PÁZMÁNY

1635

PÁZMÁNY PÉTER KATOLIKUS EGYETEM ADATKEZELÉSI SZABÁLYZATA

Hatályos 2026. január 05. napjától.

TARTALOMJEGYZÉK

BEVEZETŐ RENDELKEZÉSEK

Preambulum

A Pázmány Péter Katolikus Egyetem (a továbbiakban: **Egyetem**) mint a Katolikus Egyház küldetésében részt vevő felsőoktatási intézmény, különös felelősséget vállal az emberi személy méltóságának és szabadságának tiszteletben tartásáért. Az Egyetem a működése során olyan személyes adatokat kezel, amelyek az oktatási, kutatási, lelkipásztori és közösségépítő feladatok ellátásához nélkülözhetetlenek. Ezen adatok kezelése minden esetben az igazságosság, a bizalom és az átláthatóság szellemében történik.

Az adatvédelem és az adatbiztonság terén intézményünk elkötelezett amellett, hogy megfeleljen mind a hatályos magyar és európai jogszabályoknak, mind pedig az Egyház tanításában megfogalmazott erkölcsi alapelveknek. Az adatkezelési szabályzat célja, hogy biztosítsa a személyes adatok jogszerű, tisztességes és célhoz kötött kezelését, valamint védelmet nyújtson a visszaélésekkel szemben.

Az Egyetem számára a közösség tagjainak – hallgatók, oktatók, munkatársak és partnerek – bizalma alapvető érték. E bizalom megőrzése érdekében kiemelten fontos a személyes adatok felelős kezelése, a titoktartás és az információbiztonság garantálása.

A jelen szabályzat (a továbbiakban: **Szabályzat**) ezért nem csupán jogi és technikai előírásokat tartalmaz, hanem kifejezi az intézmény azon törekvését is, hogy az adatvédelemben a keresztény értékek – így a személy tisztelete, a közjó szolgálata és a közösségi felelősség – vezéreljék gyakorlatát.

A Szabályzat célja
1. §

(1) E Szabályzat célja, hogy a vonatkozó jogszabályi rendelkezések keretei között meghatározza az Egyetem által tárolt személyes adatok jogszerű kezelését, az Egyetemen vezetett adatkezelési nyilvántartások vezetésének szabályos rendjét, valamint biztosítsa az adatvédelem alapjogi elveinek, az információs önrendelkezési jognak és az adatbiztonság követelményeinek érvényesülését, továbbá megakadályozza a személyes adatokhoz való jogosulatlan hozzáférést, azok jogosulatlan megváltoztatását és nyilvánosságra hozatalát/kerülését.

A Szabályzat hatálya
2. §

(1) **Személyi hatály**: a jelen Szabályzatban foglalt rendelkezések kiterjednek az összes olyan természetes személyre, akik az Egyetemmel munkavégzésre vagy más egyéb polgári jogi szerződésre irányuló jogviszonyban állnak, valamint azon jogi személyekre is, amelyek közös adatkezelői és/vagy adatfeldolgozói jogviszonyban állnak az Egyetemmel.

(2) **Tárgyi hatály**: a jelen Szabályzatban foglalt rendelkezéseket az Egyetem kezelésében lévő személyes adatok kezelése során, - a személyes adatok forrására vagy az adatkezelés jogalapjára tekintet nélkül - minden esetben alkalmazni szükséges.

(3) **Területi hatály**: a jelen Szabályzatban foglalt rendelkezéseket alapvetően Magyarország területén, azon belül az Egyetem székhelyén, telephelyein és fióktelepein, valamint az Egyetemmel adatfeldolgozói és/vagy közös adatkezelői jogviszonyban lévő személyek székhelyén, telephelyein és fióktelepein szükséges alkalmazni. Amennyiben a jelen Szabályzat személyi hatálya alá tartozó személyek Magyarország területén kívül, de az Egyetem érdekében/megbízásából járnak el, úgy a jelen Szabályzatot ezeken a területeken is alkalmazni szükséges.

(4) **Időbeli hatály**: a jelen Szabályzatban foglalt rendelkezéseket a jelen Szabályzat hatálybalépésétől a jelen Szabályzat hatályon kívül helyezéséig kell alkalmazni.

(5) Az Egyetem a közérdekű adatok közzétételéről és megismerhetőségéről külön szabályzattal rendelkezik, ezért ezen tárgykör nem képezi a jelen Szabályzat tárgyát.

A szabályzat értelmezése
3. §

(1) A jelen Szabályzatban foglalt rendelkezések értelmezésére elsődlegesen az Egyetem adatvédelmi tisztviselője az Egyetem rektorával egyetértésben jogosult.

(2) Jelen szakasz (1) pontjában meghatározott értelmezés, az Egyetem Nagykancellárjának egyetértése esetén érvényes.

(3) Az Egyetem adatvédelmi tisztviselője köteles tájékoztatni az Egyetem jogi vezetésével megbízott, az Egyetem Szervezeti és Működési Szabályzatának 28. § (4) bekezdésében meghatározott személyt minden olyan lényeges adatkezelési kérdésről, fejleményről vagy intézkedésről, amely az Egyetem adatkezelési gyakorlatára vagy adatvédelmi tárgyú jogi megfelelőségére hatással lehet.

ALAPFOGALMAK ÉS ALAPELVEK

Alapfogalmak
4. §

1. „**adatfeldolgozó**”: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő (Egyetem) nevében személyes adatokat kezel;
2. „**adatkezelés**”: a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés, továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés;
3. „**adatkezelési tevékenységek nyilvántartása**”: az adatkezelést végző illetékes kar vagy más önálló szervezeti egység, a felelősségébe tartozóan végzett adatkezelési tevékenységekről nyilvántartást vezet, melyet megkeresés alapján a felügyeleti hatóság rendelkezésére átad;
4. „**adatkezelés korlátozása**”: a tárolt személyes adatok további felhasználásának érintett általi korlátozása az általános adatvédelmi rendelet 18. cikk (1) bekezdésében foglaltak tisztázásáig;
5. „**adatkezelő**”: a jelen Szabályzat szerint az Egyetem az adatkezelő, egyebekben az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza; ha az adatkezelés céljait és eszközeit az uniós vagy a tagállami jog határozza meg, az adatkezelőt vagy az adatkezelő kijelölésére vonatkozó különös szempontokat az uniós vagy a tagállami jog is meghatározhatja;
6. „**adattovábbítás**”: a személyes adat harmadik személy számára történő hozzáférhetővé tétele;
7. „**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;
8. „**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;

9. „**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;
10. „**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;
11. „**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;
12. „**érintett**”: bármely információ alapján azonosított vagy azonosítható természetes személy;
13. „**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;
14. „**felügyeleti hatóság**”: Nemzeti Adatvédelmi és Információszabadság Hatóság, www.naih.hu;
15. „**közös adatkezelő**”: az az adatkezelő, aki vagy amely – törvényben vagy az Európai Unió kötelező jogi aktusában meghatározott keretek között – az adatkezelés céljait és eszközeit egy vagy több másik adatkezelővel közösen határozza meg, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket egy vagy több másik adatkezelővel közösen hozza meg és hajtja végre vagy hajtatja végre az adatfeldolgozóval;
16. „**nyilvántartási rendszer**”: a személyes adatok bármely módon – centralizált, decentralizált vagy funkcionális vagy földrajzi szempontok szerint – tagolt állománya, amely meghatározott ismérvek alapján hozzáférhető;
17. „**nyilvánosságra hozatal**”: az adat bárki számára történő hozzáférhetővé tétele;
18. „**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; jelen szabályzat alkalmazása során profilalkotásnak különösen, de nem kizárólagosan az oktatói munka hallgatói véleményezése minősül, amennyiben azt az Egyetemmel munkavégzésre irányuló jogviszonyban foglalkoztatott személy munkahelyi teljesítményéhez kapcsolódó jellemzők elemzésére használják;
19. „**személyes adat**”: az érintettre vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy egy vagy több tényező alapján azonosítható;
20. „**személyes adatok különleges kategóriái**”: a személyes adatok különleges kategóriáiba tartozó minden adat, azaz a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a genetikai adatok, a természetes személyek egyedi azonosítását célzó biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok.

Adatkezelési alapelvek
5. §

(1) **Jogszerűség, tisztességes eljárás és átláthatóság**: személyes adatok kezelésére az irányadó jogszabályok és a jelen szabályzatban foglalt rendelkezések szerint, az adatkezelésben érintettek jogos érdekeit figyelembe véve, az érintettek számára átlátható módon kerülhet sor.

(2) **Célhoz kötöttség**: a személyes adatok kezelése csak meghatározott, egyértelmű és jogszerű célból történjen, és azokat ne kezeljék ezekkel a célokkal össze nem egyeztethető módon; nem minősül az

eredeti céllal össze nem egyeztethetőnek a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból történő további adatkezelés.

(3) **Adattakarékosság**: az adatkezelésnek a szükségesre kell korlátozódnia.

(4) **Pontosság**: a személyes adatoknak pontosnak és szükség esetén naprakésznek kell lenniük; minden észszerű intézkedést meg kell tenni annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul töröljék vagy helyesbítsék.

(5) **Korlátozott tárolhatóság**: a személyes adatok tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé; a személyes adatok ennél hosszabb ideig történő tárolására csak akkor kerülhet sor, amennyiben a személyes adatok kezelésére az általános adatvédelmi rendelet 89. cikk (1) bekezdésének megfelelően közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból kerül majd sor, az általános adatvédelmi rendeletben az érintettek jogainak és szabadságainak védelme érdekében előírt megfelelő technikai és szervezési intézkedések végrehajtására is figyelemmel.

(6) **Integritás és bizalmas jelleg**: 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.

(7) **Elszámoltathatóság**: az adatkezelő felelős az alapelveknek való megfelelésért, valamint felhívásra köteles e megfelelés igazolására.

Az adatkezelés és adatvédelem egyetemi szervezete
6. §

(1) Az Egyetem Szervezeti és Működési Szabályzatának 2. § meghatározott szervezeti egységek vezetői kötelesek gondoskodni a jelen szabályzatban foglaltak betartásáról és betartatásáról. A Hallgatói Önkormányzat vonatkozásában, jelen kötelezettség a Hallgatói Önkormányzat elnökét terheli.

(2) Az informatikai eszközökkel összefüggő technikai adatvédelemért az Informatikai Osztály az információbiztonsági szabályzatban meghatározottak szerint felelős.

(3) Az Egyetem köteles biztosítani, hogy az adatvédelmi tisztviselő a személyes adatok védelmével kapcsolatos összes ügybe megfelelő módon és időben bekapcsolódjon.

(4) Az Egyetem Szervezeti és Működési Szabályzatának 2. § meghatározott szervezeti egységek vezetői kötelesek gondoskodni arról, hogy felmerülő adatvédelmi vonatkozású kérdések esetén az adatvédelmi tisztviselő a kérdés eldöntésének támogatása érdekében elektronikus úton megkeresésre kerüljön. Kötelesek továbbá gondoskodni arról, hogy az adatvédelmi tisztviselő tájékoztatásra kerüljön minden adatvédelmet vagy egyéb módon adatkezelési műveletek érintő döntésről, valamint hogy a döntés meghozatalába bevonásra kerüljön.

Az adatkezelés jogszerűsége (jogalapja)
7. §

(1) A személyes adatok kezelése kizárólag akkor és annyiban jogszerű, amennyiben legalább az alábbiak egyike teljesül:

a) az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez (az érintett hozzájárult);
b) az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél, vagy az a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges (az érintettel létrejött/létrejövő szerződés teljesítéséhez szükséges);
c) az adatkezelés az Egyetemre vonatkozó jogi kötelezettség teljesítéséhez szükséges (jogszabályi kötelezettség);
d) az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges (az érintett vagy más természetes személy létfontosságú érdekvédelme);
e) az adatkezelés közérdekű vagy az Egyetemre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges (közfeladat teljesítése);
f) az adatkezelés az Egyetem vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé, különösen, ha az érintett gyermek (jogos érdek).

(2) Jogos érdek alapján történő adatkezelés esetén az Egyetem e jogalapon történő adatkezelés megkezdése előtt érdekmérlegelési teszt megalkotására köteles. Az Egyetem az érdekmérlegelési tesztet az e jogalapon történő adatkezelés végéig megőrizni köteles.

(3) Kétség esetén a jogalap alkalmazhatóságáról az adatvédelmi tisztviselője dönt.

Az érintett hozzájárulása mint adatkezelési jogalap
8. §

(1) Az érintett személyes adatainak kezeléséhez való hozzájárulása kizárólag akkor érvényes, amennyiben az az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel az érintett – írásbeli vagy szóbeli - nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez. Bármely ezzel ellentétes hozzájárulás érvénytelen.

(2) Annak megállapítása során, hogy a hozzájárulás önkéntes-e, a lehető legnagyobb mértékben figyelembe kell venni azt a tényt egyebek mellett, hogy a szerződés teljesítésének – beleértve a szolgáltatások nyújtását is – feltételéül szabták-e az olyan személyes adatok kezeléséhez való hozzájárulást, amelyek nem szükségesek a szerződés teljesítéséhez. Ha a szerződés fő szolgáltatása az érintett hozzájárulása nélkül is teljesíthető, úgy az érintett hozzájárulása önkéntes tud lenni.

(3) Ha az adatkezelés hozzájáruláson alapul, az Egyetemnek képesnek kell lennie annak – írásos vagy más adathordozó általi - igazolására, hogy az érintett személyes adatainak kezeléséhez hozzájárult.

(4) Az érintett jogosult arra, hogy hozzájárulását bármikor visszavonja, viszont a hozzájárulás visszavonása nem érinti a hozzájáruláson alapuló, a visszavonás előtti adatkezelés jogszerűségét. A hozzájárulás megadása előtt az érintettet erről tájékoztatni kell. A hozzájárulás visszavonását ugyanolyan egyszerű módon kell lehetővé tenni, mint annak megadását.

(5) Ha az érintett olyan hozzájárulást ad, amely más ügyekre is általánosságban vonatkozik, a hozzájárulás beszerzése iránti kérelmet a többi ügyektől egyértelműen megkülönböztethető módon kell előadni, érthető és könnyen hozzáférhető formában, világos és egyszerű nyelvezettel. Az érintett

hozzájárulását tartalmazó ilyen nyilatkozat bármely olyan része, amely sérti az általános adatvédelmi rendeletet, kötelező erővel nem bír. Amennyiben az érintett olyan hozzájárulást ad, amely csak bizonyos ügyekre vonatkozik, úgy az nem értelmezhető kiterjesztően, valamint a többi ügytől elkülönítetten kezelendő.

A személyes adatok különleges kategóriáinak kezelése
9. §

(1) A személyes adatok különleges kategóriáinak kezelése alapvetően tilos, kivéve, ha

a) az érintett kifejezett hozzájárulását adta az említett személyes adatok egy vagy több konkrét célból történő kezeléséhez, kivéve, ha az uniós vagy tagállami jog úgy rendelkezik, hogy az említett tilalom nem oldható fel az érintett hozzájárulásával (érintett hozzájárult);
b) az adatkezelés az Egyetemnek vagy az érintettnek a foglalkoztatást, valamint a szociális biztonságot és szociális védelmet szabályozó jogi előírásokból fakadó kötelezettségei teljesítése és konkrét jogai gyakorlása érdekében szükséges, ha az érintett alapvető jogait és érdekeit védő megfelelő garanciákról is rendelkező uniós vagy tagállami jog, illetve a tagállami jog szerinti kollektív szerződés ezt lehetővé teszi (foglalkoztatási vagy szociális biztonsági jogviszonyból eredő jogi kötelezettség teljesítése);
c) az adatkezelés az érintett vagy más természetes személy létfontosságú érdekeinek védelméhez szükséges, ha az érintett fizikai vagy jogi cselekvőképtelensége folytán nem képes a hozzájárulását megadni (létfontosságú érdekek védelme az érintett cselekvőképességének hiányában);
d) az adatkezelés valamely politikai, világnézeti, vallási vagy szakszervezeti célú alapítvány, egyesület vagy bármely más nonprofit szervezet megfelelő garanciák mellett végzett jogszerű tevékenysége keretében történik, azzal a feltétellel, hogy az adatkezelés kizárólag az ilyen szerv jelenlegi vagy volt tagjaira, vagy olyan személyekre vonatkozik, akik a szervezettel rendszeres kapcsolatban állnak a szervezet céljaihoz kapcsolódóan, és hogy a személyes adatokat az érintettek hozzájárulása nélkül nem teszik hozzáférhetővé a szervezeten kívüli személyek számára (belső tagsággal rendelkező civil szervezet tagjainak nyilvántartása céljából);
e) az adatkezelés olyan személyes adatokra vonatkozik, amelyeket az érintett kifejezetten nyilvánosságra hozott (már ismert adat);
f) az adatkezelés jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez szükséges, vagy amikor a bíróságok igazságszolgáltatási feladatkörükben járnak el (jogi igények előterjesztéséhez szükséges);
g) az adatkezelés jelentős közérdek miatt szükséges, uniós jog vagy tagállami jog alapján, amely arányos az elérni kívánt céllal, tiszteletben tartja a személyes adatok védelméhez való jog lényeges tartalmát, és az érintett alapvető jogainak és érdekeinek biztosítására megfelelő és konkrét intézkedéseket ír elő (jelentős és arányos közérdek);
h) az adatkezelés megelőző egészségügyi vagy munkahelyi egészségügyi célokból, a munkavállaló munkavégzési képességének felmérése, orvosi diagnózis felállítása, egészségügyi vagy szociális ellátás vagy kezelés nyújtása, illetve egészségügyi vagy szociális rendszerek és szolgáltatások irányítása érdekében szükséges, uniós vagy tagállami jog alapján vagy egészségügyi szakemberrel kötött szerződés értelmében (munkavállaló munkavégzési képességének felmérése);
i) az adatkezelés a népegészségügy területét érintő olyan közérdekből szükséges, mint a határokon át terjedő súlyos egészségügyi veszélyekkel szembeni védelem vagy az egészségügyi ellátás, a gyógyszerek és az orvostechnikai eszközök magas színvonalának és biztonságának a biztosítása, és olyan uniós vagy tagállami jog alapján történik, amely

megfelelő és konkrét intézkedésekről rendelkezik az érintett jogait és szabadságait védő garanciákra, és különösen a szakmai titoktartásra vonatkozóan (népegészségügyi érdek);

j) az adatkezelés a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból szükséges olyan uniós vagy tagállami jog alapján, amely arányos az elérni kívánt céllal, tiszteletben tartja a személyes adatok védelméhez való jog lényeges tartalmát, és az érintett alapvető jogainak és érdekeinek biztosítására megfelelő és konkrét intézkedéseket ír elő (közérdekű archiválási, tudományos, történelmi kutatási célból);

(2) Az (1) bekezdésben említett személyes adatokat abban az esetben lehet a (1) bekezdés h) pontjában említett célokból kezelni, ha ezen adatok kezelése olyan szakember által vagy olyan szakember felelőssége mellett történik, aki uniós vagy tagállami jogban, illetve az arra hatáskörrel rendelkező tagállami szervek által megállapított szabályokban meghatározott szakmai titoktartási kötelezettség hatálya alatt áll, illetve olyan más személy által, aki szintén uniós vagy tagállami jogban, illetve az arra hatáskörrel rendelkező tagállami szervek által megállapított szabályokban meghatározott titoktartási kötelezettség hatálya alatt áll.

(3) A különleges adatok tekintetében fokozott gondossággal kell eljárni. A különleges adatok vonatkozásában megfelelő technikai és szervezési intézkedésekkel kell biztosítani, hogy az adatkezelési műveletek során a különleges adatokhoz kizárólag olyan személyek rendelkezzenek hozzáféréssel, akinek az adatkezelési művelettel összefüggő feladatának ellátásához az feltétlenül szükséges.

AZ EGYETEM MINT ADATKEZELŐ FELADATAI

Belső szabályzat készítése
10. §

(1) A Szabályzat betartatásáért az Egyetem Szervezeti és Működési Szabályzatának 2. §-ban meghatározott szervezeti egységek vezetői felelnek. A Szabályzat előírásai kötelezőek továbbá minden olyan személy számára, aki az Egyetemmel munkavégzésre irányuló vagy más polgári jogi szerződéses jogviszonyban áll. Az Egyetem a Szabályzatot és a belső adatkezelési folyamatokat évente felülvizsgálja.

(2) Az Egyetem továbbá technikai és szervezési intézkedéseket alkot, amelyek a jelen Szabályzatban foglaltakon túl biztosítják a jogszerű adatkezelést és adatvédelmet.

(3) Az Egyetem állandó jelleggel adatvédelmi tisztviselőt alkalmaz, amely az Egyetemet az adatkezeléssel kapcsolatos jogszabályok és a jelen Szabályzat alapján rá irányadó kötelezettségek teljesítésében segíti.

Az adatvédelmi tisztviselő alkalmazása
11. §

(1) Az Egyetem adatvédelmi tisztviselőt alkalmaz. Adatvédelmi tisztviselőnek az nevezhető ki, aki a személyes adatok védelmére vonatkozó jogi előírások és jogalkalmazási gyakorlat megfelelő szintű ismeretével rendelkezik.

(2) Az adatvédelmi tisztviselő mindenkori elektronikus levelezési elérhetőségét az Egyetem a következő elektronikus levelezési címen köteles biztosítani: dpo@ppke.hu.

(3) Az Egyetem (és annak minden adatfeldolgozója) az adatvédelmi tisztviselő részére biztosítja azokat a forrásokat, amelyek a feladatai végrehajtásához, a személyes adatokhoz és az adatkezelési műveletekhez való hozzáféréshez, valamint az adatvédelmi tisztviselő szakértői szintű ismereteinek fenntartásához szükségesek.

(4) Az adatvédelmi tisztviselő a feladatai ellátása során személyes adatokhoz és adatkezelési műveletekhez hozzáférhet, a feladatai ellátásával kapcsolatban utasításokat senkitől nem fogadhat el. Az Egyetem az adatvédelmi tisztviselőt feladatai ellátásával összefüggésben nem bocsáthatja el és szankcióval nem sújthatja. Az adatvédelmi tisztviselő, e minőségében közvetlenül az Egyetem rektorának tartozik felelősséggel.

(5) Az érintettek a személyes adataik kezeléséhez és az általános adatvédelmi rendelet szerinti jogaik gyakorlásához kapcsolódó valamennyi kérdésben jogosultak az Egyetem adatvédelmi tisztviselőjéhez fordulni.

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

(7) Az adatvédelmi tisztviselő más feladatokat is elláthat. Az Egyetem biztosítja, hogy e feladatokból ne fakadjon összeférhetetlenség.

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

a) tájékoztat és szakmai tanácsot ad az Egyetem vagy az adatfeldolgozó, továbbá az adatkezelést végző alkalmazottak részére az e Szabályzat, az általános adatvédelmi rendelet, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezések szerinti kötelezettségeikkel kapcsolatban (irányadó jogszabályoknak való megfelelés céljából tájékoztat, tanácsot ad, döntést előkészít, döntést támogat);
b) ellenőrzi az e Szabályzatnak, az általános adatvédelmi rendeletnek, valamint az egyéb uniós vagy tagállami adatvédelmi 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) az e Szabályzatot legalább évente felülvizsgálja és javaslatot tesz annak esetleges módosítására, kiegészítésére;
d) kérésre szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomon követi a hatásvizsgálat jogszabályszerű elvégzését;
e) együttműködik a felügyeleti hatósággal; és
f) az adatkezeléssel összefüggő ügyekben – ideértve az előzetes konzultációt is – kapcsolattartó pontként szolgál a felügyeleti hatóság felé, valamint adott esetben bármely egyéb kérdésben konzultációt folytat vele;
g) naprakészen vezeti a következő nyilvántartásokat:
    i. adatvédelmi incidens nyilvántartás;
    ii. közérdekű adatigénylésekre vonatkozó nyilvántartás.

A személyes adatok kezelésének szabályai
12. §

(1) A személyes adatok gyűjtésének szabályai:
a) A cél eléréséhez feltétlenül szükséges adatokat kell gyűjteni;

b) Ami nem a cél eléréséhez szükséges, ott indokolt az érintett hozzájárulásának beszerzése; Az érintett hozzájárulását bizonyítható formában (írásos vagy elektronikus) formában kell beszerezni;
c) Az adatokat az érintettek részére legkisebb erőfeszítést okozó módon kell gyűjteni: online vagy írásos módon. Amennyiben lehetséges, az adatok gyűjtése során a digitális technológia lehetőségeit igénybe kell venni;
d) Az adatokat a felhasználás előtt legalább 15 nappal kell begyűjteni, ezzel az érintettek számára megfelelő határidőt biztosítva.

(2) A személyes adatok tárolásának szabályai:
a) Az Egyetem által kezelt személyes adatok kizárólag olyan fizikai helyen vagy informatikai tárolóegységen tárolhatóak, amelyekhez kizárólag az Egyetem fér hozzá. Ha ezen cél részben vagy teljesen nem megvalósítható, akkor törekedni kell arra, hogy a személyes adatok Magyarország területén, ennek hiányában pedig az általános adatvédelmi rendelet hatálya alá tartozó országok területén kerüljön tárolásra;
b) Törekedni kell a személyes adatok digitális formában való tárolására: a papír alapon beszerzett személyes adatokat – amennyiben lehetséges – digitális formába kell átalakítani;
c) Törekedni kell a személyes adatok rendszerbe foglalt, könnyen kereshető és módosítható, adatbázis jellegű tárolására, különös tekintettel a digitális adatbázisok létrehozására;
d) Törekedni kell az adatok több adatbázisban való egyidejű tárolásának (duplikációnak) az elkerülésére;
e) Törekedni kell az adatok helyességének meghatározott időközönkénti ellenőrzésére.

(3) A személyes adatok őrzésének szabályai: az Egyetem iratkezelési és információbiztonsági szabályzataiban foglalt rendelkezéseken túl törekedni kell arra, hogy
a) a személyes adatokhoz kizárólag az illetékes munkatársak férjenek hozzá;
b) munkaidőn kívül a személyes adatokhoz való hozzáférés ki legyen zárva;
c) a személyes adatokhoz való hozzáférést fizikai (kulccsal, chipkártyával vagy kóddal zárható tárolóegység) és/vagy szoftveres (biztonsági kód vagy ujjlenyomat) biztonsági zárolás előzze meg.

(4) A személyes adatok törlésének szabályai:
a) a személyes adatok tárolásáról, ezáltal törlési kötelezettségéről minden szervezeti egység törlési határidő-nyilvántartás vezetésére köteles;
b) amennyiben a személyes adat megőrzésének idejét nem jogszabály határozza meg, annak megállapítására az egyetem adatvédelmi tisztviselője jogosult;
c) az érintett kérésének megfelelően vagy a tárolási idő lejártát követően törölhető személyes adat;
d) amennyiben a körülmények indokolják, úgy a személyes adatok törléséről jegyzőkönyvet szükséges felvenni;
e) személyes adatot véglegesen kell törölni.

Kötelező nyilvántartások
13. §

(1) Az adatkezelési tevékenységek nyilvántartását az Egyetem az elszámoltathatóság elvéből következően annak érdekében végzi, hogy az általános adatvédelmi rendeletnek való megfelelést nyomon követni, és igazolni tudja.

(2) A következő nyilvántartások létrehozása és fenntartása kötelező:

a) adattovábbítások nyilvántartása;
b) érintetti jogok érvényesítése iránti kérelmek és az azokra az Egyetem által adott válaszok nyilvántartása;
c) hatósági megkeresések és az azokra az Egyetem által adott válaszok nyilvántartása;
d) adatkezelés megszüntetése iránti kérelmek nyilvántartása;
e) hallgatók nyilvántartása;
f) marketing célú megkeresések nyilvántartása;
g) munkaviszonnyal összefüggő személyes adatok kezelésének nyilvántartása;
h) munkaerő-felvétel nyilvántartása;
i) adatvédelmi incidensek nyilvántartása.

(3) Az adatnyilvántartásokon belül vagy amellett határidő-nyilvántartás létrehozása is kötelező, amely tartalmazza a személyes adatok tárolási határidejét, illetve törlésének megtörténtét.

Nyilvántartások vezetése
14. §

(1) Az Egyetem – és annak szervezeti egysége - köteles az adatkezelési tevékenységeiről nyilvántartást vezetni.

(2) A nyilvántartásoknak az alábbi adatokat szükséges tartalmaznia:
a) az adatkezelés céljai;
b) az érintettek kategóriái, valamint a személyes adatok kategóriáinak ismertetése;
c) olyan címzettek kategóriái, akikkel a személyes adatokat közlik vagy közölni fogják, ideértve a harmadik országbeli címzetteket vagy nemzetközi szervezeteket;
d) adott esetben a személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk, beleértve a harmadik ország vagy a nemzetközi szervezet azonosítását, valamint az általános adatvédelmi rendelet 49. cikk (1) bekezdésének második albekezdés szerinti továbbítás esetében a megfelelő garanciák leírása;
e) a különböző adatkategóriák törlésére előirányzott határidők;
f) ha lehetséges, az általános adatvédelmi rendelet 32. cikk (1) bekezdésében említett technikai és szervezési intézkedések általános leírása.

(3) E nyilvántartások vezetése a tevékenységek szerint kategóriákra bontandó például de nem kizárólagosan az alábbiak szerint:
a) az adatkezelés céljai a jelen Szabályzat 8. §-ával összhangban adhatóak meg, általánosan is nevesítve a célt, például hallgatói szerződés teljesítése, munkaszerződés teljesítése, Egyetem jogos érdekének kielégítése, érintett hozzájárulása egy konferencián való részvétel vonatkozásában stb.;
b) az érintettek kategóriái a nagy személycsoportoktól a legkisebb személycsoportokig meghatározhatóak:
    i. munkavállalók, hallgatók, oktatók;
    ii. munkavállalók az alkalmazó különböző szervezeti egységek szerint csoportosíthatóak;
    iii. hallgatók karonként, tagozatonként, évfolyamonként, diákcsere vagy ERASMUS programban való résztvevőként;
    iv. oktatók állandó vagy megbízott oktatóként;
c) a személyes adatok kategóriáit az érintettektől bekért adathalmazok nevesítéseként: teljes név, születési dátum, diploma azonosítója, telefonszám stb.;
d) a címzettek kategóriáit azok megnevezése és elérhetősége alapján: hatóság, minisztérium, TEMPUS Közalapítvány stb.;

e) nemzetközi szervezet vagy harmadik ország részére történő továbbítás esetén azok megnevezése és elérhetősége alapján: Európai Bizottság vagy Dél-Korea és az ottani elérhetőség egyszerű feltüntetése mellett;
f) a jogszabályban és/vagy nemzetközi szerződésben előírt adatkezelési határidők feltüntetése, amelyeket követően a személyes adatok törölhetőek.

Az adatfeldolgozók kezelése
15. §

(1) Ha az adatkezelést az Egyetem nevében más végzi (például bérszámfejtés, szerverszolgáltatás, honlap-üzemeltetés stb.), az Egyetem kizárólag olyan adatfeldolgozókat vehet igénybe, akik vagy amelyek megfelelő garanciákat nyújtanak az adatkezelés általános adatvédelmi rendelet követelményeinek való megfelelését és az érintettek jogainak védelmét biztosító, megfelelő technikai és szervezési intézkedések végrehajtására.

(2) Az adatfeldolgozó az Egyetem előzetesen írásban tett eseti vagy általános felhatalmazása nélkül további adatfeldolgozót nem vehet igénybe.

(3) Az adatfeldolgozó által végzett adatkezelés vonatkozásában az Egyetem és az adatfeldolgozó szerződést kötnek. Ezen szerződés az

a) adatkezelés tárgyát,
b) időtartamát,
c) jellegét és
d) célját,
e) a személyes adatok típusát,
f) az érintettek kategóriáit, valamint
g) a felek kötelezettségeit és jogait határozza meg.

(4) Az előző pont szerinti adatfeldolgozói szerződés különösen előírja, hogy az adatfeldolgozó:

a) a személyes adatokat kizárólag az Egyetem írásbeli utasításai és az Egyetem mindenkori adatkezelési szabályzata alapján kezeli,
b) biztosítja azt, hogy a személyes adatok kezelésére feljogosított személyek titoktartási kötelezettséget vállalnak vagy jogszabályon alapuló megfelelő titoktartási kötelezettség alatt állnak;
c) alkalmazza a legalább az Egyetem által előírt szintű adatbiztonsági intézkedéseket;
d) tiszteletben tartja a további adatfeldolgozó igénybevételére vonatkozóan fentebb említett feltételeket;
e) az adatkezelés jellegének figyelembevételével megfelelő technikai és szervezési intézkedésekkel a lehetséges mértékben segíti az Egyetemet abban, hogy teljesíteni tudja kötelezettségét az érintett jogainak gyakorlásához kapcsolódó kérelmek megválaszolása tekintetében;
f) segíti az Egyetemet a felmerült adatvédelmi incidens szerinti kötelezettségek teljesítésében, figyelembe véve az adatkezelés jellegét és az adatfeldolgozó rendelkezésére álló információkat;
g) vállalja, hogy a nála bekövetkező adatvédelmi incidens esetén haladéktalanul tájékoztatja erről az Egyetemet;
h) az adatkezelési szolgáltatás nyújtásának befejezését követően az Egyetem döntése alapján minden személyes adatot töröl vagy visszajuttat az Egyetemnek, és törli a meglévő másolatokat, kivéve, ha az uniós vagy a tagállami jog a személyes adatok tárolását írja elő;

i) az Egyetem rendelkezésére bocsát minden olyan információt, amely az e felsorolásban meghatározott kötelezettségek teljesítésének igazolásához szükséges, továbbá amely lehetővé teszi és elősegíti az Egyetem által vagy az általa megbízott más ellenőr által végzett auditokat, beleértve a helyszíni vizsgálatokat is.

(5) Ha az adatfeldolgozó bizonyos, az Egyetem nevében végzett konkrét adatkezelési tevékenységekhez további adatfeldolgozó szolgáltatásait is igénybe veszi, uniós vagy tagállami jog alapján létrejött szerződés vagy más jogi aktus útján erre a további adatfeldolgozóra is ugyanazok az adatvédelmi kötelezettségeket kell telepíteni, mint amelyek az Egyetem és az adatfeldolgozó között létrejött, és az adatfeldolgozói szerződésben vagy egyéb jogi aktusban szerepelnek, különösen úgy, hogy a további adatfeldolgozónak megfelelő garanciákat kell nyújtania a megfelelő technikai és szervezési intézkedések végrehajtására, és ezáltal biztosítania kell, hogy az adatkezelés megfeleljen e Szabályzat követelményeinek. Ha a további adatfeldolgozó nem teljesíti adatvédelmi kötelezettségeit, az őt megbízó adatfeldolgozó teljes felelősséggel tartozik az Egyetem felé a további adatfeldolgozó kötelezettségeinek a teljesítéséért.

(6) Az adatfeldolgozókról, illetve az adatfeldolgozói szerződésekről az Egyetem nyilvántartást vezet, amely tartalmazza az e § (3) bekezdésének a)-f) pontjaiban foglalt adatokat, valamint adott esetben azt, ha az adatfeldolgozó az Egyetem nevében adatot továbbít harmadik országba vagy nemzetközi szervezet részére.

ADATTOVÁBBÍTÁS

Az adattovábbítás általános szabályai
16. §

(1) Az Egyetem személyes adatot továbbítani harmadik személy részére kizárólag jogi kötelezettség teljesítése, szerződés teljesítése vagy az érintett hozzájárulása alapján jogosult.

(2) Az Egyetem csak az (1) pontban rögzített feltételek fennállása, valamint az adattovábbítás GDPR-nak, és más releváns jogszabályoknak való megfelelősége esetén végez adattovábbítást. Minden más esetben az adattovábbítás teljesítését meg kell tagadni.

(3) Olyan személyes adatok továbbítására – ideértve a személyes adatok harmadik országból vagy nemzetközi szervezettől egy további harmadik országba vagy további nemzetközi szervezet részére történő újbóli továbbítását is –, amelyeket harmadik országba vagy nemzetközi szervezet részére történő továbbításukat követően adatkezelésnek vetnek alá vagy szándékoznak alávetni, csak abban az esetben kerülhet sor, az általános adatvédelmi rendelet egyéb rendelkezéseinek betartása mellett, ha az Egyetem és az adatfeldolgozó teljesíti az általános adatvédelmi rendeletben rögzített feltételeket. E rendelkezéseket alkalmazni kell annak biztosítása érdekében, hogy a természetes személyek számára az általános adatvédelmi rendeletben garantált védelem szintje ne sérüljön.

(4) Külföldre irányuló adattovábbítás esetén az adattovábbítást végzőnek külön meg kell győződnie arról, hogy a külföldre történő adattovábbítás az általános adatvédelmi rendeletben írt feltételei fennállnak-e. Ennek kapcsán vizsgálandó, hogy az adattovábbítás az általános adatvédelmi rendeletben meghatározott valamely jogalapnak megfelelően történik-e, és az adatok megfelelő védelmi szintje az adatokat átvevő adatkezelőnél biztosított-e. Ha az adattovábbítás az Európai Gazdasági Térség valamely államába irányul, úgy a személyes adatok megfelelő szintű védelmét nem kell vizsgálni.

Adattovábbítás pályázat benyújtása esetén
17. §

Aki az Egyetem részére pályázatot nyújt be, vagy az Egyetem által benyújtott pályázatban saját kérése alapján megvalósítóként szerepel, a pályázat benyújtását félreérthetetlen beleegyezést adó hozzájárulásnak kell tekinteni ahhoz, hogy az Egyetem a pályázat kiírója, illetve a pályázat benyújtását, végrehajtását, elszámolását ellenőrizni jogosult szervezet részére a pályázattal összefüggő személyes adatokat továbbítsa. Ezen tájékoztatást a pályázati kiírásban feltétlenül feltüntetni szükséges.

ADATBIZTONSÁG ÉS INCIDENSKEZELÉS

Alapvető adatbiztonsági szabályok
18. §

(1) Az Egyetem a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságára jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja.

(2) Az Egyetemnek az adatok biztonságát szolgáló intézkedések meghatározásakor és alkalmazásakor tekintettel kell lenni a technika mindenkori fejlettségére. Több lehetséges adatkezelési megoldás közül azt kell választani, amely a személyes adatok magasabb szintű védelmét biztosítja, kivéve, ha az aránytalan nehézséget jelentene az intézménynek.

(3) Az Egyetem köteles garantálni az általa kezelt adatok bizalmasságát, sérthetetlenségét és rendelkezésre állását. A megfelelő szintű adatbiztonsági intézkedések meghatározása érdekében az Egyetem a kezelésében lévő minden egyes adatállományt a védelmi igény szempontjából értékel, és biztonsági fokozatba sorol.

(4) Az egyes adatkezelések biztonsági fokozatának megállapításához elemezni kell:

a) a kezelt személyes adatok jogosulatlan megismerésével, megváltoztatásával, törlésével, a hardver- és szoftvereszközök megrongálásával járó kockázatot és a várható kárt;
b) azt, hogy helyreállítható-e a sérült adatállomány, valamint az esetleges helyreállítás ráfordításait, a személyes adatok reprodukálásához szükséges adatforrások rendelkezésre állását, a manuális háttérnyilvántartásból az elveszített adatok pótlásának lehetőségét;
c) azt, hogy a kezelt személyes adatok jellegére tekintettel indokolt-e megkülönböztetett biztonsági előírásokat alkalmazni;
d) az adatbiztonságot veszélyeztető más kockázati elemeket.

(5) Az adatokat védeni kell, különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen. Az adatbiztonsági rendszabályok érvényesítése érdekében a szükséges intézkedéseket meg kell tenni mind a manuálisan kezelt, mind a számítógépen tárolt és feldolgozott személyes adatok biztonsága érdekében.

(6) Az adatkezelés biztonsága megvalósítása érdekében az Egyetem fizikai, logikai és adminisztratív kontrollokat alkalmaz együttesen:

Az Egyetem legalább az alábbi fizikai kontrollokat alkalmazza:

a) az Egyetem a jogosulatlan személyek belépésének kiszűrésére alkalmas beléptetési rendszer működtetésével biztosítja, hogy épületébe/irodájába jogosulatlan személyek ne léphessenek be. (Ez lehet elektronikus beléptetési rendszer működtetés; vagy egyszerű kulcsos beléptetés, ahol a kulcs csak belépésre jogosultaknak áll rendelkezésre; vagy bármi más olyan módszer, amely a cél megvalósulását biztosítja).
b) az Egyetem az általa mind elektronikusan, mind pedig papír alapon kezelt adatokhoz való jogosulatlan hozzáférés elkerülése érdekében biztosítja, hogy a kezelt adatokhoz fizikailag ne férhessen hozzá arra jogosulatlan személy. (Irodák, szerverszobák zárása; monitor automatikus kikapcsolásának alkalmazása; monitorok olyan módon történő elhelyezése, hogy az azon szereplő adatokra kizárólag a jogosultak láthassanak rá; csak az Egyetem által auditált adathordozót lehessen a számítógépekhez csatlakoztatni; vagy bármi más olyan módszer, amely a cél megvalósulását biztosítja).

Az Egyetem legalább az alábbi logikai kontrollokat alkalmazza:

a) az Egyetem biztosítja, hogy az általa kezelt adatokhoz kizárólag az arra megfelelő jogosultsággal rendelkezők férjenek hozzá. (Jogosultsági szintek meghatározása munkakörönként; számítógépes adatbázisokhoz való hozzáférés jogosultsági szinteknek megfelelő beállítása; a belső számítógépes hálózatba való belépés felhasználó névhez és jelszóhoz kötése; vagy bármi más olyan módszer, amely a cél megvalósulását biztosítja);
b) az Egyetem biztosítja, hogy az általa kezelt adatok elvesztésének lehetősége a legkisebbre csökkenjen. (Saját szerverek beszerzése és üzemeltetése, időszakos biztonsági mentések készítése, folyamatos szoftveres stressztesztek alkalmazása).

Az Egyetem legalább az alábbi adminisztratív kontrollokat alkalmazza:

a) az Egyetem biztosítja, hogy a személyes adatokhoz való esetleges hozzáférés dokumentációkban nyomon követhető legyen. (Tevékenység logolás; épületbe/irodába való beengedés naplózása (akár papír alapon); vagy bármi más olyan módszer, amely a cél megvalósulását biztosítja).
b) az Egyetem biztosítja olyan iratkezelési eljárásrend kialakítását, hogy a hozzá tévesen beérkező személyes adatokat tartalmazó iratok a lehető leghamarabb kiszűrésre kerüljenek és azokat a lehető legszűkebb személyi kör ismerje meg. (Amennyiben az iktató úgy ítéli meg, hogy ilyen adatot tartalmazó irat birtokába jutott, úgy azt kizárólag az erre felhatalmazott személyi kör ismerheti meg).

(7) A részletes adatbiztonsági szabályokat az Egyetem Információbiztonsági Szabályzata tartalmazza.

Az adatvédelmi incidens kezelése
19. §

(1) Az adatvédelmi incidens kezelése három – nem feltétlenül sorrendszerű - részből áll:

a) a megfelelő feltételek fennállása esetén - bejelentés a felügyeleti hatóság részére;
b) a megfelelő feltételek fennállása esetén - az érintettek tájékoztatása;
c) az adatvédelmi incidens mielőbbi, hatékony kezelése és elhárítása.

(2) Az adatvédelmi incidenst az Egyetem – az adatvédelmi tisztviselő útján - indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, bejelenti a felügyeleti hatóságnak, kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Ha a bejelentés nem történik meg 72 órán belül, mellékelni kell hozzá a késedelem igazolására szolgáló indokokat is.

(3) Az adatfeldolgozó az adatvédelmi incidenst, az arról való tudomásszerzését követően indokolatlan késedelem nélkül bejelenti az Egyetemnek.

(4) Minden, a jelen szabályzat alapján vagy más, az Egyetemmel összefüggésben végzett adatkezelést végző személy köteles a tudomására jutott adatvédelmi incidenst a legrövidebb, de legalább elektronikus úton az adatvédelmi tisztviselőnek haladéktalanul bejelenteni.

(5) Az (1) bekezdésben említett 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.

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

(7) Az Egyetem nyilvántartja az adatvédelmi incidenseket, feltüntetve az adatvédelmi incidenshez kapcsolódó tényeket, annak hatásait és az orvoslására tett intézkedéseket. E nyilvántartás lehetővé teszi, hogy a felügyeleti hatóság ellenőrizze az e § követelményeinek való megfelelést.

(8) Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az Egyetem indokolatlan késedelem nélkül tájékoztatja az érintettet az adatvédelmi incidensről.

(9) Az érintett részére adott tájékoztatásban világosan és közérthetően ismertetni kell az adatvédelmi incidens jellegét, és közölni kell legalább az e § (5) bekezdésének b), c) és d) pontjában említett információkat és intézkedéseket.

(10) Az érintettet nem kell tájékoztatni, ha 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 – mint például a 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, magas kockázat a továbbiakban valószínűsíthetően nem valósul meg;
c) a tájékoztatás aránytalan erőfeszítést tenne szükségessé. Ilyen esetekben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, vagy olyan hasonló intézkedést kell hozni, amely biztosítja az érintettek hasonlóan hatékony tájékoztatását.

(11) Ha az Egyetem még nem értesítette az érintettet az adatvédelmi incidensről, a felügyeleti hatóság, miután mérlegelte, hogy az adatvédelmi incidens valószínűsíthetően magas kockázattal jár-e,

elrendelheti az érintett tájékoztatását, vagy megállapíthatja a (10) bekezdésben említett feltételek valamelyikének teljesülését.

Belső tesztelés, felmérés és értékelés az adatkezelés megfelelősége vonatkozásában
20. §

(1) A jelen Szabályzatban, valamint az adatkezelésre irányadó jogszabályokban foglalt rendelkezések betartását az Egyetem köteles meghatározott időközönként ellenőrizni. Az ellenőrzési folyamatba az adatvédelmi tisztviselő bevonása kötelező.

(2) Az Egyetem ezen ellenőrzési kötelezettségének teljesítése céljából évente ellenőrzési tervet fogad el, amely alapján lefolytatja bizonyos folyamatok vagy szervezeti egységek jogszerűségének ellenőrzését, illetve rendelkezések betartását. Az ellenőrzési tervet minden év első negyedévének végéig kell megalkotni és az Egyetemi Tanáccsal elfogadtatni. Az ellenőrzési terv lefolytatásáról jelentést kell készíteni az Egyetemi Tanács részére, amely alapján az Egyetemi Tanács a jelen Szabályzat módosításáról, vagy egyedi utasítás kiadásáról dönthet. Az ellenőrzési terv az elfogadásának évében, az adatvédelmi tisztviselő által végrehajtandó.

(3) Az ellenőrzési terv tartalmazhat:

a) adatok bekérését;
b) a munkáltatói jogok gyakorlójának előzetes értesítését követően – személyes meghallgatást;
c) írásbeli vagy gyakorlati tesztek lefolytatását;
d) az informatikai osztály vezetőjével való egyeztetést követően - informatikai tesztelést;
e) az ellenőrzés során feltárt információk alapján e Szabályzat módosítására, kiegészítésére vagy normatív utasítás kiadására irányuló javaslatot.

Beépített és alapértelmezett adatvédelem
21. §

(1) Az Egyetem a jelen Szabályzatban, valamint a jelen Szabályzatra irányadó jogszabályokban foglalt rendelkezésekről az Egyetemmel munkavégzésre irányuló jogviszonyban lévő természetes személyek részére ismeretszerzést és ismeretfenntartást célzó oktatási anyagot hoz létre, abból oktatást tart, valamint ezt számonkéri.

(2) Az Egyetemmel munkavégzésre irányuló jogviszonyban álló természetes személyek kötelesek az e bekezdésben foglalt oktatáson részt venni, valamint a számonkérést teljesíteni. E kötelezettség teljesítésére a munkavégzésre irányuló jogviszonyban álló természetes személy egyszer kötelezhető, kivéve, ha az adatkezelésre és adatvédelemre irányuló jogszabályok vagy e Szabályzat utóbb lényegesen megváltoztak. Ezen esetben a munkavégzésre irányuló jogviszonyban álló természetes személy az oktatáson való részvételre és a számonkérés teljesítésére – a számonkérés sikeres teljesítéséig - ismételten kötelezhető.

ZÁRÓ RENDELKEZÉSEK
22. §

(1) A jelen Szabályzat hatálybalépésével az Egyetem 2018. május 25. napjától hatályos Adatvédelmi és Adatbiztonsági Szabályzata (AVBSZ) hatályát veszti. Jelen szabályzat rendelkezéseit a jelen szabályzat hatályba lépését követően indult eljárásokban kell alkalmazni.

(2) A jelen Szabályzat az Egyetemi Tanács által módosítható.

Elfogadási záradék:
A jelen módosított szabályzatot a Pázmány Péter Katolikus Egyetem Egyetemi Tanácsa 79/2025. (XII. 11.) számú határozatával elfogadta. Hatályos 2026. január 5. napjától.
Adatvédelmi státusz: **nyilvános.**

Kelt Budapesten, 2025. december 11-én.

PÁZMÁNY PÉTER KATOLIKUS EGYETEM REKTOR BUDAPEST

Dr. Kuminetz Géza György
rektor