PANNON EGYETEM

Adatvédelmi hatásvizsgálat

NEPTUN HRP PORTÁL rendszerben történő adatkezelés és adatfeldolgozás

A Pannon Egyetem tevékenységének ellátásához kapcsolódóan az alábbi adatkezelési eljárást kívánja bevezetni, amelynek során a Pannon Egyetem Adatkezelőként, az SDA Informatika Zrt. Adatfeldolgozóként jár el.

Az adatkezelés jogalapjának vizsgálata során az Európai Parlament és a Tanács (EU) 2016/679 Rendelete (a továbbiakban: Rendelet) 6. cikk (1) bekezdése a)-f) pontjai[1] az irányadók.

Amennyiben a jogalapot a Rendelet 6. cikk (1) bekezdés f) pontja jelenti: az adatkezelési folyamat akkor és annyiban lesz jogszerű, amennyiben az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé.

Az adatkezelés jogszerűségének vizsgálatához el kell végezni egy érdekmérlegelési tesztet, amelynek során az adatkezelés céljának szükségességét és az érintettek jogainak és szabadságainak arányos mértékű korlátozását kell vizsgálni, továbbá megfelelően alátámasztani.

A Rendelet 35. cikkének felhatalmazása alapján a Pannon Egyetem a következő hatásvizsgálatot végzi el:

1. A bevezetni kívánt adatkezelési folyamat leírása:

A NEPTUN HR PORTÁL alkalmazás segítségével a felhasználó – munkaszerződés, illetve hallgatói munkaszerződés alapján munkavállaló - megtekintheti a rendszerbe történő bejelentkezést követően az adatbázisban szereplő, a számfejtett fizetési jegyzékeit tételesen, valamint havonkénti- és éves bontásban, illetve a munkáltató által kezelt adatait.

A NEPTUN HR PORTÁL bevezetését megelőzően a fentieket a munkavállaló az államháztartásról szóló törvény végrehajtásáról szóló 368/2011. (XII. 31.) Korm. rendelet 62/D. § (7) bekezdése szerint a fizetési jegyzékek elektronikus úton történő közléséhez a Magyar Államkincstár által biztosított

---

1 (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;
b) az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az
c) az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges;
d) az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges;
e) az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges;
f) az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé, különösen, ha az érintett gyermek.

informatikai felületen tudta elvégezni, amely felületen keresztül a dolgozók az illetményszámfejtő programban előállított fizetési jegyzékeiket elektronikus formában elérhették. Ezen lehetőség kizárólag azon foglalkoztatottak részére érhető el, akik rendelkeznek ügyfélkapus belépési lehetőséggel (regisztrációval). A NEPTUN HR PORTÁL bevezetésével a munkavállalók már ügyfélkapus belépési lehetőség nélkül is képesek lesznek ezen információkhoz elektronikus úton, biztonságosan hozzáférni.

2. **Az adatkezelési műveletek módszeres leírása:**

A Pannon Egyetem a munka törvénykönyvéről szóló 2012. évi I. törvény (a továbbiakban: „Mt.") 10. § (1) bekezdése, valamint a nemzeti felsőoktatásról szóló 2011. évi CCIV. törvény (a továbbiakban: „Nftv.") 3. sz. melléklet I. pontja alapján jogosult a Pannon Egyetemmel létesített munkaviszony, valamint hallgatói jogviszony kapcsán, továbbá a 2013. évi V. törvény a Polgári Törvénykönyvről (a továbbiakban: „Ptk.") szerint a Pannon Egyetemmel létesített munkavégzésre irányuló egyéb jogviszonyok alapján a munkát végzők és a hallgatók tekintetében a jogviszony létesítése, teljesítése vagy megszűnése szempontjából lényeges adatokat kezelni, feldolgozni. A Pannon Egyetem a fent megjelölt adatokat egységes intézményirányítási rendszerben kezeli.

Az intézményirányítási szakrendszer működtetése érdekében Eötvös Loránd Tudományegyetem (ELTE) saját szervezetén belül a korábban létrehozott, elkülönített elszámoló egységet (továbbiakban ASP központ) a projekt céljának megfelelően bővítette. A projekt keretében a NISZ Zrt., mint az ELTE alvállalkozója, beszerezte és kialakította a rendszer működésének alapjául szolgáló informatikai környezetet. A rendszerek üzemeltetése alkalmazásszolgáltatási modellben (Application Service Providing – ASP, magyarul távoli alkalmazásszolgáltatás, a továbbiakban ASP) történik. Az ELTE a NISZ Zrt-ben elhelyezett és a NISZ Zrt. által működtetett infrastruktúrán az ASP központtal üzemelteti az EIIR Szoftver Rendszert és a rendszerhez történő hozzáférést, a rendszer használatát szolgáltatásként biztosítja a konzorciumi tagok számára. Ennek keretében az ELTE adatfeldolgozóként jár el az adatkezelés során. Az EIIR az intézményirányítási szakrendszer gazdálkodási, humán erőforrás menedzsment, felsőoktatás teljesítménymérési moduljait és az ezek működéséhez szükséges kiszolgáló szoftvertermékeket testesíti meg. A tanulmányi rendszert a Pannon Egyetem üzemelteti saját telephelyén.

Az ELTE és NISZ Zrt. közbeszerzési eljárás eredményeként szerződést kötöttek a nyertes SDA Zrt-vel a Pannon Egyetem székhelyére, mint a megvalósítás helyére kiterjedő hatállyal.

A munkavégzésre irányuló jogviszonyokból, továbbá a hallgatói jogviszonyokból származó kötelezettségek teljesítése céljából a Pannon Egyetem a munkavállaló személyes adatait – az adatszolgáltatás céljának megjelölésével, törvényben meghatározottak szerint – az SDA Informatika Zrt. számára átadja. A munkavállalói, illetve a hallgatói jogviszonyban állók jogszabályban meghatározott adatai SDA Informatika Zrt-vel megkötött vállalkozási szerződés keretében az SDA Informatika Zrt. által az ELTE ASP rendszerben kezelt adatokat a SDA Informatika Zrt. által létrehozott Neptun HR-GR rendszerbe alkalmazás interfészen keresztül átadásra kerülnek.

SDA Informatika Zrt. által ez idáig kezelt adatok: Neptun Tanulmányi és Poszeidon rendszermodulok, Nepun HR – GR rendszermodulok

SDA Informatika Zrt. által bevezetendő adatkezelés: Neptun HR Portál

3. **Az adatkezelés bevezetésének várható dátuma:** 2021. november 15.

4. **Az adatkezelés jogalapja**

A Pannon Egyetem a munka törvénykönyvéről szóló 2012. évi I. törvény (a továbbiakban: „Mt.") 10. § (1) bekezdése, valamint a nemzeti felsőoktatásról szóló 2011. évi CCIV. törvény (a továbbiakban:

„Nftv.”) 3. sz. melléklet I. pontja alapján jogosult a Pannon Egyetemmel létesített munkaviszony, valamint hallgatói jogviszony kapcsán keletkező adatok kezelésére.

5. Az adatkezelés célja/az adatkezelő jogos érdekének leírása

Az adatkezelés céljainak, indokainak leírása, különös tekintettel az adatkezelés szükségességének, elengedhetetlenségének alátámasztása:

A Pannon Egyetemért Alapítványról, a Pannon Egyetemért Alapítvány és a Pannon Egyetem részére történő vagyonjuttatásról szóló 2020. évi CLVIII. törvény alapján 2021. szeptember 1. napi hatállyal a jogállásváltozásból adódóan a Pannon Egyetemmel foglalkoztatotti jogviszonyban álló munkavállalók a továbbiakban nem közalkalmazottak, így a Magyar Államkincstár által végzett központi illetményszámfejtési rendszer a Pannon Egyetem részéről a továbbiakban nem vehető igénybe. A Pannon Egyetem 2021. szeptember 1. napját megelőzően a Pannon Egyetemmel létesített munkaviszony, valamint hallgatói jogviszony vonatkozásában az Elektronikus Bérjegyzék alkalmazás segítségével az ügyfélkapun keresztül történő bejelentkezést követően (Központi Azonosítási Ügynök, továbbiakban: KAÜ) tette lehetővé az adatbázisban szereplő számfejtett fizetési jegyzékeinek megismerését. Pannon Egyetem 2021. november 1. napjától a SDA Informatika Zrt. által működtetett online felületen (továbbiakban: Neptun HRP), egyedi azonosítást követő belépés követően teszi lehetővé a számfejtett fizetési jegyzékeinek megismerését.

Az adatkezelés célja: A Pannon Egyetem, mint Adatkezelő, köteles a munkáltató számfejtett fizetési jegyzékeinek, valamint a munkavállalói nyilvántartásban rögzített adatainak megismerését biztosítani. A kezelt adatok az adatkezelés céljának eléréséhez alkalmasak és szükségesek.

Adattovábbítás címzettje: SDA Informatika Zrt., mint Adatfeldolgozó

Adattovábbítás jogalapja: GDPR 6. cikk (1) bekezdés b) pontjában rögzített jogi kötelezettség teljesítése.

HRP által szinkronizált adatok köre: A Neptun HR (SAP) modulból a következő adatkörök (személyi és szervezeti adatok) kerülnek át a HRP-be a szinkronizációt követően.

Személyi és munkaügyi adatkör

HR Portál	Neptun HR (SAP) modul	Adat felhasználási célja a HRP-ben
Személyes adatok		
Név	0002IT	Munkavállaló tájékoztatása a személyéről nyilvántartott adatokról.
Születési név	0175IT	
Születési hely	0002IT	
Születési idő	0002IT	
Állampolgárság	0002IT	
Nem	0002IT	
Anyja neve	0175IT	
Adóazonosító	0163IT	
TAJ szám	0164IT	
Gyermekek száma	0021IT	
Címadatok (ahány érvényes címtípussal a munkatárs rendelkezik az átadás pillanatában)		
Címtípus megnevezése (*Lakóhely / Tartózkodási hely/ Levelezési cím* /…)	0006IT	Munkavállaló tájékoztatása a személyéről nyilvántartott adatokról.
Irányítószám	0006IT	
Település	0006IT	

HR Portál	Neptun HR (SAP) modul	Adat felhasználási célja a HRP-ben
Cím	0006IT	
Emelet/ajtó	0006IT	
Egyéb elérhetőségek		
Telefonszám	0105IT CELL altípus	Munkavállaló tájékoztatása a személyéről nyilvántartott adatokról.
Magán e-mail	0105IT 0020 altípus	
Intézményi e-mail	0105IT 0010 altípus	
Vész esetén értesítendő neve	további fejlesztésre fenntartva - jelen verzióban nem használt mezők -	
Vész esetén értesítendő telefonszáma		
Munkaügyi adatok		
Személyügyi törzsszám	0000IT	A jogviszony egyedi azonosítója a HRP-ben.
Szervezeti egység	0001IT Szervezeti egység mező	**Távollétmodul:** egy távollétigény elbírálója a szervezeti egység vezetője.
Funkcióterület	0001IT Funkcióterület mező	**Cafeteria modul:** a funkcióterület határozza meg a juttatási paramétereket (keretösszegek, jogcímek, fizetési időszakok száma, stb.).
Személyi kör	0001IT Személyi kör mező	**Cafeteria modul:** a Cafeteria nyilatkozatban engedélyezett jogcímenkénti keretösszeg kiszámításához szükséges paraméterek.
Szerződésfajta	0016IT szerződésfajta mező	
Munkaviszony-munkarend	0007IT munkarendszabály mező	
Belépés dátuma	0041IT	
Határozott idejű szerződés lejárta	0016IT	
Foglalkoztatási sorszám	9010IT*	
Kiléptetés dátuma	0000IT	
Próbaidő hossza	0016IT	
Próbaidő mértékegysége	0016IT	
Főtörzsszám	0163IT*	
Napi munkaóra	0007IT	
Havi munkaóra	0007IT	
Bankkapcsolatok (annyi darab, ahány bankkapcsolattal a munkatárs rendelkezik)		
Bankkapcsolat típus kódja	0009IT	Utalási adatok pl. a Cafeteria fizetéshez.
Bankkapcsolat típus megnevezése	0009IT	
Bank megnevezése	0009IT	
Bankszámlaszám	0009IT	
Érvényesség kezdete	0009IT érvényességének kezdete	
Érvényesség vége	0009IT érvényességének vége	

6. Az érintettek köre

A munka törvénykönyvéről szóló 2012. évi I. törvény (a továbbiakban: „Mt.") 10. § (1) bekezdése, valamint a nemzeti felsőoktatásról szóló 2011. évi CCIV. törvény (a továbbiakban: „Nftv.") 3. sz. melléklet I. pontjában foglalt a Pannon Egyetemmel munkaszerződés alapján létesített munkaviszonyban, valamint hallgatói jogviszonyban álló személyek.

7. Az adatkezelés időtartama

7.1. Munkaviszonnyal kapcsolatos olyan dokumentumok, mely a munkaviszony létesítésével, fennállásával, megszűnésével kapcsolatosak: főszabály szerint a munkaviszony megszűnésétől számított három (3) év.

Vonatkozó jogszabály: Mt. 286. § (1) bekezdése (a munkajogi igény három év alatt évül el)
Ide tartoznak: az Mt. 14-18. §-aiban foglalt jognyilatkozatok: munkaszerződés, tanulmányi szerződés, felmondás, utasítás, kötelezettségvállalás, munkáltatói szabályzat, tájékoztatás.

A bűncselekménnyel okozott kár megtérítésére, illetve a személyiségi jogsértéssel összefüggő sérelemdíj megfizetésére irányuló igény és ezzel kapcsolatos dokumentumok: öt (5) év, mivel ezekre öt (5) éves elévülési idő vonatkozik.

7.2. Az adó megállapításához kapcsolódó, vagy ahhoz szükséges Munkavállalói adatokat tartalmazó dokumentumok: annak a naptári évnek az utolsó napjától számított öt (5) év amelyben az adóról bevallást, adatbejelentést, bejelentést kellett volna tenni, illetve bevallás, adatbejelentés, bejelentés hiányában az adót meg kellett volna fizetni. Figyelembe kell azonban venni az adózás rendjéről szóló 2017. évi CL. törvény (Art.) 203. §-ban foglaltakat is, mely esetekben az elévülési idő meghosszabbodhat.

Vonatkozó jogszabály: Art. 202. § (1) bekezdése: az adó megállapításához való jog annak a naptári évnek az utolsó napjától számított öt év elteltével évül el, amelyben az adóról bevallást, adatbejelentést, bejelentést kellett volna tenni, illetve bevallás, adatbejelentés, bejelentés hiányában az adót meg kellett volna fizetni.

A költségvetési támogatás igényléséhez, a túlfizetés visszaigényléséhez való jog - ha törvény másként nem rendelkezik - annak a naptári évnek az utolsó napjától számított öt év elteltével évül el, amelyben az annak igényléséhez való jog megnyílt. Továbbá az adó megállapításhoz való jog elévülésének meghosszabbodásának az Art. 203.§-ban foglalt szabályai, melyek közül kiemelendő, hogy az elévülési idő meghosszabbodhat akár 6-12 hónappal is.

Ide tartoznak: adóbevallás, adóbevallás alapját képző dokumentumok (M30-as nyomtatvány, Adatlap 201x – évközi kilépés esetén), adókedvezménnyel kapcsolatos dokumentumok.

7.3. Társadalombiztosítási nyugellátás megállapításához szükséges munkavállaló adatok: a munkavállalóra irányadó öregségi nyugdíjkorhatár betöltését
követő öt (5) év.

Vonatkozó jogszabály: a 1997. évi LXXXI. törvény (Tbny.) 43. § (2) bekezdése, mely szerint a munkavállaló a társadalombiztosítási igazgatási szerv által kiszámolt szolgálati idővel szemben az egyet nem értését csak a korábbi munkáltató/foglalkoztató által kiállított egykorú eredeti okirattal (igazolással) vagy hiteles másolattal, vagy a foglalkoztató eredeti nyilvántartásai alapján kiállított igazolással tudja bizonyítani.

Tny. 99/A. §-a szerint a Tbj. 44. § (1) bekezdése szerinti nyilvántartásra kötelezett biztosított, volt biztosított biztosítási jogviszonyával összefüggő, a szolgálati időről vagy a nyugellátás megállapítása során figyelembevételre kerülő keresetről, jövedelemről adatot tartalmazó munkaügyi iratokat a biztosítottra, volt biztosítottra irányadó öregségi nyugdíjkorhatár betöltését követő öt évig köteles megőrizni.

Ide tartoznak a járulékalapot képző kereset összege és a szolgálati idő megállapításához szükséges dokumentumok: járulékköteles munkabér és táppénz/gyed/gyes megfizetését igazoló dokumentumok (járulékalapot képző jövedelemről és a levont járulékról kiállított igazolás, kilépő dokumentumok, munkaviszony igazolás, be-és kijelentési nyomtatványok).

8. Várható hatások, kockázatok (más módszer)

8.1. Milyen lehetséges kockázatokkal jár az adatkezelés az érintettek jogainak esetleges sérelme szempontjából? Adatbiztonsági kockázatok vizsgálata. Az esetleges adatvesztések, jogosulatlan hozzáférések, vagy egyéb adatvédelmi incidensek bekövetkezésének lehetséges esetei, az incidensbekövetkezés valószínűségének vizsgálata.

Az adatkezelés során bekövetkező esetleges adatvesztések a Neptun HR (SAP) modulból bármikor pótolhatók. Az adatok biztonsága az adatkezelésben résztvevő valamennyi Adatfeldolgozóval. Adatfeldolgozási szerződésben rögzítésre került.

Kockázatok:

- Az adatokhoz való jogosulatlan hozzáférés

Főbb következmények: a munkavállaló személyére vonatkozó, a munkaszerződés teljesítése alapján kezelt személyes adatok, juttatásra vonatkozó adatok illetéktelenek általi megismerése.

- Az adatok véletlen vagy jogellenes megváltoztatása

Főbb következmények: a munkavállaló személyére vonatkozó, a munkaszerződés teljesítése alapján kezelt személyes adatok pontatlansága, a munkavégzésre irányuló jogviszonyokból és a hallgatói jogviszonyokból származó munkáltatói kötelezettségek hibás teljesítése

- Adatvesztés

Főbb következmények: a munkavállaló személyére vonatkozó, a munkaszerződés teljesítése alapján kezelt személyes adatok teljes hiánya akadályozhatja a munkavégzésre irányuló jogviszonyokból, továbbá a hallgatói jogviszonyokból származó munkáltatói kötelezettségek teljesítését.

Fő fenyegető veszélyek, amelyek előidézhetik a fenti kockázatokat: adatvédelmi incidens, külső támadás informatikai rendszeren keresztül, informatikai hiba

A megadott kockázatok forrásai: az Adatkezelő és az Adatfeldolgozó adatkezeléssel megbízott munkatársainak hibája, külső informatikai támadás, Adatfeldolgozó informatikai rendszerének meghibásodása.

Meglévő és tervezett intézkedések a kockázatok kezelésére: *itt kell felsorolni az adatkezelő informatikai rendszerében található adatbiztonsági megoldásokat, technikai intézkedéseket (titkosítás stb.)*

Kockázat súlyosságának megbecslése, különösen a lehetséges következményekre és a kockázatok kezelését célzó meglévő és tervezett intézkedésekre való tekintettel: *csekély*

8.1.1. Adatkezelés biztonsága (GDPR 32. cikk)

8.1.1.1. Az Adatfeldolgozó az adatkezelési műveletek körében – a tudomány, a technológia állása szerint – köteles a megfelelő technikai és szervezési intézkedéseket végrehajtani annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja.

8.1.1.2. Az adatok megfelelő szintű biztonsága kiterjed arra eszközre, amelyen tárolásra kerülnek a személyes adatok és magában foglalja az eszközök fizikai biztonságát (védelmét) is.

8.1.1.3. Az Adatfeldolgozó teljesíti a GDPR 32. cikk (1) bekezdésében foglal alábbi intézkedéseket:

- a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítását, integritását, rendelkezésre állását és ellenálló képességét,
- fizikai vagy műszaki incidens esetén az arra való képességet, hogy a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását kellő időben vissza tudja állítani,

- az adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedések hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárást.

8.1.1.4. Adatfeldolgozó az általa végzett adatkezelési műveletek során megteszi a megfelelő biztonsági intézkedéseket annak érdekében, hogy a megakadályozza a személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosultalan nyilvánosságra hozatalát vagy az azokhoz való jogosulatlan hozzáférést.

8.1.1.5. Az Adatfeldolgozó a személyes adatok feldolgozása során biztosítja a jogosulatlan adatbevitel megakadályozását, az automatikus adatfeldolgozó rendszerek jogosulatlan személyek általi, adatátviteli berendezés segítségével történő használatának akadályozását.

8.1.2. Adatvédelmi incidens (GDPR 33. cikk)

8.1.2.1. Az adatvédelmi incidens bekövetkezése esetén az Adatfeldolgozó haladéktalanul, de legkésőbb 36 órán belül köteles az incidens bekövetkeztéről az Adatkezelőnek jelentést küldeni.

8.1.2.2. Az Adatfeldolgozó által küldött jelentés alapján az Adatkezelő – amennyiben az incidens kockázatot jelent az érintettek jogaira – az Infotv.-ben meghatározott hatóság részére bejelenti az incidens bekövetkezését.

8.1.2.3. Adatfeldolgozó az incidens megtörténte esetén köteles minden szükséges intézkedést megtenni az elhárításra, adatok védelmére, vagy adott esetben a helyreállításukra.

8.1.2.4. Az Adatfeldolgozó által megküldött jelentésnek tartalmaznia kell legalább: az incidenssel érintett személyes adatok körét, érintettek körét, számát, az incidens elhárítására tett intézkedéseket és azok eredményét.

8.1.2.Melyek az érintettek érdekei az adatkezeléssel kapcsolatban?

Az online HRP felületen történő hozzáférés biztosítás a papír alapú tájékoztatásához mérten nagyobb adatbiztonságot tesz lehetővé. Nagyban hozzájárul a munkavállalók számára a kezelt adatok körének nyomon követésében. A számfejtési adatok felhasználói belépést követően azonnal, korlátozás nélkül elérhetőek és visszakövethetők.

Az adatok pontosságát, naprakészségét az Adatkezelő a következő intézkedésekkel biztosítja:
Adatkezelő az Érintett adatszolgáltatási kötelezettsége alapján részére átadott adatot a Neptun HR (SAP) modulba rögzíti, mely a Neptun HRP-be átemelésre kerül.
A munkavállaló az adataiban bekövetkező változást jelzi a Pannon Egyetem Munkaügyi Főosztálya, mint a munkáltató adatkezelésben érintett szervezeti egysége felé. Az adatokban bekövetkezett változások rögzítésre kerülnek a NEPTUN HR (SAP) modulban és változatlan tartalommal, szinkronizálás útján kerülnek át a NEPTUN HRP rendszerbe.

9. A kockázatok elhárítására tett intézkedések, garanciák, a felek együttműködése

9.1. A személyes adatok kezelésével kapcsolatos jogok

9.1.1.A tájékoztatás kéréshez való jog

Az Érintett írásban tájékoztatást kérhet a Pannon Egyetemtől, hogy tájékoztassa:

- milyen személyes adatait,
- milyen jogalapon,
- milyen adatkezelési cél miatt,
- milyen forrásból,
- mennyi ideig kezeli,
- az Egyetem kinek, mikor, milyen jogszabály alapján, mely személyes adataihoz

biztosított hozzáférést

A Pannon Egyetem a kérelmet legfeljebb 25 napon belül, a megadott elérhetőségre küldött levélben teljesíti.

9.1.2.A helyesbítéshez való jog

Az Érintett írásban kérheti, hogy a Pannon Egyetem módosítsa valamely személyes adatát. A Pannon Egyetem a kérelmét legfeljebb 25 napon belül teljesíti, és erről az Érintettet értesíti.

9.1.3.A törléshez való jog

Az Érintett írásban kérheti a Pannon Egyetemtől a személyes adatainak a törlését.

Amennyiben azonban nincs ilyen kötelezettség, akkor a Pannon Egyetem az Érintett kérelmét legfeljebb 25 napon belül teljesíti, és erről az Érintett által megadott elérhetőségre küldött levélben értesíti.

9.1.4.A zároláshoz való jog

Az Érintett írásban kérheti, hogy a személyes adatait a Pannon Egyetem zárolja. A zárolás addig tart, amíg az Érintett által megjelölt indok szükségessé teszi az adatok tárolását.

Az Érintett az adatai zárolását kérheti például abban az esetben, ha úgy gondolja, hogy a beadványát a Pannon Egyetem jogellenesen kezelte, azonban az Érintett által kezdeményezett hatósági vagy bírósági eljárás érdekében szükséges az, hogy a beadványát a Pannon Egyetem ne törölje. Ebben az esetben a hatóság vagy a bíróság megkereséséig a Pannon Egyetem tovább tárolja a személyes adatot, ezt követően törli az adatokat.

9.1.5.A tiltakozáshoz való jog

Az Érintett írásban tiltakozhat az adatkezelés ellen, ha a Pannon Egyetem személyes adatot közvetlen üzletszerzés, közvélemény-kutatás vagy tudományos kutatás céljából továbbítaná, felhasználná. Így például az Érintett tiltakozhat az ellen, ha a Pannon Egyetem hozzájárulása nélkül az Érintett személyes adatait tudományos kutatás céljából felhasználná.

Az Érintett tiltakozhat az adatkezelés ellen akkor is, ha a Pannon Egyetem kizárólag jogi kötelezettség teljesítéséhez vagy jogos érdekének érvényesítéséhez szükséges, kivéve a jogszabályi felhatalmazáson alapuló adatkezeléseket. Így például nem tiltakozhat az ellen, ha az irattárazásra vonatkozó belső szabályzatunk alapján a személyes adatait tartalmazó beadványát – az ügy irataival együtt – átadjuk a Levéltár számára.

9.1.6.Adatbiztonsági intézkedések

Adatkezelő az adatok biztonságos kezelése, tárolása érdekében mindent megtesz. A kezelt adatok egy magas rendelkezésre állású, megbízható dedikált kiszolgálói környezetben üzemelnek.

Az Adatkezelő kötelezi magát arra, hogy gondoskodik az általa kezelt személyes adatok biztonságáról.

A tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megteszi azokat a technikai és szervezési intézkedéseket, és kialakítja azokat az eljárási szabályokat, amelyek biztosítják, hogy a felvett, tárolt, illetve kezelt adatok védettek legyenek, illetőleg megakadályozza azok megsemmisülését, jogosulatlan felhasználását és jogosulatlan megváltoztatását.

Az Adatkezelő kötelezi magát arra is, hogy minden olyan harmadik felet, akiknek az adatokat

bármilyen jogalappal továbbítja vagy átadja, felhívja, hogy tegyenek eleget az adatbiztonság követelményének.

Az Adatkezelő gondoskodik arról, hogy a kezelt adatokhoz illetéktelen személy ne férhessen hozzá, ne hozhassa nyilvánosságra, ne továbbíthassa, valamint azokat ne módosíthassa, törölhesse. A kezelt adatokat kizárólag az Adatkezelő, valamint alkalmazottai, illetve az Adatkezelő által igénybe vett adatfeldolgozó(k) ismerhetik meg jogosultsági szintek szerint.

Azokat az Adatkezelő harmadik, az adat megismerésére jogosultsággal nem rendelkező személynek nem adja át. Az Adatkezelő és Adatfeldolgozó által meghatározott munkakörökhöz rendelten, meghatározott módon, jogosultsági szintek szerint férhetnek hozzá az Adatkezelő, illetve az Adatfeldolgozó munkavállalói a személyes adatokhoz.

Az Adatkezelő az informatikai rendszerek biztonsága érdekében az informatikai rendszereket tűzfallal védi, valamint a külső- és belső adatvesztések megelőzése érdekében víruskereső és vírusirtó programot használ. Az Adatkezelő gondoskodott továbbá arról, hogy a visszaélések megelőzése érdekében bármely formában történő bejövő és kimenő kommunikációt megfelelően ellenőrizze.

Az Adatkezelő, illetve az Adatfeldolgozó a személyes adatokat bizalmas adatként minősíti és kezeli. Az Adatkezelő a különböző nyilvántartásokban elektronikusan kezelt adatállományok védelme érdekében biztosítja, hogy a nyilvántartásokban tárolt adatok – törvényben meghatározott kivételekkel – közvetlenül ne legyenek összekapcsolhatók és az Érintetthez rendelhetők.

Az Adatkezelő a kockázat mértékének megfelelő szintű adatbiztonságot garantálja, ideértve, többek között, adott esetben:

- a személyes adatok álnevesítését és titkosítását,
- a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítását, integritását, rendelkezésre állását és ellenálló képességét (üzemeltetés- és fejlesztésbiztonság, behatolás elleni védelem és felderítés, a jogosulatlan hozzáférés megelőzése)
- fizikai vagy műszaki incidens esetén az arra való képességet, hogy a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását kellő időben vissza lehet állítani (az adatszivárgás megelőzése; a sérülékenység- és incidenskezelés)
- az adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedések hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárást (az üzletfolytonosság fenntartása, kártékony kódok elleni védelme, az adatok biztonságos tárolása, továbbítása, feldolgozása, munkavállalóink biztonsági képzése)

A biztonság megfelelő szintjének meghatározásakor kifejezetten figyelembe kell venni az adatkezelésből eredő olyan kockázatokat, amelyek különösen a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítéséből, elvesztéséből, megváltoztatásából, jogosulatlan nyilvánosságra hozatalából vagy az azokhoz való jogosulatlan hozzáférésből erednek.

Adatvédelmi incidens esetén Adatkezelő haladéktalanul megteszi az Adatvédelmi és adatbiztonsági szabályzatban foglaltak szerinti szükséges intézkedéseket.

9.2. Érintett jogai, jogorvoslati lehetőségek

9.2.1. Az adatvédelmi tisztviselő elérhetősége:

A Pannon Egyetem adatvédelmi tisztviselője: EU-Tender Gazdasági Szaktanácsadó Kft.

Cégjegyzékszám: 01-09-980262

Adószám: 23830619-2-41

Székhely: 1024 Budapest, Retek utca 20.

Elérhetősége: adatvedelem@uni-pannon.hu

A Pannon Egyetem adatvédelmi kapcsolattartója:

dr. Zsargó Adrienn Ügyvivő szakértő, jogi előadó

Elérhetősége: 8200 Veszprém, Egyetem utca 10.

Telefon: +36 (88) 624-000 /6277

E-mail: adatvedelem@uni-pannon.hu

9.2.2.Bírósági eljáráskezdeményezése

A jogellenes adatkezelés esetén polgári pert kezdeményezhet az Egyetem ellen. A per elbírálása a törvényszék hatáskörébe tartozik. A per – az adatkezelésben érintett választása szerint – a lakóhelye szerinti törvényszék előtt is megindítható (a törvényszékek felsorolását és elérhetőségét az alábbi linken keresztül tekintheti meg: http://birosag.hu/torvenyszekek).

9.2.3.Hatósági bejelentés

A Nemzeti Adatvédelmi és Információszabadság Hatóságnál (www.naih.hu; 1363 Budapest, Pf.: 9.; telefon: +36-1-391-1400; fax: +36-1-391-1410; e-mail: ugyfelszolgalat@naih.hu) bejelentéssel bárki vizsgálatot kezdeményezhet arra hivatkozással, hogy személyes adatok kezelésével, illetve a közérdekű adatok vagy a közérdekből nyilvános adatok megismeréséhez fűződő jogok gyakorlásával kapcsolatban jogsérelem következett be, vagy annak közvetlen veszélye fennáll.

10. A hatásvizsgálat eredményének megállapítása, a kockázat mértékének, jellegének leírása, további intézkedések megtételének szükségessége, előzetes konzultáció szükségessége

A fentiek alapján a lehetséges fenyegetések beazonosítása megtörtént és bekövetkezésük valószínűsége megállapítása került az alkalmazott védelmi intézkedések ismeretében, továbbá mérlegelésre került, hogy az Adatkezelés és Adat átadás csekély hatással lehet az érintettekre. A táblázat a kiszámított kockázati szint alapján megmutatta, hogy további védelmi intézkedések nem szükségesek, ahhoz, hogy a kockázatokat elfogadható szintűre (így legalább korlátozott mértékűre) csökkentse az adatkezelő. Jelen esetben az adatvédelmi kockázatokat mindegyik esetben sikerült elfogadható szintűre csökkenteni, így további intézkedések az Adatkezelő részéről a tisztviselő által lefolytatott kockázatelemzés alapján nem szükségesek.
Az adatkezeléshez és adatfeldolgozáshoz előzetes konzultáció nem szükséges. Az adatkezelés a korábbi, azonos adatkörre vonatkozó adatok adatkezelése, illetve adatfeldolgozása vonatkozásában nem eredményez magasabb kockázatot. Az adatkezelés az adatkezelésben érintetti jogok vonatkozásában arányos, az az Érintettek és az Adatkezelő Pannon Egyetem jogát, jogos érdekét szolgálja.

Kelt..:2021. 11. 24.

1. sz. melléklet

Értékelési kritériumok az adatkezelés kockázati hatásának értékeléséhez
BEKÖVETKEZÉS HATÁSA
(Az érintett szempontjából)

Pont-szám	Besorolás	Hatások leírása	Példálózó felsorolás
5	**Kritikus**		
4	**Jelentős**	Az adatkezelés **különleges adatot érint, vagy nagy mennyiségű személyes adat**ot érint, **vagy nagyszámú érintett**re vonatkozik **és az adatkezelés vagy az adatokhoz történő jogosulatlan hozzáférés, változtatás, törlés** az érintettre nézve fizikai, vagyoni, nem vagyoni **kárral**, hátrányos **megkülönböztetéssel**, gazdasági és szociális **hátránnyal vagy az adatok nyilvánosságra hozatalával járhat**. Az adatkezelés gyermekek személyes adatait érinti és a gyermekre nézve fizikai, vagyoni, nem vagyoni **kárral**, hátrányos **megkülönböztetéssel**, gazdasági és szociális **hátránnyal járhat vagy az adatok nyilvánosságra hozatalával járhat**.	A Pannon Egyetem munkavállalói állománya munkaügyi, egészségügyi adatai, rögzítésre kerülnek.

3	**Mérsékelt**	Az adatkezelés következményeként az **érintettek nem gyakorolhatják jogaikat**, illetve **nem rendelkezhetnek saját személyes adataik felett vagy** az adatkezelés során **az adatok nem kívánt megsemmisülése, az adatokhoz történő jogosulatlan hozzáférés történhet**.	A Pannon Egyetem munkavállalók adatai tárolása egy cég szerverén történik és az adatbiztonság nem garantált.
2	**Csekély**	Az **adatkezelési műveletek nem garantálják teljes körűen** az adatok sérthetetlenségét és a hozzáférés korlátozását.	Az adatkezelés során előfordulhat az álnevesítés engedély nélküli feloldása.
1	**Minimális**	Az **adatkezelési műveletek** – a **rendelkezésre álló technológiai feltételek miatt** – **nem garantálják teljes körűen** az adatok sérthetetlenségét és a hozzáférés korlátozását, vagy az érintettek jogainak gyakorlását. Az adatkezelés során nem történik **profilalkotás** vagy **automatikus döntéshozatal** történik, és **nagy mennyiségű személyes adat**ot érint, **vagy nagyszámú érintett**re vonatkozik **és** az adatkezelés **vagy az adatokhoz történő jogosulatlan hozzáférés az adatok nyilvánosságra hozatalával járhat.**	Az egyes adatok törlése a technológiai feltételek miatt nem lehetséges (pl. biztonsági mentések adathalmazából).

Értékelési kritériumok az adatkezelés kockázati valószínűségének értékeléséhez

BEKÖVETKEZÉS VALÓSZÍNŰSÉGE
(Az érintett szempontjából)

Pont-szám	Besorolás	Leírás
5	**Biztos**	A kockázat bekövetkezésének valószínűsége igen magas, rendszeresen kell számolni vele.
4	**Valószínű**	A kockázat bekövetkezésének valószínűsége magas, többször kell majd a kockázatot kezelni.
3	**Várható**	A kockázat bekövetkezhet néhányszor (1-2 alkalommal).
2	**Lehetséges**	A kockázat esetleg előfordulhat.
1	**Valószínűtlen**	A kockázat bekövetkezése majdnem kizárt.

Kockázati szintbe való besorolásra szolgáló mátrix

Kockázati forrás	Hatás (0;1;2;3; 4)	Valószínűség (0;1;2;3;4)	Kockázati szint (1;2;3;4)
Fizikai, vagyoni vagy nem vagyoni károk	2	2	2
Az érintett nem rendelkezhet adatai felett, nem gyako- rolhatja jogait és sza- badságait	0	0	0
Személyes adatok különleges kategóriá- it tervezik kezelni	2	2	2
Személyes jellemzők ér- tékelésére, előrejelzésére kerül sor	0	0	0
Kiszolgáltatott érintetti pozícióban lévő adatainak kezelésére kerülne sor	3	2	2
Nagy mennyiségű szemé- lyes adat, jelentős számú érintettre kiterjedő kezelése	4	3	3

Egy adatkezelési tevékenység kockázati szintjét a táblázat „Kockázati szint” oszlopban található legmagasabb érték határozza meg. Az 1-től 4-ig besorolható kockázati szintekhez kapcsolódó értékeléseket az érintettek jogai és szabadságai szempontjából az alábbi táblázat szemlélteti:

Egyes kockázati szintekhez tartozó következmények értékelése az érintettek szemszögéből

Kockázatértékelés		
Besorolás	**Kockázati szint**	**Leírás**
0-4 pont	1. szint: Elhanyag- olható	Az adatkezelési tevékenység valószínűsíthetően egyáltalán nem vagy csak nagyon elhanyagolható kockázattal jár a természetes személyek jogaira és szabadságaira nézve. Az érintettek nem szenvednek kárt, vagy néhány kellemetlenséget kell csupán elviselniük, amelyen könnyen túlteszik magukat. Ilyenek például: fizikai/testi következmény: átmeneti fejfájás; anyagi következmény: időveszteség a formasá- gok ismétlése vagy teljesítése miatt, kéretlen levelek (például spamek) érkezé- se, weboldalakon közölt adatok újbóli felhasználása célzott reklámok küldése céljából stb.; erkölcsi következmények: egyszerű bosszúság, magánszférába való beavatkozás érzése valóságos vagy objektív sérelem nélkül stb.

5-8 pont	2. szint: Korlátozott	Az adatkezelési tevékenységnek valószínűsíthetően van kockázata a természetes személyek jogaira és szabadságaira nézve, de ez a megfelelő szervezési és techni- kai intézkedésekkel könnyen mérsékelhető. Az érintettek jelentősebb kellemetlenségeket tapasztalhatnak, de néhány nehézség ellenére könnyebben túlteszik magukat rajtuk. Például: testi kellemetlenség (eny- he betegség az ellenjavallatok be nem tartása miatt); becsületsértés, amely fizikai vagy pszichológiai megtorláshoz vezet stb.; anyagi kellemetlenségek: váratlan költségek (tévesen kiszabott kisebb bírságok), közigazgatási vagy kereskedelmi szolgáltatások igénybevételétől való eltiltás; kéretlen üzenetek érkezése, ami árt az érintettek jóhírnevének; erkölcsi kellemetlenségek: kisebb, de objektív pszi- chés betegség, a magánszféra megsértésének érzése visszafordíthatatlan sérelem nélkül, megalázás közösségi hálókon stb.

9-12 pont	3. szint: Jelentős	Az adatkezelési tevékenységnek valószínűsíthetően magas kockázata van a természetes személyek jogaira és szabadságaira nézve. A természetes személyek a megfelelő intézkedések hiányában a magánszférájuk szempontjából komoly és jelentős következményekkel szembesülhetnek, azokat képesek lehetnek leküzde- ni, de csak nehézségek árán. Az érintettek komoly következményekkel szembesülhetnek, amelyeken ugyan túlteszik magukat, de jelentős és valós nehézségek árán. Ilyenek például a testi következmény: komoly betegségek hosszú távú következményekkel (egészség- romlás szakszerűtlen gondozás vagy az ellenjavallatok be nem tartása miatt), a testi épség megváltozása például erőszak, otthoni vagy munkahelyi baleset folytán; anyagi következmény: pénz hűtlen kezelése kártalanítás nélkül, tervezett, egyedi és meg nem ismételhető lehetőségek elvesztése (lakáshitel, tanulmányi, gyakornoki vagy munkahelyi felvétel elutasítása, eltiltás vizsgázástól), lakás vagy állás elvesztése stb.; komoly pszichológia betegség (depresszió, fóbia kialaku- lása), a magánszféra megsértésének érzése maradandó sérelemmel, zsarolás, kibermegfélemlítés és zaklatás áldozatává válás stb.
13-16 pont	4. szint: Maximális	Az adatkezelési tevékenységnek valószínűsíthetően magas kockázata van a természetes személyek jogaira és szabadságaira nézve. A természetes személyek a magánszférájuk szempontjából kiemelkedően jelentős vagy akár visszafordítha- tatlan következményekkel szembesülhetnek, melyeken nem tudják túltenni magukat, ha az adatkezeléssel kapcsolatban az adatkezelő nem alkalmaz megfelelő intézkedéseket. Ilyen például: az egészségkárosodás: hosszú távú vagy állandó testi betegség, a testi épség maradandó károsodása, halál; anyagi következmény: pénzügyi koc- kázat, adósság, munkaképtelenség, áthelyezkedésre való képtelenség, bizonyí- tékvesztés peres eljárásban, létfontosságú közművektől való elzárás stb.; erkölcsi következmény: hosszú távú vagy állandó pszichológiai betegség, büntetőjogi szankció, emberrablás áldozatává válás, családi kötelékek elvesztése, jogállás megváltozása és/vagy jogi önállóság elvesztése (gyámság) stb.