

## ADATVÉDELMI INCIDENSEK KEZELÉSE ÉS BEJELENTÉSE

### *Adatvédelmi incidensek esetei*

(1) A Debreceni Campus Nonprofit Közhasznú Kft., továbbiakban Campus esetében adatvédelmi incidens különösen:

- a) a személyes adatokat tároló, kezelő informatikai rendszer vagy szoftverhez történő jogosulatlan hozzáférés,
- b) a személyes adatok jogosulatlan titkosítása, amelynek következtében a személyes adatokhoz - akár átmenetileg - nem lehet hozzáférni vagy az adatkezelések során felhasználni,
- c) ha a Campus alkalmazottja jogosulatlanul hozzáfér személyes adatokhoz, a jogosultsági szintjét meghaladóan fér hozzá a személyes adatokhoz, vagy az alkalmazott által jogosulatlanul végrehajtott adatkezelési művelet (például a személyes adatokat tartalmazó adatbázis kimentése külső adathordozóra),
- d) személyes adatok véletlen vagy szándékos, felhatalmazás nélküli nyilvánosságra hozatala,
- e) személyes adatokat tartalmazó dokumentum más számára történő hozzáférhetővé tétele,
- f) személyes adatokat tartalmazó postai küldemény téves címzethez történő elpostázása,
- g) személyes adatokat tartalmazó e-mail téves címzettnek történő kiküldése,
- h) személyes adatokat tartalmazó adathordozó vagy informatikai eszköz elvesztése,
- i) a személyes adatokat tároló informatikai eszköz vagy az ilyen adatokat tartalmazó dokumentumok sérülése, megsemmisülése (ideértve a tűzesetet vagy a vízkár által okozott sérülést vagy megsemmisülést), amelynek következtében a személyes adatokhoz - akár átmenetileg - nem lehet hozzáférni vagy a Campus adatkezelései során felhasználni.

### *Tudomásszerzés az adatvédelmi incidensről*

- (1) Tudomásszerzésnek minősül az, ha
- a) az adatvédelmi incidens bekövetkezésére utaló körülményt a Campus alkalmazottja fedezi fel,
  - b) a Campusnak e-mailben, postai levélben vagy más kommunikációs eszköz útján küldött üzenet, levél adatvédelmi incidens bekövetkezésére utaló körülményt tartalmaz (abban az esetben is, ha az üzenet vagy a levél névtelen),
  - c) a sajtóban vagy más honlapon, adatvédelmi incidens bekövetkezésére utaló körülmény jelent meg, amelyről a Campus értesül, vagy arról értesítik,
  - d) a Campus által megbízott adatfeldolgozó e-mailben jelzi, hogy a Campus által kezelt személyes adatokkal összefüggésben adatvédelmi incidens következett be.

(2) A Campus alkalmazottai az adatvédelmi incidens bejelentését az Adatvédelmi felelősnek az [info@lovarda.hu](mailto:info@lovarda.hu) vagy az [info@campusfesztival.hu](mailto:info@campusfesztival.hu) e-mail címre megküldve is megtehetik.

(3) A Campus alkalmazottja soron kívül köteles értesíteni a hivatali út betartásával a közvetlen munkahelyi felettesét. Az egyes szervezeti egységek az Adatvédelmi felelősnek történő bejelentést megelőző szakaszra vonatkozóan külön belső szabályokat állapíthatnak meg magukra.

(4) Amennyiben a Campus alkalmazottja úgy ítéli meg, hogy közvetlen felettese az adott ügyben érintett, akkor a vezető felettesét kell értesítenie.

#### *Adatkezelés felfüggesztése adatvédelmi incidens esetén*

(1) Adatvédelmi incidensre vonatkozó értesítést követően haladéktalanul fel kell függeszteni azt az adatkezelést, amit az adatvédelmi incidens érintett.

(2) A felfüggesztés különösen az alábbi esetekben szüntethető meg, ha

- a) a rendelkezésre álló információk alapján az adatvédelmi incidensnek nincsenek és nem is várhatóak súlyos következményei, vagy
- b) a felfüggesztést követően a Campus olyan intézkedéseket hozott, amelyek biztosítják, hogy az adatvédelmi incidensnek nincsenek és nem is várhatóak súlyos következményei.

(3) A felfüggesztés megszüntetéséről az Adatvédelmi felelős javaslata alapján az Ügyvezető igazgatók döntenek. A javaslatban ki kell térni arra, hogy

- a) milyen adatvédelmi incidens történt (a személyes adatok típusa, mennyisége, érintettek száma, kategóriái, milyen következményei voltak vagy lehettek volna az érintettre),
- b) miért javasolja a felfüggesztés megszüntetését.

#### *Az adatvédelmi incidens bejelentése és vizsgálása*

(1) Az adatvédelmi incidenst a Campusnak- az Adatvédelmi képviselőn keresztül - a tudomásszerzést követő 72 órán belül be kell jelentenie a NAIH honlapján, függetlenül attól, hogy mennyi információ áll a Campus rendelkezésére az adatvédelmi incidenssel összefüggésben. Ha a Campus a bejelentési kötelezettséget akadályoztatása miatt határidőben nem teljesíti, azt az akadály megszűnését követően haladéktalanul teljesíti, és a bejelentéshez mellékeli a késedelem okait feltáró nyilatkozatát is.

(2) Az adatkezelés felfüggesztését követően haladéktalanul meg kell kezdeni az adatvédelmi incidens vizsgálatát. A vizsgálat során az alábbi körülményeket kell tisztázni:

- a) az adatvédelmi incidens típusa (bizalmassági, integritási vagy elérhetőségi),
- b) az adatvédelmi incidens bekövetkezése előtt alkalmazott intézkedések,
- c) az adatvédelmi incidens oka (valószínűsíthető oka),
- d) az adatvédelmi incidenssel érintett személyes adatok típusa és mennyisége (legalább becsléssel),
- e) az érintettek száma (legalább becsléssel),
- f) az érintettek kategóriái, így különösen, hogy az adatvédelmi incidensben van-e sérülékeny érintetti kör (például gyerekek, idős emberek, vagy más ország állampolgárai),
- g) mennyire egyszerű az érintettek azonosítása azon adatkör alapján, amelyet az adatvédelmi incidens érintett,
- h) az adatvédelmi incidens lehetséges vagy már megtörtént következményei, illetve azok súlyossága az érintettekre nézve,
- i) szükséges-e az érintetteket tájékoztatni az adatvédelmi incidensről, és amennyiben nem, akkor ennek indoka,
- j) milyen intézkedéssel lehet az adatvédelmi incidens következményeit mérsékelni vagy azokat megszüntetni.

(3) Az adatvédelmi incidens kivizsgálását a Debreceni Campus Nonprofit Közhasznú Kft. igazgatósági tagjai (a továbbiakban: Igazgatóság) végzi. (**1. számú melléklet**)

Az Igazgatóság állandó tagja az Adatvédelmi felelős és az Ügyvezető igazgatók. Az állandó tagok mellett tagja lehet:

- a) az adatvédelmi incidenssel érintett szervezeti egység vezetője,
- b) az adatvédelmi incidens bejelentője,
- c) amennyiben a Campus által megbízott adatfeldolgozó tevékenysége során merült fel az adatvédelmi incidens, az adatfeldolgozó képviselője.

(4) Amennyiben az adatvédelmi incidens kivizsgálás függetlensége vagy hatékonysága a Campus szervezetén belül nem biztosítható, akkor az adatvédelmi incidens kivizsgálásával külső szakértőt kell megbízni.

(5) Az adatvédelmi incidens kivizsgálása során feltárt új körülményeket az Adatvédelmi tisztviselőnek haladéktalanul be kell jelentenie a NAIH-nak.

*Az adatvédelmi incidens bejelentésének mellőzése*

- (1) Abban az esetben, ha bizonyítottan adatvédelmi incidens történt, azonban arról történő tudomásszerzés időpontjában megállapítható, hogy az incidensnek valószínűsíthetően nincs kockázata az érintetteknek nézve, akkor az incidensről nem kell bejelentést tenni a NAIH-nak.
  
- (2) Ilyen adatvédelmi incidensnek tekinthető különösen az, ha a személyes adatokat tartalmazó, az érintett téves lakcímére küldött postai küldemény felbontás nélkül visszaérkezik a Campushoz.
  
- (3) Az adatvédelmi incidens bejelentésének mellőzéséről az Adatvédelmi felelős javaslata alapján az Ügyvezető igazgató dönt. A javaslatban ki kell térni arra, hogy
  - a) milyen adatvédelmi incidens történt (a személyes adatok típusa, mennyisége, érintettek száma, kategóriái, milyen következményei voltak vagy lehetnek volna az érintetteknek),
  - b) miért nem következett be az érintetteknek nézve kockázatot jelentő adatvédelmi incidens,
  - c) - amennyiben az adott adatvédelmi incidens kapcsán értelmezhető - hogyan lehet megelőzni azt, hogy a jövőben ne következzen be hasonló adatvédelmi incidens,
  - d) miért javasolja azt, hogy erről a Campus ne tegyen bejelentést a NAIH-nak.
  
- (4) Amennyiben az Ügyvezető igazgató a javaslatot elfogadja, akkor az adatvédelmi incidenst fel kell vezetni az incidens-nyilvántartásba. Az adatvédelmi incidens-nyilvántartást az Adatvédelmi felelős vezeti. (**3. számú melléklet**)

#### *Érintettek tájékoztatása*

- (1) Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár az érintetteknek nézve, a Campusnak indokolatlan késedelem nélkül tájékoztatnia kell az érintettet az adatvédelmi incidensről.
  
- (2) Az adatvédelmi incidens magas kockázattal jár, és az érintetteket tájékoztatni kell, ha az incidens az alábbi adatkategóriák egyikére vonatkozik:
  - a) a különleges adatok,
  - b) az érintett pénzügyi helyzetére vonatkozó adatok (például tartozás),
  - c) az érintett társadalmi megbecsülésére kiható adatok,
  - d) felhasználónév, jelszó,
  - e) a személyiséglopásra alkalmas adatok.
  
- (3) Az érintetteknek adott tájékoztatóban ismertetni kell
  - a) az adatvédelmi incidens jellegét,
  - b) a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit,

- c) ismertetni kell az adatvédelmi incidens lehetséges vagy már megtörtént következményeit, illetve azok súlyosságát az érintettekre nézve,
- d) az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

(4) Az előzetes tájékoztatást az érintettek e-mail címére kell elküldeni. Ha nem áll rendelkezésre az érintettek e-mail címe, akkor a postai elérhetőségükre kell továbbítani a tájékoztatást. Amennyiben van olyan érintett, akit nem lehet az adatvédelmi incidensről tájékoztatni, vagy az érintettek tájékoztatása aránytalan erőfeszítést tenne szükségessé, akkor a honlapon közlemény helyezhető el.

(5) A (3) bekezdésében szereplő tájékoztató szövegére és a tájékoztatás (4) bekezdés szerinti formájára, illetve tartalmára az Adatvédelmi képviselő tesz javaslatot, és arról az Ügyvezető igazgató dönt.

(6) Az előzetes tájékoztatás mellőzhető, ha

- a) a Campus megfelelő adatbiztonsági intézkedéseket hajtott végre, és ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében alkalmazták, így különösen olyan intézkedések jöhetnek szóba, amelyek a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik az adatokat (például titkosítás alkalmazása),
- b) a Campus az adatvédelmi incidenst követően olyan további intézkedéseket tett, amelyek biztosítják, hogy az adatvédelmi incidens valószínűsíthetően nem jár magas kockázattal az érintetteknek nézve.

(7) Az érintettek előzetes tájékoztatásának mellőzéséről az Adatvédelmi felelős javaslata alapján az Ügyvezető Igazgató dönt. A javaslatban ki kell térni arra, hogy

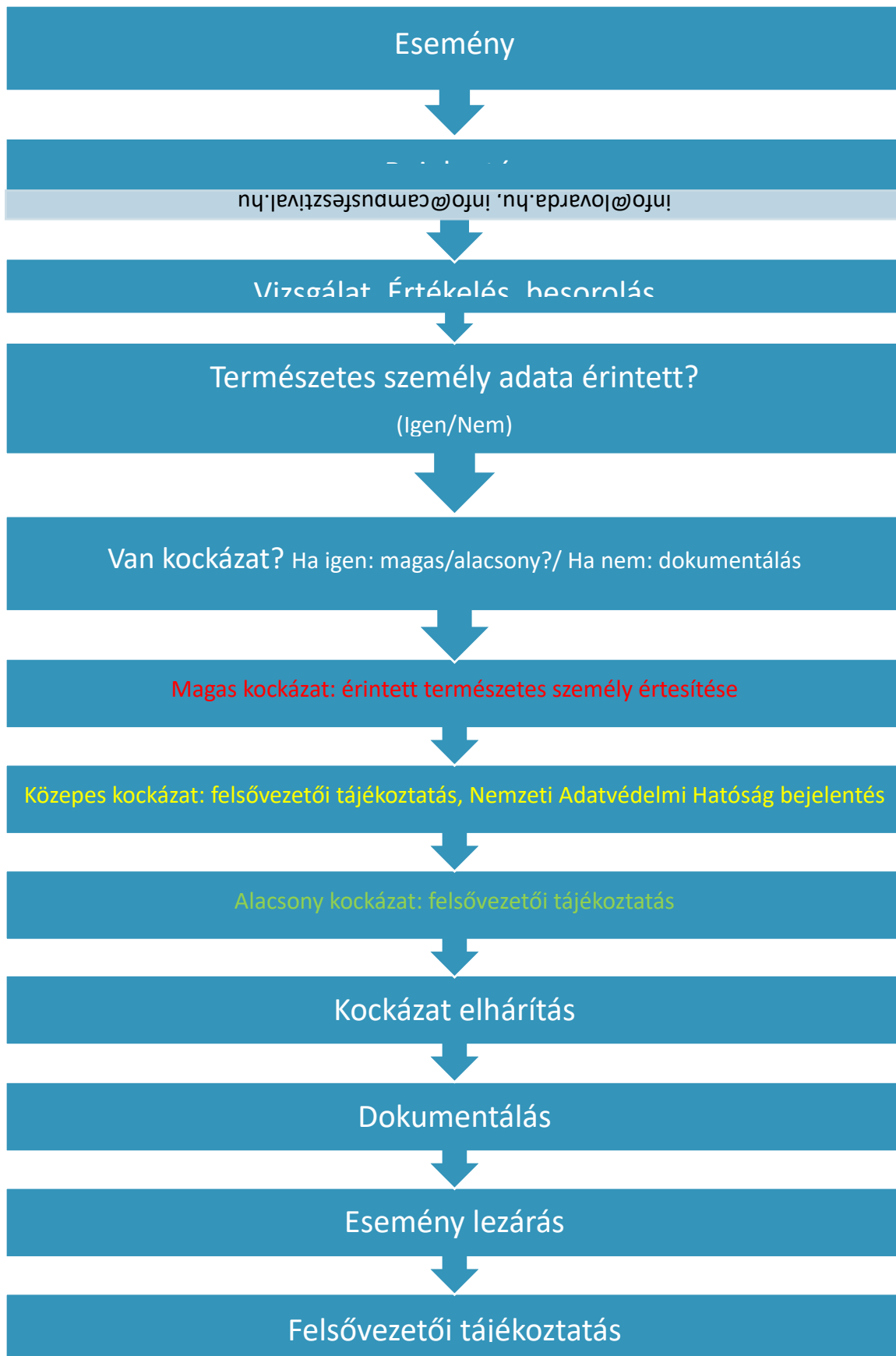
- a) milyen adatvédelmi incidens történt (a személyes adatok típusa, mennyisége, érintettek száma, kategóriái, milyen következményei voltak vagy lehettek volna az érintettre),
- b) miért lenne szükséges az érintettek tájékoztatása,
- c) miért javasolja azt, hogy a Campus ne tájékoztassa az érintetteket az adatvédelmi incidensről.

#### *Jegyzőkönyv a kivizsgálásról és az incidens-nyilvántartás*

(1) Az adatvédelmi incidens kivizsgálását írásban, jegyzőkönyvben kell rögzíteni, amelyben javaslatot kell tenni az adatvédelmi incidens orvoslására és az okainak megszüntetésére. A szükséges intézkedések meghozataláról és bevezetéséről az Ügyvezető igazgató dönt.

(2) A Campusnál történt valamennyi adatvédelmi incidensről a belső adatvédelmi szabályzat szerinti nyilvántartást kell vezetni, függetlenül attól, hogy a NAIH-nak kellett-e bejelentést tenni vagy sem.

(3) Az incidens-nyilvántartást adatvédelmi incidensenként külön-külön kell vezetni, úgy, hogy annak alapján a NAIH ellenőrizhesse az irányadó jognak való megfelelést. Az adatvédelmi incidens nyilvántartást az Adatvédelmi felelős vezeti.



Cím: [az adatvédelmi incidens időpontja és az adatvédelmi incidens jellege]

1. Az adatvédelmi incidens bekövetkezése előtt alkalmazott intézkedések:

2. Az adatvédelmi incidens jellege:

3. Az adatvédelmi incidens oka:

4. Az adatvédelmi incidenssel érintett személyes adatok típusa és mennyisége (legalább becsléssel):

5. Az érintettek száma:

6. Az érintettek kategóriái:

7. Az adatvédelmi incidens lehetséges vagy már megtörtént következményei, illetve azok súlyossága az érintettekre nézve:

8. Amennyiben az Adatkezelő mellőzte az adatvédelmi incidens bejelentést, akkor ennek oka:

9. Amennyiben nem volt szükséges az érintettek tájékoztatása, akkor ennek oka:

10. Amennyiben szükséges lett volna, de az Adatkezelő mellőzte az érintettek tájékoztatását, akkor ennek oka:

11. Az adatvédelmi incidens orvoslására és az okainak megszüntetésére tett intézkedések:

3. sz. melléklet

a, Az adatvédelmi képviselő által végzett feladatok nyilvántartása



Nyilvántartási szám / sorszám	Intézkedés dátuma	Intézkedés megnevezése	Intézkedés leírása	Intézkedés eredménye

#### **b, Incidens kezelési nyilvántartás**

**[az adatvédelmi incidens időpontja és az adatvédelmi incidens jellege]**

Az adatvédelmi incidens bekövetkezése előtt alkalmazott intézkedések:	
Az adatvédelmi incidens jellege:	
Az adatvédelmi incidens oka:	
Az adatvédelmi incidenssel érintett személyes adatok típusa és mennyisége (legalább becsléssel):	
Az érintettek száma:	
Az érintettek kategóriái:	
Az adatvédelmi incidens lehetséges vagy már megtörtént következményei, illetve azok súlyossága az érintettekre nézve:	
Amennyiben az Adatkezelő mellőzte az adatvédelmi incidens bejelentést, akkor ennek oka:	
Amennyiben nem volt szükséges az érintettek tájékoztatása, akkor ennek oka:	
Amennyiben szükséges lett volna, de az Adatkezelő mellőzte az érintettek tájékoztatását, akkor ennek oka:	
Az adatvédelmi incidens orvoslására és az okainak megszüntetésére tett intézkedések:	

#### **4. sz. melléklet - Érdemérlelési teszt**

[adatkezelés megnevezése] vonatkozásában

### 1. Az érdekmérlegelés jogalapja és az érdekmérlegelési teszt

A GDPR 6. cikk (1) bekezdés f) pontja alapján az adatkezelés jogszerűnek tekinthető abban az esetben is, ha "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."

Ezen jogalap alkalmazása esetén az adatkezeléshez nem szükséges az érintett hozzájárulása, hanem azt követeli meg, hogy a Campus az érintettek számára igazolni tudja azt, hogy

- valósnak, tényleges jogos érdekekkel rendelkezik az adatkezeléshez,
- az adatkezelés milyen jogokat érint, milyen elvárásai lehetnek az érintettnek az adatkezeléssel összefüggésben.
- olyan garanciális intézkedéseket hozott, amelyek biztosítják azt, hogy a jogos érdeke alapján végzett adatkezelések arányosan korlátozzák az érintettek jogait, magánszféráját.

Ezen megfelelést a Campus egy érdekmérlegelési tesztben foglalja össze, amelyben bemutatja, hogy az [adatkezelés megnevezése] esetében milyen jogos érdekei vannak, és az Ön jogai védelme érdekében milyen garanciális intézkedéseket hozott.

### 2. Jogos érdekek

Az adatkezeléssel összefüggésben az alábbi jogos érdeke(i) vannak:

- [miért előnyös az adatkezelőnek]
- [miért előnyös magának az érintettnek]
- [de az is idetartozik, ha az adatkezelés valami más céggel kötött szerződéses kötelezettség teljesítéséhez szükséges]

### 3. Az érintetti elvárások és garanciális intézkedések

Vizsgálatunk alapján az adatkezelésünk az Ön személyes adatok védelméhez fűződő jogát érinti.

Emellett a vizsgálatunk alapján arra a következtetésre jutottunk, hogy az adatkezelésünk során biztosítani kell, hogy (a lehető legrövidebb ideig tartson az adatkezelés,

- csak az elengedhetetlenül szükséges adatok kezelésére terjedjen ki,
- csak olyan személyek férjenek hozzá a személyes adatokhoz, akiknek feladataik vagy munkakörük ellátása érdekében ez ténylegesen indokolt,
- megfelelő tájékoztatást kapjon az adatkezelésről,
- tiltakozása esetén az adatkezelést megszüntessük (ez csak néhány adatkezelés esetén jöhet szóba, pl. marketing célú adatkezeléseknél).

Annak érdekében, hogy az adatkezelés csak a szükséges mértékben korlátozza az adatkezelést, az alábbi garanciális intézkedéseket alkalmazzuk:

- Az adatkezelés a jogviszony keletkezésétől ... napig / évig tart. Ez azért indokolt, mert ...
- Az alábbi adatok szükségesek ezen adatkezelés esetében: (felsorolni a kezelt adatokat). Ezek közül például a név, születési hely és idő adat kezelése azért szükséges az adatkezeléshez, mert ... . A ... és a ... személyes adatok kezelése azért fontos, mert ...
- A jogosultsági rendszerünk alapján a személyes adatokhoz csak ... munkakörben és a ... munkakörben dolgozó munkavállalók férnek hozzá. A ... személyes adatok nem kapják meg.
- Jelen érdekmérlegelési teszt többek között azt a célt is szolgálja, hogy Ön megfelelő információkkal rendelkezzen az adatkezelésről.
- Az Önt megillető jogokat és jogorvoslati lehetőségeket megtalálja az adatkezelési tájékoztatónkban, amely a [www.campusfesztival.hu](http://www.campusfesztival.hu) oldalon érhető el.

Kelt: Debrecen, 2020. április 27.