt álló és/vagy az irányításukkal működő szervezeti egység által igénybe vett külső adatfeldolgozóval történő adatfeldolgozási szerződés megkötésének előkészítése az illetékes jogi terület (Gazdasági Jogi, Beszerzési, Munkajogi Szolgáltatások vagy Jog, Igazgatás, Szabályozás) iránymutatása alapján és a jogi vezető bevonásával;

g) az Informatika vezetőjével és a jogi vezetővel egyeztetett adatbiztonsági szabályok meghatározása és alkalmazása;

h) az adatvédelmi tisztviselő és/vagy a jogi vezető által a GDPR megfelelőség érdekében javasolt intézkedés végrehajtásában történő közreműködés;

i) a vezetésük alatt álló és/vagy az irányításukkal működő szervezeti egység által megbízott külső adatfeldolgozók nyilvántartása, legkevesebb a jelen Rendelkezés 2. melléklete szerinti tartalommal;

j) a vezetésük alatt álló és/vagy az irányításukkal működő szervezeti egység munkájában részt vevő külső adatfeldolgozó felé az Informatika által meghatározott adatbiztonsági technikai és szervezési intézkedések („Technical and organisational measures” – TOM) becsatornázása;

k) a GDPR szerinti érintetti jogok (tájékoztatás, helyesbítés, tiltakozás, adathordozhatóság, törlés, adatkezelés korlátozása, hozzáférés a személyes adatokhoz) érvényre juttatása a jogi vezető iránymutatása szerint (lásd jelen Rendelkezés 16. §–25. §-ait;

l) a vezetésük alatt álló és/vagy az irányításukkal működő területeken folyó adatkezelések tekintetében a szükséges adatkezelési tájékoztató elkészítése a jogi

vezető útmutatása szerint; a vezetésük alatt álló és/vagy az irányításukkal működő területen végzett adatkezelésben bekövetkező változásnak a bejelentése a jogi vezető számára annak érdekében, hogy a jogi vezető a jelen Rendelkezés szerinti nyilvántartási kötelezettségének eleget tehessen;

m) a lejárt adatkezelésű adatok törlése;

n) a vezetésük alatt álló és/vagy az irányításukkal működő területre vonatkozó NAIH megkeresés kivizsgálása, és/vagy NAIH határozatban foglaltak végrehajtása a jogi vezető iránymutatása szerint;

o) külső vagy belső adatvédelmi audit támogatása;

p) az adatvédelmi tisztviselő munkájának támogatása pl. információszolgáltatással, oktatás vagy adatvédelmi audit támogatásával;

q) a vezetésük alatt álló és/vagy az irányításukkal működő szervezeti egységnél adatvédelmi kapcsolattartó kijelölése;

r) a vezetésük alatt álló és/vagy az irányításukkal működő területen dolgozó munkavállalók munkakörének megfelelő (célhoz-kötött) IT jogosultságprofil kialakítása és naprakészen tartása, betartva a legkisebb jogosultság elvét.

(6) Az adatvédelmi kapcsolattartók az adatkezelő szervezeti egység vezetőjének az utasítása szerint közreműködnek a jelen Rendelkezésben részletezett megfelelési intézkedések végrehajtásában. Feladatuk a szakmai kapcsolattartás a jogi vezető és/vagy az adatvédelmi tisztviselő irányába, a szervezeti egységüket érintő adatvédelmi követelmények becsatornázása, közreműködés a vezetők felelősségi körébe tartozó GDPR megfelelőség kialakításában.

(7) Adatvédelmi tisztviselő felelősségére vonatkozó szabályokat, valamint a feladatait a jelen Rendelkezés 41. §-a rögzíti.

(8) Jogi vezető speciális felelőssége: megkeresés és/vagy hiányosság észlelése esetén a jogi vezető feladata az Egyetem prudens adatvédelmi működéséhez szükséges jogi álláspont kialakítása. A jogi vezető ugyanakkor nem felel az Egyetem GDPR-konform működéséért, annak biztosítása az adott szervezeti egység vezetőjének feladata, míg Egyetemi szinten a GDPR megfelelés biztosítása az elnök felelőssége. Adatvédelmi kérdés esetén a jogi vezető az adatvédelmi tisztviselőhöz fordulhat azzal, hogy az adatvédelmi tisztviselő álláspontja a jogi vélemény kialakításában nem köti.

(9) A jogi vezető feladata az Egyetem által végzett valamennyi adatkezelésről a GDPR 30. cikke szerinti nyilvántartás vezetése és naprakészen tartása. Nem felelős a jogi vezető az adatkezelési nyilvántartás naprakészen tartásáért, amennyiben az adatkezelésért felelős vezető a vezetése alatt álló és/vagy az irányításával működő területen végzett adatkezelésekről vagy a bekövetkezett módosításokról nem ad kellő tájékoztatást a jogi vezető részére.

(10) Az érintetti joggyakorlás, valamint az egyes területek által végzett adatkezelésekre vonatkozó adatkezelési tájékoztató jogi megfelelőségéért a jogi vezető felel a jelen Rendelkezés 23. §–26. §-ai szerint.

(11) A jogi vezető felelős a jogszabályoknak mindenkor megfelelő adatvédelmi szabályok kialakításáért.

(12) A jogi vezető felel az adatvédelmi oktatási anyag összeállításáért, valamint kezdeményezi és/vagy közreműködik az adatkezelést végző egyetemi szervezeti egységek rendszeres oktatásának a megszervezésében.

(13) Az Informatika kijelölt szakemberei minden olyan jogosultsággal rendelkeznek, amelyek az informatikai rendszerek, szolgáltatások adminisztrálásához szükségesek. Ezek a jogosultságok nagyon magas szintűek, amelyekkel minden munkavállaló által létrehozott adathoz hozzáférnek. Ez alatt kell érteni a levelezést, a létrehozott állományokat, internet-forgalmat stb. Az Informatika munkavállalóin kívül az Egyetemen senki sem rendelkezhet ilyen jogosultságokkal, amely kitételt az Egyetem minden munkavállalójának, ideértve a vezetőket is, el kell fogadnia. Továbbá az Egyetem minden munkavállalójának el kell fogadnia a fentieket, miszerint az Informatika megfelelően magas jogosultságokkal rendelkező munkavállalói minden informatikai rendszerben végrehajtott műveletről tudomásul bírnak és minden keletkezett adattal kapcsolatban információval rendelkeznek.

(14) A személyes adatok kezelésének egy jelentős része külső szolgáltatónál történik. Ide tartozik a teljes M365 szolgáltatási rendszer. Ebben található a levelezés, a fájlkiszolgálás jelentős része. Ezekben a rendszerekben tárolt adatok bármilyen módosítása, törlése vagy bővítése lehetséges, de ezek az adatok fizikailag nem az Egyetem infrastruktúráján vannak elhelyezve.

II. AZ ÉRINTETT JOGAI ÉS GYAKORLÁSUK

Az érintett által érvényesíthető jogok

6. §

(1) Az érintett tájékoztatást kérhet személyes adatai kezeléséről, valamint kérheti személyes adatainak helyesbítését és/vagy – a kötelező adatkezelések kivételével – törlését, az adatkezelés korlátozását, visszavonhatja az adatkezeléshez történő hozzájárulását, valamint élhet adathordozási jogával és tiltakozási jogával az adat felvételénél jelzett módon a jelen Rendelkezés III. fejezete szerint.

(2) A jelen Rendelkezésben szereplő jogok gyakorlása ingyenes, kivéve, ahol ezt az Egyetem kifejezetten jelzi.

Tájékoztatáshoz való jog

7. §

(1) Minden Adatkezelő (személyes adatokat kezelő egyetemi szervezeti egység) vezetője megfelelő intézkedésekkel garantálja, hogy az érintettek részére a személyes adatok kezelésére vonatkozó, a GDPR 13. és a 14. cikkben említett valamennyi információt és a 15–22. és 34. cikk szerinti minden egyes tájékoztatást tömör, átlátható, érthető és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva nyújtsa.

(2) Ha az érintettre vonatkozó személyes adatokat az érintettől gyűjti az Adatkezelő (személyes adatokat kezelő egyetemi szervezeti egység), a személyes adatok megszerzésének időpontjában az érintett rendelkezésére bocsátja a következő információk mindegyikét:

a) az Adatkezelőnek (személyes adatokat kezelő egyetemi szervezeti egység) és a képviselőjének a kiléte és elérhetőségei;

b) az adatvédelmi tisztviselő elérhetőségei;

c) a személyes adatok tervezett kezelésének célja, valamint az adatkezelés jogalapja;

d) amennyiben jogos érdek az adatkezelés jogalapja, az Egyetem vagy harmadik fél jogos érdekei;

e) adott esetben a személyes adatok címzettjei és/vagy a címzettek kategóriái, ha van ilyen;

f) adott esetben annak ténye, hogy az Adatkezelő (személyes adatokat kezelő egyetemi szervezeti egység) harmadik országba vagy nemzetközi szervezet részére kívánja továbbítani a személyes adatokat, továbbá az ilyen adattovábbítás alkalmazott garanciákat;

g) a személyes adatok tárolásának időtartama, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjai;

h) tájékoztatás az érintett azon jogáról, hogy kérelmezheti az Adatkezelőtől (személyes adatokat kezelő egyetemi szervezeti egység) a rá vonatkozó személyes adatokhoz való hozzáférést, azok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen, valamint az érintett adathordozhatósághoz való jogáról;

i) amennyiben az Adatkezelő (személyes adatokat kezelő egyetemi szervezeti egység) az érintettről különleges adatokat az érintett hozzájárulása alapján kezel, a hozzájárulás bármely időpontban történő visszavonásához való jogról szóló tájékoztatás;

j) tájékoztatás a felügyeleti hatósághoz címzett panasz benyújtásának jogáról;

k) tájékoztatás arról, hogy a személyes adat szolgáltatása jogszabályon vagy szerződéses kötelezettségen alapul vagy szerződés kötésének előfeltétele-e, valamint, hogy az érintett köteles-e a személyes adatokat megadni, továbbá, hogy milyen lehetséges következményeikkel járhat az adatszolgáltatás elmaradása;

l) amennyiben releváns, tájékoztatás az automatizált döntéshozatalról, ideértve a profilalkotást is, valamint legalább ezekben az esetekben az alkalmazott logikára és arra vonatkozóan érthető információkról, hogy az ilyen adatkezelés milyen jelentőséggel, és az érintettre nézve milyen várható következményekkel bír;

m) amennyiben az adatok forrása nem az érintett, tájékoztatás arról, hogy a személyes adatok forrásáról és adott esetben arról, hogy az adatok nyilvánosan hozzáférhető forrásokból származnak-e.

Az érintett hozzáféréshez való joga

8. §

(1) Az érintett jogosult arra, hogy Adatkezelőtől (személyes adatokat kezelő egyetemi szervezeti egység) visszajelzést kapjon arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e, és ha ilyen adatkezelés folyamatban van, jogosult arra, hogy a személyes adatokhoz és a következő információkhoz hozzáférést kapjon:

a) az adatkezelés céljai;

b) az érintett személyes adatok kategóriái;

c) azon címzettek vagy címzettek kategóriái, akikkel és/vagy amelyekkel a személyes adatokat közölték vagy közölni fogják, ideértve különösen a harmadik országbeli címzetteket és/vagy a nemzetközi szervezeteket;

d) a személyes adatok tárolásának tervezett időtartama;

e) a helyesbítés, törlés vagy adatkezelés korlátozásának és a tiltakozás joga;

f) a felügyeleti hatósághoz címzett panasz benyújtásának joga;

g) az adatforrásokra vonatkozó információ;

h) az automatizált döntéshozatal ténye, ideértve a profilalkotást is, valamint az alkalmazott logikára és arra vonatkozó érthető információk, hogy az ilyen adatkezelés milyen jelentőséggel bír, és az érintettre nézve milyen várható következményekkel jár;

i) személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítása esetén az érintett jogosult arra, hogy tájékoztatást kapjon a továbbításra vonatkozó megfelelő garanciákról.

(2) Az érintett kérelmére az információkat az érintett egyetemi szervezeti egység elektronikus formában szolgáltatja. Ha az érintett elektronikus úton nyújtotta be a kérelmet, az információkat széles körben használt elektronikus formátumban (pl. html, txt, pdf, jpg) kell rendelkezésre bocsátani, kivéve, ha az érintett másként kéri.

(3) Az Adatkezelő (személyes adatokat kezelő egyetemi szervezeti egység) az igazoltan az érintett személytől érkező megkeresésre az adatkezelés tárgyát képező személyes adatok másolatát az érintett rendelkezésére bocsátja. Az érintett által kért további másolatokért az adatkezelő az adminisztratív költségeken alapuló, ésszerű mértékű díjat számíthat fel az alábbiak szerint:

a) színes A/4: 150 Ft, A/3: 300 Ft;

b) fekete-fehér A/4: 50 Ft, A/3: 100 Ft;

c) postaköltség a mindenkori postai díjszabás szerint;

d) a kimutatások, másolatok összeállításához szükséges munkaerő-ráfordítás: bruttó 3000 Ft/óra (egész órára kerekítve).

(4) A másolat kiadásának fenti költségeiről az Adatkezelő (személyes adatokat kezelő egyetemi szervezeti egység) az érintettet a másolat igénylése során előzetesen köteles tájékoztatni. A másolat igénylésére vonatkozó jog nem érintheti hátrányosan mások jogait

és szabadságait, így a másolat más személyre vonatkozó adatot nem tartalmazhat. A jelen bekezdés szerinti szabályok nem vonatkoznak az Egyetem által készített kamerafelvételek másolatainak a kiadására, tekintettel arra, hogy ezen szabályokat a kamerarendszer üzemeltetésére vonatkozó belső szabályozó rögzíti.

Helyesbítés joga

9. §

(1) Az érintett kérheti az Adatkezelő (személyes adatokat kezelő egyetemi szervezeti egység) által kezelt, rá vonatkozó pontatlan személyes adatok helyesbítését és a hiányos adatok kiegészítését. A helyesbítés joga az eredetileg pontatlanul rögzített, valamint az adatkezelés ideje alatt megváltozott adatok tekintetében is megilleti az érintettet.

(2) A helyesbítéssel érintett új adatot az érintett az azt igazoló okmány, okirat, dokumentum bemutatásával igazolhatja, az Adatkezelő (személyes adatokat kezelő egyetemi szervezeti egység) pedig kijegyzetelés útján rögzíti. Amíg az új adat pontosan nem kerül igazolásra, az adatkezelés korlátozásra kerül a jelen Rendelkezés 11. §-a szerint. Nincs szükség a megváltozott és/vagy helyesbíteni kért adat igazolására, amennyiben az adat eredeti szolgáltatása során sem volt szükség az adat valódiságának igazolására.

(3) A helyesbítéssel érintett korábbi adat az új, javított adattal véglegesen felülírásra kerül.

(4) A helyesbítés, a korábbi adatok felülírása nem terjed ki olyan adatokra, amelyeknél ez a gyakorlatban értelmezhetetlen, kivitelezhetetlen (pl.: elektronikus megfigyelő- és rögzítőrendszerrel rögzített felvétel, hangfelvétel). Ezen adatok tekintetében a helyesbítés csak az adatkezelés tévesen rögzített körülményeire (pl.: téves dátum, időpont) terjedhet ki.

(5) A helyesbítés joga nem egyezik meg az érintett azon kötelezettségével, hogy vonatkozó belső szabályozók szerint mind a munkavállalók, mind a hallgatók és más érintettek kötelesek az adataikban bekövetkezett változást a belső szabályozókban rögzített határidőn belül az Egyetem tudomására hozni.

Törléshez való jog

10. §

(1) Az érintett az alábbi indokok valamelyikének fennállása esetén jogosult arra, hogy kérésére az Adatkezelő (személyes adatokat kezelő egyetemi szervezeti egység) indokolatlan késedelem nélkül törölje a rá vonatkozó személyes adatokat amennyiben:

a) a személyes adatokra már nincs szükség abból a célból, amelyből azokat gyűjtötték vagy más módon kezelték;

b) az érintett visszavonja az adatkezelés alapját képező hozzájárulását, és az adatkezelésnek nincs más jogalapja;

c) az érintett tiltakozik az adatkezelés ellen, és nincs elsőbbséget élvező jogszerű ok az adatkezelésre;

d) a személyes adatokat jogellenesen kezelték;

e) a személyes adatokat az adatkezelőre alkalmazandó uniós vagy tagállami jogban előírt jogi kötelezettség teljesítéséhez törölni kell;

f) a személyes adatok gyűjtésére információs társadalommal összefüggő szolgáltatások kínálásával kapcsolatosan került sor.

(2) A fenti indokok valamelyikének fennállása esetén az érintett által megjelölt adatokat törölni kell minden, az Egyetem által kezelt adatbázisból. A fenti kötelezettség teljesítése érdekében az Adatkezelő (személyes adatokat kezelő egyetemi szervezeti egység) az adatvédelmi kapcsolattartókat értesíti az adatok törléséről. Amennyiben az adatok törlése informatikai megoldással központilag lehetséges, az informatikai területet is értesíteni kell.

(3) Az adatok törlése nem kezdeményezhető, ha az adatkezelés:

a) a véleménynyilvánítás szabadságához és a tájékozódáshoz való jog gyakorlása céljából;

b) a személyes adatok kezelését előíró, az adatkezelőre alkalmazandó uniós vagy tagállami jog szerinti kötelezettség teljesítése és/vagy

c) közérdekből vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlása keretében végzett feladat végrehajtása céljából;

d) a népegészségügy területét érintő közérdekből, vagy

e) közérdekű archiválási, tudományos és történelmi kutatási célból, illetve statisztikai célból, végül

f) jogi igények előterjesztéséhez, érvényesítéséhez és/vagy védelméhez szükséges.

Az adatkezelés korlátozásához való jog

11. §

(1) Az érintett kérésére az Adatkezelő (személyes adatokat kezelő egyetemi szervezeti egység) korlátozza az adatkezelést, ha az alábbi feltételek valamelyike teljesül:

a) az érintett vitatja a személyes adatok pontosságát, ez esetben a korlátozás arra az időtartamra vonatkozik, amely lehetővé teszi a személyes adatok pontosságának ellenőrzését;

b) az adatkezelés jogellenes, és az érintett ellenzi az adatok törlését, és ehelyett kéri azok felhasználásának korlátozását;

c) az adatkezelőnek már nincs szüksége a személyes adatokra adatkezelés céljából, de az érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez; vagy

d) az érintett tiltakozott az adatkezelés ellen; ez esetben a korlátozás arra az időtartamra vonatkozik, amíg megállapításra nem kerül, hogy az adatkezelő jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben.

(2) A személyes adatok kezelésének korlátozása a tárolt személyes adatok megjelölése jövőbeli kezelésük korlátozása céljából. A korlátozás történhet a szóban forgó személyes adatoknak egy másik adatkezelő rendszerbe történő ideiglenes áthelyezésével, a felhasználók számára való hozzáférhetőségük megszüntetésével, az éles adatbázisból történő ideiglenes törlésével, elkülönítésével. Az adatkezelés korlátozását az automatizált nyilvántartási rendszerekben alapvetően technikai eszközökkel kell biztosítani, oly módon, hogy a személyes adatokon további adatkezelési műveleteket ne végezzenek el és azokat ne lehessen megváltoztatni.

(3) Ha az adatkezelés korlátozás alá esik, a személyes adatokat a tárolás kivételével csak az érintett hozzájárulásával, vagy jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez, vagy más természetes vagy jogi személy jogainak védelme érdekében, vagy az Unió, és/vagy valamely tagállam fontos közérdekéből lehet kezelni.

(4) Az Adatkezelő (személyes adatokat kezelő egyetemi szervezeti egység) az érintettet az adatkezelés korlátozásának feloldásáról előzetesen tájékoztatja.

Adathordozáshoz való jog

12. §

(1) Az érintett jogosult arra, hogy a rá vonatkozó, általa az Adatkezelő (személyes adatokat kezelő egyetemi szervezeti egység) rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja, és ezeket az adatokat egy másik adatkezelőnek továbbítsa, és/vagy arra, hogy kérje a személyes adat közvetlen továbbítását egy általa megjelölt másik adatkezelőhöz.

(2) A 2013/37/EU irányelv alapján egy dokumentum akkor tekinthető számítógéppel olvasható formátumú dokumentumnak, ha olyan fájlformátumú, amely lehetővé teszi a szoftveres alkalmazások számára, hogy a benne lévő egyedi adatokat könnyen azonosítsák, felismerjék és kinyerjék.

(3) Az adathordozhatóság joga kizárólag az érintett hozzájárulása vagy a GDPR 6. cikk (1) bekezdésének b) pontján alapuló adatkezelés esetén (az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél, vagy az a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges) illeti meg az érintettet, és kizárólag akkor, ha az adatkezelés automatizált módon történik. Az adathordozhatóság a kezelt adatokra vonatkozik, az azokból származtatott, az adatkezelés során az Egyetemnél keletkezett adatokat nem kell a fentiek szerint kiadni.

Tiltakozás joga

13. §

(1) Az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból bármikor tiltakozzon személyes adatainak az Adatkezelő (személyes adatokat kezelő egyetemi szervezeti egység) vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges kezelése ellen.

(2) Tiltakozás esetén az érintett egyetemi szervezeti egység a személyes adatokat nem kezelheti tovább, kivéve, ha azt olyan kényszerítő erejű jogos okok indokolják, amelyek elsőbbséget élveznek az érintett érdekeivel, jogaival és szabadságaival szemben, vagy amelyek jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódnak.

(3) Ha a személyes adatok kezelése közvetlen üzletszerzés érdekében történik, az érintett jogosult arra, hogy bármikor tiltakozzon a rá vonatkozó személyes adatok e célból történő kezelése ellen, ideértve a profilalkotást is, amennyiben az a közvetlen üzletszerzéshez kapcsolódik. A személyes adatok közvetlen üzletszerzés érdekében történő kezelése elleni tiltakozás esetén az adatokat e célból az Adatkezelő (személyes adatokat kezelő egyetemi szervezeti egység) többé nem kezeli. Az érintett kérése alapján az Adatkezelő (személyes adatokat kezelő egyetemi szervezeti egység) felfüggeszti az adatkezelést a tiltakozás érdemi elbírálásáig.

Automatizált döntéshozatal egyedi ügyekben, beleértve a profilalkotást

14. §

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

(2) Nem alkalmazható a fenti jogosultság, ha az adatkezelés:

a) az érintett és az Egyetem közötti szerződés megkötése vagy teljesítése érdekében szükséges;

b) meghozatalát az Egyetemre alkalmazandó olyan uniós vagy tagállami jog teszi lehetővé, amely az érintett jogainak és szabadságainak, valamint jogos érdekeinek védelmét szolgáló megfelelő intézkedéseket is megállapít; vagy

c) az érintett kifejezett hozzájárulásán alapul.

Az adatkezelési hozzájárulás visszavonásának a joga

15. §

(1) Az érintett jogosult arra, hogy hozzájárulását bármikor visszavonja. A hozzájárulás visszavonása nem érinti a hozzájáruláson alapuló, a visszavonás előtti adatkezelés jogszerűségét. Az érintett hozzájárulása alapján kezelt adatokat annak visszavonása után az adatokat kezelő egyetemi szervezeti egység törli, kivéve, ha az adatok kezelése más jogalap szerint tovább folytatódhat.

III. AZ ÉRINTETT JOGOK GYAKORLÁSÁRA VONATKOZÓ ELJÁRÁSI SZABÁLYOK

Az érintettek köre és az adatvédelmi megkeresési lehetőségeik

A kérelem azonosítása

16. §

(1) Amennyiben a megkeresést fogadó munkavállalónál vagy szervezeti egység vezetőjénél kétség merül fel a megkeresés tárgyát képező adatok személyes adat volta iránt, vagy azzal kapcsolatban, hogy a megkeresés érintetti joggyakorlásnak minősül-e, úgy a jogi vezetőhöz fordul.

A kérelem teljesítése

17. §

(1) A kérelem címzettjeként eljáró Adatkezelő (személyes adatokat kezelő egyetemi szervezeti egység) az érintett jelen Rendelkezésben foglalt jogai jogszerű gyakorlására irányuló kérelmének a teljesítését csak akkor tagadhatja meg, ha bizonyítja, hogy az érintettet – szándéka ellenére – nem áll módjában azonosítani.

(2) Az érintett részére kérésére – személyazonosságának hitelt érdemlő igazolását és beazonosítását követően – szóban is teljesíthető a jogai gyakorlására irányuló kérelme.

(3) A személyazonosság igazoltnak tekinthető abban az esetben, ha a jogok gyakorlására irányuló kérelem az Egyetem által kezelt elérhetőségről (e-mail cím, cím, telefonszám) érkezik. Tekintettel arra, hogy ekkor sincs kizárva annak lehetősége, hogy valaki más nevében és e-mail címéről írjon elektronikus levelet, kellő körültekintéssel kell eljárni, és a választ – az érintett esetleges külön kérésének ellenére is – csak az ismert elérhetőségre lehet megküldeni.

(4) Egyéb csatornán történő megkeresések (pl. személyes, online kapcsolati űrlap vagy telefonszám) esetén az alábbi azonosító adatok közül legalább hármat kell az érintettnek megadnia:

a) név;

b) születési név;

c) születési hely, idő;

d) anyja neve.

(5) Különleges esetekben (pl. hangfelvétel vagy kamerás videófelvétel kapcsán) az azonosítás a fenti módszerekkel nem lehetséges. Ilyenkor is törekedni kell az érintett beazonosítására, pl.: a hang összevetésével, a hangfelvétel dátumának, időpontjának, hosszának, témájának azonosításával.

Az adatvédelmi tisztviselő közvetlen megkeresése

18. §

(1) Az Egyetem biztosítja mind a külső partnerek és más természetes személyek, mind a munkavállalók és hallgatók számára, hogy az adatvédelmi tisztviselő közvetlen e-mail címe számukra mint érintettek számára elérhető legyen a közvetlen megkereshetőség érdekében.

Intézkedés határideje

19. §

(1) Az Adatkezelő (személyes adatokat kezelő egyetemi szervezeti egység) vezetője a hozzá elektronikus úton beérkező panaszok és megkeresések ügyében haladéktalanul, de legkésőbb három (3) munkanapon belül köteles intézkedéseket tenni.

Címzettek tájékoztatása

20. §

(1) Az Adatkezelő (személyes adatokat kezelő egyetemi szervezeti egység) minden olyan címzettet tájékoztat a jelen Rendelkezés szerint végrehajtott helyesbítésről, korlátozásról vagy törlésről, akivel az adatokat közölték.

(2) A tájékoztatás kiterjed az érintett azonosítására és a helyesbített, korlátozott vagy törölt adat pontos megjelölésére. A jelen § szerinti értesítés nem szükséges, ha ez lehetetlen, vagy aránytalanul nagy erőfeszítést igényel.

A kérelem adatainak a kezelése

21. §

(1) A jelen Rendelkezés szerinti megkeresések teljesítése során keletkezett adatokat a megkeresést teljesítő szervezeti egység az érintett adattal együtt, annak törlési határidejéig, valamint az esetlegesen a kérelem teljesítésével összefüggésben érvényesített jogi igény elévüléséig kezeli. Az átláthatóság elvének megfelelően a megkeresések, intézkedések és az adott válaszok nyilvántartását az érintett szervezeti egység vezetője vezeti.

Külső megkeresések

22. §

(1) Bármely érintett (pályázó, jelentkező, partner, volt hallgató stb.) bármilyen formában élhet adatainak kezelésével kapcsolatos megkereséssel, és/vagy panasszal az Egyetem bármely, személyes adatokat kezelő szervezeti egysége felé, azokat a megkeresett egyetemi szervezeti egységek kezelni kötelesek.

(2) Az érintett szóbeli panaszát, kérését a szervezeti egység vezetője vagy annak helyettese által felvett jegyzőkönyvben rögzíti.

(3) A szervezeti egység vezetője a megkeresésben foglaltak alapján a tervezett intézkedésekről javaslatot készít és azt a jegyzőkönyvvel együtt a jegyzőkönyv keltétől számított hét (7) munkanapon belül megküldi jóváhagyásra az adatvedelem@uni-corvinus.hu e-mail címre. Az érintett szervezeti egység vezetője a jogi vezető jóváhagyása nélkül az adatkezeléssel kapcsolatos panaszokat (érintetti joggyakorlásnak minősülő megkereséseket) nem válaszolhatja meg, az azokban foglalt kéréseket, igényeket nem teljesítheti, a megkeresésekre nem válaszolhat.

(4) A jogi vezető legkésőbb három (3) munkanapon belül a rendelkezésére álló adatok alapján megvizsgálja az esetet és jóváhagyás esetén értesíti a szervezeti egység vezetőjét, hogy a panasz, illetve megkeresés kezelését az általa jóváhagyott javaslat szerint kezdje meg.

(5) Amennyiben a megkeresés közvetlenül az adatvédelmi tisztviselőhöz érkezik, a tisztviselő a megkeresést állásfoglalásával együtt az ügy kivizsgálása céljából az illetékes szervezeti egység vezetőjének megküldi. A szervezeti egység vezetője a jelen Rendelkezés 16. §- 21. §-ban foglaltak szerint jár el.

(6) A megkereséssel érintett egyetemi szervezeti egység indokolatlan késedelem nélkül, de legkésőbb a kérelem beérkezésétől számított egy (1) hónapon belül köteles tájékoztatni az érintettet a kérelem nyomán hozott intézkedésekről. Szükség esetén, figyelembe véve a kérelem összetettségét és a kérelmek számát, ez a határidő a jogi vezető döntése alapján kivételes esetben, további két (2) hónappal meghosszabbítható. A határidő meghosszabbításáról a kérelem kézhezvételétől számított egy (1) hónapon belül a késedelem okainak megjelölésével az érintettet az ügyben eljáró szervezeti egység vezetője tájékoztatja.

(7) Ha az érintett elektronikus úton nyújtotta be a kérelmet, az információkat a megkeresett egyetemi szervezeti egység is elektronikus formátumban bocsátja az érintett rendelkezésére, kivéve, ha az érintett másként kéri.

(8) Amennyiben az érintett telefon keresztül fordul az Egyetem bármely szervezeti egységéhez az adatkezelésével kapcsolatos panasszal és/vagy megkereséssel, az érintettet tájékoztatni kell az adatvédelmi tisztviselő elérhetőségéről.

Munkavállalói megkeresések

23. §

(1) A munkavállalói adatkezeléssel kapcsolatos panaszát és/vagy kérelmét az érintett illetékesség szerint a HR-hez és/vagy a Pénzügyhöz címzett megkeresésével nyújthatja be. A HR és/vagy a Pénzügy a válasz összeállítása érdekében hét (7) munkanapon belül a megkeresésben foglaltak teljesítéséhez szükséges más szervezeti egységhez, valamint a jogi vezetőhöz fordul, akik három (3) munkanapon belül kötelesek a válasz összeállításhoz szükséges adatokat, valamint a jogi állásfoglalást megadni, amennyiben az szükséges. Az ügyintézés határidejére a jelen Rendelkezés 17. §–21. §-aiban foglalt határidők az irányadók. A HR és/vagy a Pénzügy a jogi vezető jóváhagyása után az adatkezeléssel kapcsolatos panaszokra (érintetti joggyakorlásnak minősülő megkeresésekre),

megkeresésekre válaszol, az abban foglalt kéréseket teljesíti vagy amennyiben annak jogszerű feltételei fennállnak elutasítja.

Hallgatói megkeresések

24. §

(1) A hallgatói adatkezeléssel kapcsolatos panaszát és/vagy kérelmét az érintett illetékesség szerint a Hallgatói Szolgáltatásokhoz (HSZ) vagy a Corvinus Doktori Iskolákhoz (CDI) címzett megkeresésével nyújthatja be. A HSZ a válasz összeállítása érdekében hét (7) munkanapon belül a megkeresésben foglaltak teljesítéséhez szükséges más szervezeti egységhez, valamint a jogi vezetőhöz fordul, akik három (3) munkanapon belül kötelesek a válasz összeállításhoz szükséges adatokat, valamint a jogi állásfoglalást megadni, amennyiben az szükséges. Az ügyintézés határidejére a jelen Rendelkezés 17. §–21. §-aiban foglalt határidők az irányadók. A HSZ a jogi vezető jóváhagyása után az adatkezeléssel kapcsolatos panaszokra (érintetti joggyakorlásnak minősülő megkeresésekre), megkeresésekre válaszol, az abban foglalt kéréseket teljesíti, vagy amennyiben annak jogszerű feltételei fennállnak elutasítja.

Az Egyetem tájékoztatási kötelezettsége a jogorvoslatról

25. §

(1) Ha az érintett szervezeti egység vezetője nem tesz intézkedéseket az érintett kérelme nyomán, vagy a kérelem kifejezetten elutasításra kerül, késedelem nélkül, de legkésőbb a kérelem beérkezésétől számított egy (1) hónapon belül a válaszadásra köteles szervezeti egység tájékoztatja az érintettet az intézkedés elmaradásának okairól, valamint arról, hogy az érintett panaszt nyújthat be a Nemzeti Adatvédelmi és Információszabadság Hatóságnál és élhet bírósági jogorvoslati jogával. Az elutasításra vonatkozó válaszlevelet a jogi vezető állítja össze.

IV. TÁJÉKOZTATÁS A SZEMÉLYES ADATOK KEZELÉSÉRŐL

Általános tájékoztatási kötelezettségek

26. §

(1) Minden esetben, amikor személyes adatok kezelésére kerül sor (akár munkavállalói, akár más foglalkoztatási jogviszonyban dolgozó személy, akár külső partner, akár hallgató vagy jelentkező esetében), az adatok kezelésének megkezdését megelőzően az adatkezelésért felelős vezető köteles a jogi vezető közreműködésével az érintettek számára adatkezelési tájékoztatót összeállítani és hozzáférhetővé tenni a jelen Rendelkezés 7. §-a szerint.

(2) Az adatkezelési tájékoztatóban minden esetben ki kell térni az

a) adatkezelés érintettjeire;

b) az adatvédelmi tisztviselő nevére és elérhetőségére;

c) adatkezelés céljára;

d) a kezelt adatok körére;

e) adatkezelés időtartamára, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjaira;

f) adatkezelés jogalapjára;

g) amennyiben az adatkezelés jogalapja az Egyetem jogos érdeke, a jogos érdek rövid ismertetésére;

h) amennyiben az adatkezelés jogalapja az érintett hozzájárulása, a hozzájárulás bármely időpontban történő visszavonásához való jogra, amely nem érinti a visszavonás előtt a hozzájárulás alapján végrehajtott adatkezelés jogszerűségét;

i) esetlegesen igénybe vett adatfeldolgozók vagy más címzettek személyére;

j) amennyiben az adatokat harmadik országba továbbítja az Egyetem, az alkalmazott jogi eszközre;

k) az érintetti jogok gyakorlásának rendjére;

l) a Nemzeti Adatvédelmi és Információszabadság Hatósághoz fordulás jogára;

m) arra, hogy a személyes adat szolgáltatása jogszabályon vagy szerződéses kötelezettségen alapul vagy szerződés kötésének előfeltétele-e, valamint, hogy az érintett köteles-e a személyes adatokat megadni, továbbá, hogy milyen lehetséges következményekkel járhat az adatszolgáltatás elmaradása.

(3) Az adatkezelési tájékoztatót minden esetben az adatkezelésért felelős vezető és/vagy az adatvédelmi kapcsolattartó közreműködése mellett a jogi vezető állítja össze. Az adatkezelési tájékoztató igénylése a jogi vezető által rendszeresített online űrlap kitöltésével igényelhető.

(4) Az elkészített adatkezelési tájékoztatót úgy kell az érintettek számára hozzáférhetővé tenni, hogy utólag az igazolható legyen (elszámoltathatóság elve). Megfelelő eljárás, ha az érintettek számára e-mail-ben küldik el a tájékoztató szövegét, vagy a tájékoztatóra mutató kattintható linket, ahogy szintén megfelelő, ha egy online regisztrációs felületen a regisztráció befogadása technikailag csak az adatkezelési tájékoztatóra mutató kattintható link melletti rubrika bepipálását követően lehetséges. Az alkalmazott tájékoztatási folyamat kialakítása az adatkezelésért felelős vezető feladata, aki a megfelelőség kétségessége esetén köteles a jogi vezető véleményét kikérni. Az adatkezelési tájékoztatás megtörténtét (a hozzáférhetőség utólagos igazolhatóságára vonatkozó adatokat) az adatkezelésért felelős szervezeti egység öt (5) évig, vagy a tájékoztatással összefüggésben esetlegesen érvényesített jogi igény elévüléséig tárolja a jelen Rendelkezés 5. §(5) bekezdés a) pontja szerint.

Különös tájékoztatási kötelezettségek

27. §

(1) A valamennyi jelentkezőt érintő adatkezelések esetében az adatkezelést a Felvételi Adatkezelési Tájékoztatóban (FAT) rögzíteni kell. Valamennyi jelentkezőre vonatkozó

adatkezelésnek minősül az adatkezelés, amennyiben az minden, az adott képzéstípusra jelentkezőt érint (pl.: alapképzés, mesterképzés, doktori képzés, mobilitás). A FAT elérhetőségéről, valamint ennek tudomásulvételéről a jelentkezőket a jelentkezés során a jelentkezési csatorna (FELVI, DreamApply, Mobility stb.) függvényében papíron vagy online formában nyilatkoztatni szükséges. A tájékoztatásért az adott jelentkezési csatornán a jelentkezések fogadásáért és feldolgozásáért felelős szervezeti egység felel. A tájékoztatási folyamat kialakításával összefüggésben az adatkezelésért felelős vezetőt kérésére a jogi vezető állásfoglalásával segíti. A FAT tartalmáért és frissítésért a jogi vezető felel azzal, hogy a jelentkezések fogadásáért és feldolgozásáért felelős szervezeti egység felelős az adatkezelésben bekövetkező változás jogi vezetővel történő közléséért.

(2) Amennyiben az adatkezelés valamennyi hallgatót érint, azt a Hallgatói Adatkezelési Tájékoztatóban (HAT) rögzíteni kell. A HAT szerinti adatkezelésekről a hallgatók tájékoztatása a beiratkozási lap és/vagy képzési szerződés megkötésén keresztül történik, amely során a képzési szerződésben egy külön pont meghivatkozza a HAT elérhetőségét, valamint a szerződés rögzíti, hogy a hallgató annak aláírásával a HAT rendelkezéseit tudomásul veszi. A HAT tartalmáért és frissítéséért a jogi vezető felel azzal, hogy a hallgatói tanulmányi adminisztrációért felelős szervezeti egység felelős az adatkezelésben bekövetkező változás jogi vezetővel történő közléséért.

(3) Amennyiben az adatkezelés valamennyi munkavállalót érint, azt a Munkavállalói Adatkezelési Tájékoztatóban (MAT) rögzíteni kell. A MAT szerinti adatkezelésekről a munkavállalók tájékoztatása a munkaszerződés megkötésén keresztül történik, mely során a munkaszerződésben egy külön pont meghivatkozza a MAT elérhetőségét, valamint a szerződés rögzíti, hogy a munkavállaló annak aláírásával a MAT rendelkezéseit tudomásul veszi. A MAT tartalmáért és frissítéséért a jogi vezető felel azzal, hogy adott HR/munkavállaló ügyintézési folyamatért felelős szervezeti egység felelős az adatkezelésben bekövetkező változás jogi vezetővel történő közléséért.

(4) Minden egyéb esetben az adatkezelésért felelős vezető a vezetése alatt álló és/vagy az irányításával működő területen folyó adatkezelések tekintetében felelős a szükséges adatkezelési tájékoztató elkészítéséért a jogi vezető irányítása mellett a jelen Rendelkezés 26. §-a szerint.

V. A SZEMÉLYES ADATOK TÖRLÉSÉVEL KAPCSOLATOS SZABÁLYOK

Az adatok törlése

28. §

(1) A személyes adatokat kezelő egyetemi szervezeti egységek az általuk végzett adatkezelések során kötelesek gondoskodni a személyes adatok törléséről, amennyiben az adott adatkezeléshez definiált adatmegőrzési időtartam eltelt.

(2) A jelen Rendelkezés 3. melléklete szerinti tartalommal köteles minden Adatkezelő (személyes adatokat kezelő egyetemi szervezeti egység) rögzíteni, hogy az adott terület által végzett különböző adatkezelések esetében mikor kell az adatokat törölni. Az adatok

törlési határidejére vonatkozóan a Hallgatói, valamint a Munkavállalói adatkezelési tájékoztatóban rögzített határidők az irányadók. Egyéb adatkezelések esetén az adott adatkezelésre vonatkozó Adatkezelési Tájékoztató az irányadó. Kétség esetén a jogi vezető állásfoglalását kell kérni. Minden adatkezelésért felelős vezető köteles a jelen utasítás kiadását követő száznyolcvan (180) napon belül a jelen Rendelkezés 3. melléklete szerinti törlési folyamatleírást elkészíteni.

(3) Annak naprakészen tartása, hogy egy adott szervezeti egység milyen adatkezeléseket végez, az adott terület vezetőjének a felelőssége a jelen Rendelkezés 5. §(2) bekezdés a) pontja szerint.

(4) A lejárt adatkezelési határidejű adatok törléséről az adott szervezeti egység vezetője gondoskodik, mely feladat elvégzésében az adatvédelmi kapcsolattartókra támaszkodik. Amennyiben az adatok törlése informatikai úton is lehetséges, a megoldással kapcsolatban a vezető köteles az Informatikai vezetőjével egyeztetni. A rendelkezésre álló informatikai és költségkeretek között törekedni kell az adatok automatikus törlésére. Az adatok törlésére vonatkozó eljárás kidolgozásába lehetőség szerint be kell vonni a jogi vezetőt.

(5) A személyes adatokat kezelő szervezeti egység vezetőjének a felelőssége az irányítási területéhez tartozó törlési folyamatleírásnak megfelelő, valós törlési mechanizmus működtetése. Minden, a törlési folyamatban bekövetkező változást a vezető harminc (30) napon belül frissít. A vezető jelen pont szerinti kötelezettsége teljesítésében a jogi vezető a kérésére segíti.

(6) Amennyiben az adatok törlésében külső vállalkozó is közreműködik (adatfeldolgozó), a személyes adatokat kezelő szervezeti egység vezetője köteles a fenti adatkezelések törlésében közreműködő adatfeldolgozóival a GDPR 28. cikkében foglaltaknak megfelelő tartalmú adatfeldolgozási szerződést kötni, melyben rögzíteni kell az egyes adatkezelésekhez tartozó törlési határidőket. A vezető kérésére az adatfeldolgozási szerződés tervezetét a jogi vezető készíti el.

VI. ADATVÉDELMI INCIDENSEK

Az adatvédelmi incidensek kezelése

29. §

(1) Adatvédelmi incidensnek minősül a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi.

(2) Az incidens fizikai, vagyoni vagy nem vagyoni károkat okozhat a természetes személyeknek, többek között:

a) a személyes adataik feletti rendelkezés elvesztését vagy a jogaik korlátozását;

b) hátrányos megkülönböztetést;

c) személyazonosság-lopást vagy hasonló visszaélést;

d) pénzügyi veszteséget;

e) az álnevesített (pszeudonim) adatok jogosulatlan személyhez kötését;

f) a jó hírnév sérelmét;

g) a szakmai titoktartási kötelezettséggel védett személyes adatok bizalmasságának sérülését;

h) illetve egyéb jelentős gazdasági vagy szociális hátrányt.

(3) Az incidensek jellegüknél fogva az alábbiak szerint csoportosíthatóak:

Az adatok megsemmisülése	A személyes adat • többé nem létezik, vagy • nem létezik többé a korábbi, felhasználható formájában.
Adatvesztés	A személyes adat ugyan még létezik, • de az érintett többé nem képes hozzáférni, vagy • az adat kikerült az érintett birtokából. <u>Példák</u>: • adathordozó elvesztése/lopása (USB stick, laptop stb.), vagy • az adatok egyetlen példánya titkosított, vagy • a titkosított adatok kulcsa elvész
Adatmódosulás	A személyes adat • tartalma megváltozott, vagy • az adatok nem teljesek, vagy • az adatok olvashatatlanok.
Az adatok nyilvánosságra kerülése	Az adatokat • olyan személyek kapják meg, akik arra nem jogosultak, vagy • az adatokat olyan személyek is megismerik, akik arra nem jogosultak. <u>Példák:</u> • hacker támadás • téves közzététel • adathordozók elvesztése

Az adatvédelmi incidensek csoportosítása

30. §

(1) Az Adatkezelő (személyes adatokat kezelő egyetemi szervezeti egység) feladata a tudomására jutott incidensek elemzése és értékelése abból a célból, hogy az incidenskezeléshez szükséges további megfelelő intézkedéseket megtegye.

(2) Az incidensek súlyosságuk szerinti csoportosítása:

a) Jelentéktelen (bagatell) incidensek: valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve.

b) Kockázattal járó incidens: csak minimális sérelmet kilátásba helyező, és akár egyetlen természetes személyt érintő adatvédelmi incidens is ide sorolandó.

c) Valószínűsíthetően magas kockázattal járó incidensek:

ca) a hátrányos helyzet fennállását egyrészt az adatok jellege és tartalma alapján lehet megítélni (pl.: pénzügyi információk vagy különleges adatok, helymeghatározó adatok, internetes naplófájlok, böngészési előzmények, elektronikus levelezési adatok és tételes híváslisták;

cb) másrészt az incidens várható következményei alapján (pl. ha az személyes adattal visszaéléshez, testi épség sérelméhez, becsületsértéshez, rágalmazáshoz vagy a jóhírnév sérelméhez vezethet);

cc) végül az incidens körülményei is relevánsak lehetnek (pl. ha a Btk. szerinti tiltott adatszerzés vagy információs rendszer vagy adat megsértése, valamint az információs rendszer védelmét biztosító technikai intézkedés kijátszása, bűncselekmény gyanúja merül fel).

(3) Az adatvédelmi incidensek besorolásának szempontjait a jelen Rendelkezés 4. melléklete tartalmazza.

Példák az adatvédelmi incidensre

31. §

(1) A kezelt személyes adatokkal kapcsolatban adatvédelmi incidenst, azaz személyes adat jogellenes kezelését vagy feldolgozását, így különösen jogosulatlan hozzáférést, megváltoztatást, továbbítást, nyilvánosságra hozatalt, törlést vagy megsemmisítést, valamint véletlen megsemmisülést és sérülést valószínűsíthetően különösen, de nem kizárólag az alábbi helyeken, tevékenységek során észlelhet a munkavállaló vagy az adatok kezelésével, feldolgozásával megbízott más személy:

a) elektronikus megfigyelő- és rögzítőrendszer igénybevételével felvételek nem szándékolt (vagy szándékosan szabálytalan) jogosulatlan készítése, és/vagy azok határidőn túli szándékolatlan tárolása, és/vagy illetéktelenek számára történő hozzáférhetővé tételével;

b) fényképfelvételek szándék ellenére történő készítése, és/vagy ezen felvételek határidőn túli szándékolatlan (vagy szándékosan szabálytalan) tárolása, és/vagy illetéktelenek számára történő hozzáférhetővé tételével;

c) álláshirdetésre történő toborzások alkalmával az adatkezelő szándékán túl a szükségesnél több adat felvétele, illetve a jelentkezők adatainak határidőn túli szándékolatlan tárolása;

d) az érintett kérésére történő hírlevélről leiratkozás esetén az adatok nem kerülnek ténylegesen és haladéktalanul törlésre;

e) zsarolóvírus támadása titkosítja az Egyetem adatbázisait (pl. a hírlevél-küldéshez kapcsolódó hallgatói adatbázisokat);

f) az Egyetem fennhatósága alól kikerülő személyes adatokat tartalmazó adatbázisok. (A munkavállaló munkaeszközéről jogosulatlanul adatokat nyer ki, azokat jogosulatlan személyeknek hozzáférhetővé tesz vagy személyes adatokat tartalmazó munkaeszközét munkavégzésének helyéről jogosulatlanul elvisz.);

g) kibertámadás veszélyezteti az Egyetem által kezelt adatbázisokat (pl. egy hackeroldalon megjelenik egy regisztrációs adatbázisrész);

h) adatkezelési határidő lejártát követően nem megfelelően tárolt, selejtezett iratok, egyéb adathordozók;

i) rossz címzettnek küldött postai küldemény vagy e-mail, vagy jogosulatlan címzettek megjelölése másolatként e-mail küldése során;

j) adathordozók (laptop, táblagép, mobiltelefon) meghibásodásának azon esetei, amelyek a személyes adatok biztonságát, integritását veszélyeztetik, és/vagy ezen adathordozók, illetve ezen adathordozók ellopása, elvesztése;

k) személyes adatokhoz történő jogosulatlan hozzáférés rosszul beállított jogosultságkezelés miatt;

l) munkaviszony megszűnése utáni jogosulatlan hozzáférés;

m) egyéb külső rosszindulatú támadások;

n) adathalász (phising) levelek esetén adatok megadása.

Szervezeten belüli feladatok és felelősségek

32. §

(1) Az a munkavállaló, vagy az Egyetem részére munkaviszonyon túli egyéb foglalkoztatási jogviszony keretében munkát végző, aki az Egyetem bármely szervezeti egysége által kezelt vagy feldolgozott személyes adatokkal kapcsolatban adatvédelmi incidenst, azaz személyes adat jogellenes kezelését vagy feldolgozását, így különösen jogosulatlan hozzáférést, megváltoztatást, továbbítást, nyilvánosságra hozatalt, törlést vagy megsemmisítést, valamint véletlen megsemmisülést és sérülést észlel, azt köteles a közvetlen vezetője útján a tudomásszerzést követően haladéktalanul bejelenteni a jelen Rendelkezés 5. melléklete szerinti adatkörrel a jogi vezetőnek. A bejelentő további olyan

információkat is megadhat, amelyeket az incidens beazonosítása, megvizsgálása szempontjából lényegesnek ítél.

(2) Tudomásszerzésnek az tekinthető, amikor a munkavállaló ésszerű mértékű bizonyossággal rendelkezik arról, hogy olyan biztonsági esemény történt, amely személyes adatokkal kapcsolatos jogellenes műveletekhez vezethet. Az incidenssel érintett szervezeti egység vezetője azonnali vizsgálatot kezdeményez annak megállapítására, hogy történt-e adatvédelmi incidens, és ha igen, milyen intézkedések szükségesek.

(3) Az Egyetem az adatvédelmi incidensek jelentésére dedikált e-mail címet hoz létre és biztosítja azok 24 órán át történő elérhetőségét. Adatvédelmi incidens bejelentésére szolgáló e-mail cím: adatvedelem@uni-corvinus.hu

Szervezeten kívülre mutató intézkedések

33. §

(1) Minden Adatkezelő (személyes adatokat kezelő egyetemi szervezeti egység) – amennyiben külső adatfeldolgozó szolgáltatását veszi igénybe – köteles olyan tartalmú adatfeldolgozói szerződést kötni a megbízott adatfeldolgozóval, amely biztosítja, hogy az adatfeldolgozó az általa észlelt adatvédelmi incidenst a jelen Rendelkezésben foglaltak szerint kezeli.

Szervezeti szintű intézkedések

34. §

(1) A jogi vezető eljár a hozzá beérkező incidensjelentések kapcsán, így megvizsgálja, hogy az incidens mekkora adatvédelmi kockázatot képvisel, majd dönt, hogy az incidenst a Nemzeti Adatvédelmi és Információszabadság Hatóságnak bejelenteni szükséges-e (a mérlegelés szempontjait a jelen Rendelkezés 6. melléklete tartalmazza), valamint dönt arról is, hogy az incidensről az érintett(ek)et tájékoztatni szükséges-e.

(2) Amennyiben a jogi vezető az incidens körülményeinek az ismeretében úgy dönt, hogy a Nemzeti Adatvédelmi és Információszabadság Hatóságot és/vagy az érintetteket az incidensről nem szükséges tájékoztatni, a döntését megalapozó okokat, körülményeket dokumentálni köteles.

(3) Az incidenssel érintett szervezeti egység vezetőjének a feladata az észlelt adatvédelmi incidenssel összefüggésben az esemény kellő mélységű dokumentálása a jelen Rendelkezés 5. melléklete szerint, valamint az informatikai terület közreműködésével ésszerű, munkafolyamatokat nem befolyásoló sürgősségi intézkedések megtétele (jogellenes állapot mielőbbi felszámolása, így eszközök kikapcsolása, hozzáférések megszűntetése, biztonsági rések felszámolása, biztonsági másolatok helyreállítása, eredeti állapot visszaállítása), ha lehetséges, valamint hasonló esetek elkerülése érdekében a szükséges intézkedések felmérése.

(4) Az Egyetemen személyes adatok kezelését végző munkavállaló vagy más foglalkoztatási jogviszonyban álló személy a tevékenységi körén belül köteles az észlelt adatvédelmi

incidenst a közvetlen vezetőjének és rajta keresztül a jogi vezetőnek jelenteni jelen Rendelkezés 32. §-a szerint.

Incidensek nyilvántartása

35. §

(1) Az Egyetem által kezelt adatokat érintő incidens esetén a jogi vezető a bejelentést megvizsgálja, a bejelentőtől igény esetén további adatszolgáltatást kér, amelyet a bejelentő köteles haladéktalanul, de legkésőbb két (2) munkanapon belül teljesíteni.

(2) Az incidenst észlelő személy adatszolgáltatásának a jelen Rendelkezés 5. melléklete szerinti adatokat kell tartalmaznia.

(3) Az adatszolgáltatást követően a jogi vezető vizsgálatot végez. Amennyiben vizsgálatának eredményeképpen megállapítja, hogy a szóban forgó adat valóban személyes adat, illetve azt, hogy a bejelentés tartalma kimeríti az incidens fogalmát, úgy köteles az incidenst súlyossági fokozatától függetlenül nyilvántartásba venni.

(4) A nyilvántartásba rögzíteni kell:

a) az érintett személyes adatok körét;

b) az adatvédelmi incidenssel érintettek körét és számát;

c) az adatvédelmi incidens időpontját;

d) az adatvédelmi incidens körülményeit, hatásait;

e) az adatvédelmi incidens elhárítására megtett intézkedéseket;

f) az incidens besorolását (csak nyilvántartás/NAIH/érintett értesítése);

g) a besorolást elvégző személyek nevét;

h) a NAIH/érintetti értesítés időpontját és módját;

i) az adatkezelést előíró jogszabályban meghatározott egyéb adatokat.

A nyilvántartási és értesítési kötelezettség alanyai, tartalma

36. §

(1) Az adatszolgáltatás alapján a jogi vezető javaslatot tesz az adatvédelmi incidens elhárításához szükséges intézkedésekről az adatok kezelését vagy feldolgozását végző szervezeti egység vezetője számára.

(2) A javaslat alapján megvalósítandó további intézkedésekről az adatok kezelését vagy feldolgozását végző szervezeti egység vezetője dönt.

(3) Az adatvédelmi incidens elhárítása érdekében megvalósított egyes intézkedésekről az adatok kezelését vagy feldolgozását végző szervezeti egység vezetője az adott intézkedések végrehajtását követő két munkanapon belül köteles a jogi vezetőt tájékoztatni. A jogi vezető az adatvédelmi incidensekről nyilvántartást vezet, melynek az adatait köteles öt (5) évig, vagy az incidenssel összefüggésben esetlegesen érvényesített jogi igények elévüléséig megőrizni.

(4) Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, a jogi vezető javaslatára az incidenssel érintett szervezeti egység vezetője indokolatlan késedelem nélkül világos és közérthető módon tájékoztatja az érintettet az adatvédelmi incidensről az alábbi tartalommal:

a) az adatvédelmi tisztviselő neve és elérhetősége;

b) az adatvédelmi incidens jellege, következményei;

c) az adatvédelmi incidens orvoslására tett vagy tervezett intézkedések.

(5) Az érintettek incidensről való tájékoztatásához kifejezetten erre vonatkozó üzeneteket kell alkalmazni, amelyek nem küldhetők más jellegű tájékoztatással, például az aktualitásokról szóló rendszeres értesítésekkel, hírlevelekkel vagy szabványüzenetekkel együtt. Átlátható tájékoztatási módszer például a közvetlen üzenetküldés (például e-mail, SMS, közvetlen üzenet), a honlapon kiemelt helyen megjelenített szalaghirdetés vagy értesítés, a postai úton történő tájékoztatás, valamint a nyomtatott sajtóban megjelenő kiemelt hirdetés. A kizárólag sajtóközleményre vagy egyetemi blogbejegyzésre korlátozódó értesítéssel nem lehet hatékonyan tájékoztatni az egyéneket az incidensről.

(6) Amennyiben az érintetteket értesíteni szükséges a bekövetkezett adatvédelmi incidensről, olyan megoldást kell választani, amellyel a legnagyobb az esély arra, hogy minden érintettet megfelelően tájékoztatnak.

(7) Amennyiben az érintett értesítése válik szükségessé, azon esetekben a Nemzeti Adatvédelmi és Információszabadság Hatóság értesítése is minden esetben kötelező, melynek a teljesítése a jogi vezető kötelezettsége.

(8) Alapesetben az Egyetemnek csak akkor áll fenn értesítési kötelezettsége a Nemzeti Adatvédelmi és Információszabadság Hatóság irányában, amennyiben az adatvédelmi incidens valószínűsíthető kockázattal jár a természetes személyek jogaira és szabadságaira nézve. Azzal kapcsolatban, hogy az adott incidenssel összefüggésben fennáll-e értesítési kötelezettség a Nemzeti Adatvédelmi és Információszabadság Hatóság irányában, a jogi vezető dönt, mely döntését minden esetben dokumentálni szükséges, amennyiben az incidenst nem jelentik be a Nemzeti Adatvédelmi és Információszabadság Hatóságnak.

(9) Amennyiben szükséges, a jogi vezető a Nemzeti Adatvédelmi és Információszabadság Hatóság felé történő bejelentését a tudomásszerzéstől számított legkésőbb hetvenkét (72) órával teljesíteni köteles. Amennyiben a bejelentés nem történik meg hetvenkét (72) órán belül, mellékelni kell a késedelem igazolására szolgáló indokokat is. Nem kell azonban bejelenteni, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. A jelen Rendelkezés 6. melléklete tartalmaz példákat arra vonatkozóan, hogy mikor kell, vagy sem bejelenteni egy incidenst a Nemzeti Adatvédelmi és Információszabadság Hatóságnak. Ha nem lehetséges a jelen Rendelkezés 5. melléklete szerinti információkat egyidejűleg közölni, azok további indokolatlan késedelem nélkül később részletekben is közölhetők.

(10) A Nemzeti Adatvédelmi és Információszabadság Hatóságnak több incidensre vonatkozó, „összevont” bejelentést is lehet tenni, feltéve, ha az incidensek viszonylag rövid időn belül

ugyanolyan módon megsértett, azonos jellegű személyes adatokat érintenek. Összevont bejelentést több hasonló, 72 órán belül jelentett incidensről is lehet tenni. Ha sorozatosan következnek be olyan incidensek, amelyek különböző módon megsértett, eltérő jellegű személyes adatokat érintenek, akkor a bejelentést a szokott módon kell megtenni, tehát mindegyik incidenst külön kell bejelenteni.

(11) Az incidens alacsony kockázata miatt nem szükséges értesíteni az érintetteket, amennyiben:

a) a személyes adatok titkosítva voltak, amely értelmezhetetlenné teszik az adatokat harmadik személyek számára;

b) az incidenssel érintett egyetemi szervezeti egység, vagy az informatikai terület olyan hatékony intézkedést tett, amelyek eredményeként a magas kockázat a továbbiakban valószínűsíthetően nem valósul meg;

c) aránytalan erőfeszítés lenne az érintettek tájékoztatása, ekkor például közleményt adhat ki az incidenssel érintett egyetemi szervezeti egység.

Az adatvédelmi incidens munkavállalói következményei

37. §

(1) Adatvédelmi incidens esetén a jogi vezető az incidens kivizsgálása utána visszajelez annak megvalósulásáról, súlyáról azon szervezeti egység vezetőjének, akinek a felelősségi területén történt az incidens és/vagy, akinek munkairányítása alatt álló munkavállaló munkavégzése során került sor az incidensre, végül azon vezetők felé is, aki(k)nek felelőssége volt az incidens bekövetkezésében. A visszajelzés alapján a vezető köteles a jogi vezető visszajelzése alapján a foglalkoztatásra irányuló belső szabályozókban előírtak mentén megvizsgálni és megállapítani, hogy történt-e munkavállalói mulasztás és amennyiben szükséges, munkáltatói intézkedést foganatosítani a munkavállalóval szemben.

VII. ÚJ ADATKEZELÉS

Az új adatkezelés bevezetésének folyamata

Új adatkezelés előkészítése

38. §

(1) Amennyiben bármely szervezeti egységen belül új adatkezelés bevezetésének lehetősége vagy szükségessége merül fel, a szervezeti egység vezetője a jogi vezetőt egyeztetés céljából megkeresi, amellyel egyidejűleg tájékoztatja az adatvédelmi tisztviselőt a jelen Rendelkezés 1. melléklete szerint azzal, hogy a tájékoztatásnak ki kell térnie az esetlegesen alkalmazott adatfeldolgozási technológia jellegére és az alkalmazott adatbiztonsági (folyamati és IT) rendelkezések leírására is.

(2) A szervezeti egység vezetője a megkeresés tárgyához kapcsolódó írásos összefoglalót készít, amelynek részét képezi minden – az új adatkezelés megkezdésére – vonatkozó tájékoztató, tervezet, rendszerspecifikáció, koncepció, illetve feljegyzés az adatkezeléssel kapcsolatban. Az új adatkezeléssel érintett szervezeti egység felelős vezetője a jogi vezetőt legalább az alábbi adatok, információk maradéktalan megküldésével tájékoztatja:

a) az adatkezelés célja;

b) az adatkezelés jogalapja;

c) az érintettek köre;

d) az érintettekre vonatkozó adatok leírása;

e) az adatok forrása;

f) az adatok kezelésének időtartama;

g) a továbbított adatok fajtája, címzettje és a továbbítás jogalapja, ideértve a harmadik országokba irányuló adattovábbításokat is;

h) amennyiben az adatokat harmadik országba továbbítják, a megfelelő adatbiztonsági szint biztosítása érdekében hozott intézkedések;

i) az adatfeldolgozó neve és címe, a tényleges adatkezelés, illetve az adatfeldolgozás helye és az adatfeldolgozónak az adatkezeléssel összefüggő tevékenysége, a feldolgozással érintett adatok típusa;

j) az alkalmazott adatfeldolgozási technológia jellege;

k) az alkalmazott adatbiztonsági (folyamati és IT) rendelkezések leírása;

l) megvalósít-e az adatkezelés profilozást (I/N).

(3) Az érintett szervezeti egység vezetőjének az új adatkezelés megindítása előtt egyeztetnie szükséges a jogi vezetővel, aki tizenöt (15) napon belül írásban megküldi a jogi álláspontját a tervezett adatkezeléssel kapcsolatban.

(4) Az új adatkezelést csak a jogi álláspont, és/vagy adott esetben az adatvédelmi tisztviselő véleményének a birtokában lehet megkezdeni. Az új adatkezelés megkezdéséről a szervezeti egység vezetője dönt a jogi vezető, illetve adott esetben az adatvédelmi tisztviselő álláspontjának a birtokában. Amennyiben az új adatkezelés bevezetéséről szóló döntésért felelős szervezeti egység vezetőjének a véleménye a jogi vezető, vagy az adatvédelmi tisztviselő véleményétől eltér, az eltérés indokát az érintett szervezeti egység vezetője dokumentálni és megőrizni köteles.

Adatkezelés megváltozásának előkészítése

39. §

(1) Az eltérő célú adatkezelések önálló adatkezelésnek minősülnek, abban az esetben is, ha a kezelt adatok köre azonos.

(2) Az adatkezelési folyamatok megváltoztatása esetén vizsgálni kell, hogy az eredeti adatkezelés keretein belüli-e a változás, vagy egy más, új adatkezelés jön létre általa.

Közös eljárási szabályok új adatkezelés megkezdése és az adatkezelés megváltozása esetére

40. §

(1) Az adatvédelmi tisztviselő minden új adatkezelés bevezetéséhez, illetve meglévő adatkezelések megváltozásához kapcsolódó tervezési, szervezési és tárgyalási folyamatban részvételi és véleményezési joggal rendelkezik. Ezen jogosultságainak gyakorlásához a szervezeti egység vezetője személyre szóló meghívóval biztosítja az adatvédelmi tisztviselő részvételét.

(2) Minden, az új adatkezeléssel, illetve a meglévő adatkezelések megváltozásával kapcsolatos elektronikus levelezés címzettjei közé fel kell venni az adatvédelmi tisztviselőt, a jogi vezetőt, hacsak bármelyikük – az új adatkezelés, vagy a változás körülményeinek megismerése után – ennek mellőzését kifejezetten nem kéri.

(3) Az adatvédelmi tisztviselő az új adatkezelés bevezetését, illetve a meglévő adatkezelések megváltozását megelőzően az új adatkezelés jogszerűségének, megfelelőségének, célszerűségének és hatékonysági vizsgálatának tárgyában véleményezési jogkörrel vesz részt a folyamatban.

(4) Ha az adatkezelés jogalapja a GDPR 6. cikk (1) bekezdésének f) pontja szerinti jogos érdek, a jogi vezető az adatkezeléssel érintett osztály közreműködésével elvégzi az érdekmérlegelési tesztet, melyről tájékoztatja az adatvédelmi tisztségviselőt.

(5) Ha az adatkezelést illetően a GDPR előírja, a jogi vezető az adatvédelmi tisztviselő bevonásával elvégzi az adatvédelmi hatásvizsgálatot.

(6) A jogi vezető az új adatkezelés bevezetését, vagy módosuló adatkezelés esetén a módosítás életbe lépését megelőző tizenöt (15) napon belül elvégzi az új adatkezelés, és/vagy az adatkezelés-változás miatt szükséges dokumentummódosításokat, továbbá felveszi az adatkezelést az Egyetem adatkezelési nyilvántartásába.

VIII. ADATVÉDELMI TISZTVISELŐRE VONATKOZÓ SZABÁLYOK

Adatvédelmi tisztviselő kijelölése

41. §

(1) Az Egyetem a GDPR 37. cikk (1) bekezdés a) pontja alapján köteles adatvédelmi tisztviselőt kijelölni. Az adatvédelmi tisztviselőt szakmai rátermettség és különösen az adatvédelmi jog és gyakorlat szakértői szintű ismerete, valamint a GDPR 39. cikkben említett feladatok ellátására való alkalmasság alapján kell kijelölni. Az adatvédelmi tisztviselő az Egyetem alkalmazottja lehet, vagy megbízási szerződés keretében láthatja el a feladatait. A Kommunikáció közzé teszi az adatvédelmi tisztviselő nevét és elérhetőségét az Egyetem honlapján. A Nemzeti Adatvédelmi és Információszabadság Hatóság tájékoztatása az adatvédelmi tisztviselő adatairól a hatóság által üzemeltetett online bejelentőfelület használatával történik és a jogi vezető felelőssége.

Adatvédelmi tisztviselő jogállása

42. §

(1) Az Egyetem valamennyi adatkezelést végző szervezeti egysége biztosítja, hogy az adatvédelmi tisztviselő a személyes adatok védelmével kapcsolatos összes ügybe megfelelő módon és időben bekapcsolódjon.

(2) Az Egyetem valamennyi adatkezelést végző szervezeti egysége támogatja az adatvédelmi tisztviselőt a GDPR 39. cikkben említett feladatai ellátásában azáltal, hogy biztosítja számára azokat a forrásokat, amelyek e feladatok végrehajtásához, a személyes adatokhoz és az adatkezelési műveletekhez való hozzáféréshez, valamint az adatvédelmi tisztviselő szakértői szintű ismereteinek fenntartásához szükségesek.

(3) Az Egyetem valamennyi vezetője biztosítja, hogy az adatvédelmi tisztviselő a feladatai ellátásával kapcsolatban utasításokat senkitől ne fogadjon el. Az Egyetem az adatvédelmi tisztviselőt feladatai ellátásával összefüggésben nem bocsáthatja el és szankcióval nem sújthatja. Az adatvédelmi tisztviselő közvetlenül az Elnöknek tartozik felelősséggel.

(4) Az érintettek a személyes adataik kezeléséhez és az e rendelet szerinti jogaik gyakorlásához kapcsolódó valamennyi kérdésben az adatvédelmi tisztviselőhöz fordulhatnak.

(5) Az adatvédelmi tisztviselőt feladatai teljesítésével kapcsolatban uniós vagy tagállami jogban meghatározott titoktartási kötelezettség vagy az adatok bizalmas kezelésére vonatkozó kötelezettség köti.

Adatvédelmi tisztviselő feladatai

43. §

(1) Az adatvédelmi tisztviselő legalább a következő feladatokat ellátja:

a) tájékoztat és szakmai tanácsot ad az Egyetem valamennyi Szervezeti és Működési Rend szerinti vezetője, továbbá az adatkezelést végző alkalmazottak, hallgatók és más érintettek részére a GDPR, valamint az egyéb uniós vagy magyar adatvédelmi rendelkezések szerinti kötelezettségeikkel kapcsolatban;

b) ellenőrzi az GDPR-nak, valamint az egyéb uniós vagy magyar adatvédelmi jogszabályi rendelkezéseknek, továbbá az Egyetem személyes adatok védelmével kapcsolatos belső szabályainak való megfelelést, ideértve a feladatkörök kijelölését, az adatkezelési műveletekben részt vevő személyzet tudatosság-növelését és képzését, valamint a kapcsolódó auditokat is;

c) kérésre szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomon követi a hatásvizsgálat elvégzését;

d) együttműködik a felügyeleti hatósággal;

e) az adatkezeléssel összefüggő ügyekben – ideértve a GDPR 36. cikkében említett előzetes konzultációt is – kapcsolattartó pontként szolgál a felügyeleti hatóság felé, valamint adott esetben bármely egyéb kérdésben konzultációt folytat vele.

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

(3) Az adatvédelmi tisztviselő más feladatokat is elláthat. Az adatkezelő vagy az adatfeldolgozó biztosítja, hogy e feladatokból ne fakadjon összeférhetetlenség.

Vegyes és záró rendelkezések

44. §

(1) Az Informatika által meghatározott adatbiztonsági technikai és szervezési intézkedésekre vonatkozó szabályokat („Technical and organisational measures" – TOM) az Informatika vezetője a jogi vezetővel együttműködve legkésőbb 2023. december 31. napjáig készíti el.

(2) Jelen rendelkezés 2023. augusztus 1. napján lép hatályba.

(3) Jelen rendelkezés hatálybalépésével egyidejűleg a Szenátus 2015. december 14-i ülésén az SZ-71/2015/2016. (2015. XII. 14.) számú határozatával elfogadott és többször módosított Adatkezelési Szabályzat hatályát veszíti.

Mellékletek:

1. melléklet: Sablon az egyes szervezeti egységek által végzett adatkezelések nyilvántartásához
2. melléklet: Sablon az adatfeldolgozók nyilvántartásához
3. melléklet: Adattörlési folyamatleírás sablon
4. melléklet: Az adatvédelmi incidens által képviselt kockázat értékelésének szempontjai
5. melléklet: Incidens bejelentőlap
6. melléklet: Példák, hogy mikor kell a Nemzeti Adatvédelmi és Információszabadság felé jelenteni az incidenst, és/vagy mikor kell az érintetteket értesíteni

1. melléklet:

Sablon az egyes szervezeti egységek által végzett adatkezelések nyilvántartásához

ŰRLAP
Adatkezelések nyilvántartásához

Az ŰRLAP kitöltőjének a neve:	
Az érintett CORVINUS terület megnevezése:	
Az ŰRLAP kitöltésének dátuma:	

Az adatkezelés megnevezése[1]	Érintettek köre[2]	A kezelt adatok köre[3]	Mi az adatkezelés célja?[4]	Az adatok címzettjei[5]	A címzettnek a személyes adatokon végzett tevékenységének a leírása[6]	Mi az adatkezelés időtartama?[7]	Továbbítják az adatokat harmadik országba?[8]
1)							
2)							
3)							
4)							
5)							
6)							
7)							

[1] Amennyiben az adatkezelésnek nincs neve, kérjük, adj neki egy olyan nevet, ami leginkább kifejezi az adatkezelés lényegét. Ha van már az adatkezelésnek neve (pl. adatkezelési tájékoztatóban), azt a nevet add meg**.**

[2] Az érintettek köre lehet pl. munkavállalók/megbízási jogviszony keretében foglalkoztatottak/oktatók/hallgatók/látogatók/Alumni közösség/stb. Amennyiben indokolt, több kategória is megjelölhető. Amennyiben az adott kategórián belül további érintetti kör azonosítása szükséges (pl. hallgatók – cserediák, doktorandusz hallgatók), erre a körülményre is utalj a kitöltéskor.

[3] Add meg, hogy pontosan milyen személyes adatokat kezel a terület. Személyes adat bármi lehet, ami egy azonosítható természetes személyhez köthető.

[4] Kérjük minél szabatosabban megfogalmazni az adatkezelés célját. Minél közérthetőbben írd le, hogy miért van szükség az adatok kezelésére, milyen folyamathoz kellenek az adatok, stb.

[5] Kérjük, itt add meg az összes olyan, harmadik személyt (pl. partneregyetem, Oktatási Hivatal, FIR, külső vállalkozó, ODT stb.), aki bármilyen minőségben megkapja/hozzáférhet az általatok kezelt személyes adatokhoz.

[6] Legjobb tudásod szerint írd le, hogy milyen célból kapja meg a személyes adatokat a címzett, mit kezd a számára továbbított személyes adatokkal.

[7] Add meg, hogy mennyi ideig szükséges az adatok tárolása/felhasználása – figyelembe véve a jogi környezet előírásait.

[8] Az Európai Gazdasági Térségen (EGT) kívüli államok (az EGT-be az EU tagállamai, valamint Izland, Liechtenstein és Norvégia tartoznak).

Mi az adatkezelés jogalapja?[9]	Amennyiben az adatkezelés jogalapja jogi kötelezettség, mely jogszabály teremti meg ezt a kötelezettséget?	Az adatkezelés keretében megvalósul-e valamilyen automatikus döntéshozatal és/vagy profilozás?[10]	Az adatkezelésről tájékoztatták-e már a Jog, Igazgatás és Szabályozást (I/N) Ha igen, mikor?	Amennyiben az adatokat adatfeldolgozónak továbbítják, kötöttek-e vele adatfeldolgozási szerződést?[11]
1)				
2)				
3)				
4)				
5)				
6)				
7)				

[9] Az adatkezelés jogalapja lehet (i) az érintett hozzájárulása, (ii) jogi kötelezettség, közérdek, (iii) a CORVINUS jogos érdeke, (iv) valamint az érintettel történő szerződéskötés, vagy a már megkötött szerződés teljesítése.

[10] „*profilalkotás*”: személyes adatok automatizált kezelésének bármely olyan formája, amelynek során a személyes adatokat valamely természetes személyhez fűződő bizonyos személyes jellemzők értékelésére, különösen a munkahelyi teljesítményhez, gazdasági helyzethez, egészségi állapothoz, személyes preferenciákhoz, érdeklődéshez, megbízhatósághoz, viselkedéshez, tartózkodási helyhez vagy mozgáshoz kapcsolódó jellemzők elemzésére vagy előrejelzésére használják; „*automatizált döntéshozatal*”: az adatkezelés során alkalmazott, az érintettre vonatkozó – emberi beavatkozás nélküli – döntéshozatal, amely a természetes személyre joghatással van, vagy őt jelentős mértékben érinti.

[11] Amennyiben az adatokat valamely címzettnek továbbítják, kötött-e vele a CORVINUS adatfeldolgozási szerződést?

2. melléklet:

Sablon az adatfeldolgozók nyilvántartásához

Az ŰRLAP kitöltőjének a neve:	
Az érintett CORVINUS terület megnevezése:	
Az ŰRLAP kitöltésének dátuma:	

Adatkezelés megnevezése, amelyhez az adatfeldolgozót igénybe veszik	Az adatfeldolgozó neve	Az adatfeldolgozó címe	Az adatfeldolgozó által végzett adatfeldolgozási tevékenység rövid leírása
1)			
2)			
3)			
4)			

3. melléklet:

Adattörlési folyamatleírás sablon

CORVINUS szervezeti egység megnevezése	Vezető:	Adatvédelmi kapcsolattartó:

Sorszám	Adatkezelés megnevezése*	Az adatok törlésének határideje
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
11.		
12.		
13.		
14.		
15.		

** Töltsd ki az adott szervezeti egységhez tartozó adatkezeléseket és a hozzájuk tartozó törlési határidőket a táblázatban.*

Adatkezelés sorszáma	A törlési folyamat leírása**
1.	
2.	
3.	
4.	
5.	
6.	
7.	
8.	
9.	
10.	
11.	
12.	
13.	
14.	
15.	

*** Az adott sorszámú adatkezelés esetén követett törlési eljárás rövid leírása (pl. „tárgyévet követő év január 31-ig bezárólag az adatok manuális törlése"; „az IT rendszer a paraméterezett időpontban automatikusan törli az adatokat" stb.)*

4. melléklet:

Az adatvédelmi incidens által képviselt kockázat értékelésének szempontjai

Az incidens típusa	Az incidens jellege befolyásolja a kockázat szintjét. Példa: Ha az orvosi nyilvántartásokat (egészségügyi személyes adatokat) illetéktelen személyek számára hozzáférhetővé teszik, a következmény súlyosabb lehet, mint az azonos adatok megsemmisítése/megsemmisülése.
A személyes adatok típusa, érzékenysége	Minél érzékenyebb az adatok, annál nagyobb a veszélye, hogy az incidens sérti az érintett jogait. Példa: Alapvetően a kockázat mindig a kontextustól függ. Általában azonban azt mondhatjuk, hogy a cég e-mail címe (xy@Egyetem.hu) általában kevés kockázatot jelent az érintett személy számára. Bankadatokkal, mozgási profilokkal, egészségügyi adatokkal, vásárlási magatartási adatokkal és más érzékeny adatokkal a kockázat nagyobb.
Az érintettek könnyű azonosítása	Minél könnyebb az érintetteket azonosítani, annál magasabb a képviselt kockázat mértéke. Így, ha az identitás már az adatokból származik, a kockázat ennek megfelelően magas; ha viszont időigényes kutatásra van szükség, akkor a kockázat csökken.
A következmények súlyossága az érintettek számára	Az incidens annál súlyosabb, minél hátrányosabbak az érintettre nézve a (potenciális) következmények. Példa: személyazonosság-lopás, vagyoni és nem vagyoni kár, sérelemdíj, jó hírnév megsértése. Ha feltételezzük, hogy az adatokat ismeretlen vagy rosszhiszemű birtokolja, a kockázatot ennek megfelelően magasabbra kell beállítani.
Az érintettek sajátos helyzete	Ha az érintettek a sajátos helyzetük miatt különösen érzékenyek adatvédelmileg, a kockázat nagyobb. Példa: gyermekek
Az érintettek száma	Általánosságban minél nagyobb az érintettek száma, annál nagyobb az incidens adatvédelmi kockázata. Megjegyzendő ugyanakkor, hogy a személyes adatok természetétől és kontextusától függően már önmagában egy érintett esetében is az incidens komoly következményekkel járhat.

5. melléklet:

Incidens bejelentőlap

Az adatvédelmi incidenst észlelő személy	
Neve:	
Telefonszáma:	
E-mail címe:	
Szervezeti egysége:	
Az adatvédelmi incidens:	
Észlelés helye, dátuma, időpontja:	
Bekövetkezésének helye, dátuma, időpontja:	
Leírása, körülményei:	
Hatása:	
Az érintett adatok köre:	
Az érintett személyek száma, köre:	
Az elhárítás érdekében tett intézkedések:	
A kár megelőzése, elhárítása, csökkentése érdekében tett intézkedések:	

6. melléklet:

Példák, hogy mikor kell a Nemzeti Adatvédelmi és Információszabadság Hatóság felé jelenteni az incidenst, és/vagy mikor kell az érintetteket értesíteni

Incidens leírása	NAIH értesítése	Érintett értesítése
Megfelelően titkosított, archivált adatbázis elvesztése	Nem	Nem
Zsarolóvírus titkosítja az adatbázisát. Vizsgálat után a vírus igazoltan csak titkosította az adatokat, azokat nem küldte tovább.	Igen	Nem
Adatfeldolgozó hibát észlel a honlap kódjában, amely kihasználásával hozzá lehet férni másik felhasználó adataihoz.	Igen	Igen
Személyes adatot tartalmazó irat ügyintézői hibából történő rossz címre való továbbítása.	Igen	Igen
Nem tervezett áramkimaradás miatt rövid ideig elérhetetlenné válik az Adatkezelő ügyfeleiről vezetett nyilvántartása.	Nem	Nem
Kibertámadás következtében online közzétételre kerülnek felhasználó nevek és jelszavak.	Igen	Igen
Direkt marketing e-mail küldése során minden címzett megismerheti a további címzettek e-mail címeit a további címzett vagy másolat mezőből.	Igen	Igen

A 29-es Munkacsoport WP250rev.01 számú iránymutatása az adatvédelmi incidensek (EU) 2016/679 rendelet szerinti bejelentéséről rögzíti, hogy mely esetekben jár valószínűsíthetően alacsony kockázattal az adatvédelmi incidens bekövetkezése a személyek jogaira nézve.

A Munkacsoport kifejtette, hogy a legkorszerűbb algoritmussal titkosított személyes adatok titkosságának megsértése is adatvédelmi incidensnek minősül, így bejelentendő. Ha azonban a kulcs titkossága sértetlen (vagyis a kulcsot nem veszélyeztette a biztonságnak semmilyen megsértése, és úgy került generálásra, hogy az elérhető technológiai eszközökkel senki olyan nem derítheti ki, aki a kulcshoz nem jogosult hozzáférni), akkor az adatok elvben értelmezhetetlenek. Ugyanígy hangsúlyozta a Munkacsoport, hogy még akkor is kockázatot jelent(het) az adatok elvesztése, amennyiben azok

titkosítottak és a kulcs titkossága sértetlen, azonban az adatokról az adatkezelőnek nincsenek megfelelő biztonsági másolatai.

Következésképpen akkor, ha a személyes adatokat jogosulatlan felek számára lényegében értelmezhetetlenné tették, és létezik belőlük még egy példány vagy biztonsági másolat, a megfelelően titkosított személyes adatok titkosságának megsértését nem feltétlenül szükséges bejelenteni a felügyeleti hatóságnak. Ugyanakkor szem előtt kell tartani, hogy kezdetben talán nem szükséges bejelentést tenni, ha valószínűsíthetően nincs az érintettek jogait érintő kockázat, ez azonban idővel változhat, és előfordulhat, hogy újra fel kell mérni a kockázatot. Ha például utólag kiderül a kulcsról, hogy veszélybe került, vagy sebezhetőségre derül fény a titkosító szoftverben, akkor szükség lehet bejelentésre.