**Adatvédelmi hatásvizsgálat eljárásrendje**

GDPR Projekt

Nagytarcsai Szociális Segítő Szolgálat (a továbbiakban: Adatkezelő)

Szerző: KÖZINFORMATIKA Nonprofit Kft.

|  |  |
| --- | --- |
| **Dokumentumszám:** |  |
| **Verzió:** |  |
| **Dátum:** |  |
| **Szerző:** |  |

2021.

# Dokumentum verzió kontroll

|  |  |  |  |
| --- | --- | --- | --- |
| **KISZK Verzió (k)** | **Dátum** | **Szerző** | **Megjegyzés** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Tartalomjegyzék

[1 Dokumentum verzió kontroll 1](#_Toc517785374)

[2 Tartalomjegyzék 1](#_Toc517785375)

[3 Bevezetés 2](#_Toc517785376)

[3.1 Definíciók 2](#_Toc517785377)

[4 Adatvédelmi hatásvizsgálat 4](#_Toc517785378)

[4.1 Folyamatábra 4](#_Toc517785379)

[4.2 A szükséglet és összefüggések meghatározása 5](#_Toc517785380)

[4.3 A személyes adatok felhasználásának dokumentálása 6](#_Toc517785381)

[4.4 A kockázatok azonosítása 6](#_Toc517785382)

[4.4.1 A kockázati forgatókönyvek azonosítása 7](#_Toc517785383)

[4.5 A kockázatok elemzése 7](#_Toc517785384)

[4.5.1 A valószínűség vizsgálata 7](#_Toc517785385)

[4.5.2 Hatásvizsgálat 8](#_Toc517785386)

[4.5.3 Kockázat besorolás 10](#_Toc517785387)

[4.6 Kockázatok értékelése 10](#_Toc517785388)

[4.7 Kockázatkezelési terv 11](#_Toc517785389)

[4.7.1 Kockázatkezelési lehetőségek 11](#_Toc517785390)

[4.7.2 Az ellenőrzési módszerek kiválasztása 11](#_Toc517785391)

[4.7.3 Adatvédelmi hatásvizsgálati jelentés 11](#_Toc517785392)

[4.8 A menedzsment jóváhagyása a fennmaradó kockázatokhoz 12](#_Toc517785393)

[4.9 Előzetes konzultáció a felügyeleti hatósággal 12](#_Toc517785394)

[4.10 Kockázatkezelési intézkedések végrehajtása 12](#_Toc517785395)

[4.11 Kockázatellenőrzés és jelentés 13](#_Toc517785396)

[4.12 Rendszeres felülvizsgálat 13](#_Toc517785397)

[4.13 Szerepkörök és felelősségek 13](#_Toc517785398)

[4.13.1 RACI mátrix 13](#_Toc517785399)

[5 Összefoglalás 14](#_Toc517785400)

# Bevezetés

A szervezet teljes mértékben elkötelezett az ügyfelei, alkalmazottai, partnerei és egyéb érdekelt felek személyes adatainak védelmében, összhangban az Európai Unió 2016. évi általános adatvédelmi szabályaival. A személyes adatok védelmét nagyon komolyan vesszük, különböző módszerek segítségével ellenőrzéseket végzünk, hogy tudjuk, milyen adatokat gyűjtünk és tartunk nyilván, és hogy ezeket az adatokat megfelelően védjük-e.

E kötelezettségvállalás részeként biztosítja, hogy adott esetben a személyes adatok felhasználásával járó tevékenységeket és projekteket adatvédelmi hatásvizsgálatnak veti alá. Ennek az értékelésnek a célja annak biztosítása, hogy a személyes adatok felhasználását teljes mértékben megértsük, és gondosan megvizsgáljuk a személyes adatok feldolgozásánál az érintett természetes személyek jogait és szabadságait, valamint minden szükséges intézkedést meghozzunk ezen jogokhoz kapcsolódóan a feldolgozás teljes életciklusa során.

Az adatvédelmi hatásvizsgálat alapvető feltétele az GDPR megfelelésnek. A felmerülő kockázatokról alkotott világos kép megismerése után lehet biztosítani a személyes adatok megfelelő védelmét.

Jelen dokumentum ismerteti az adatvédelmi hatásvizsgálat elvégzésére irányuló eljárást. E szabályzatot a hozzá kapcsolódó dokumentumokkal, valamint útmutatásokkal együtt az Adatkezelő annak biztosítására használja fel, hogy teljesítse a GDPR-ban előírt kötelezettségeit és végrehajtsa a szabályozást.

## Definíciók

A dokumentumban használt fogalmak meghatározás a GDPR szerint:

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

*“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*;*

*“adatkezelő”’* 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*;*

*“adatfeldolgozó”’ a*z a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel*;*

# Adatvédelmi hatásvizsgálat

## Folyamatábra



1. *Ábra – Adatvédelmi hatásvizsgálat folyamatábra*

## A szükséglet és összefüggések meghatározása

Számos kritérium befolyásolja, hogy mikor kell az adatvédelmi hatásvizsgálatot elvégezni. Az általános adatvédelmi rendelet (35. cikk) előírja, hogy hatásvizsgálatra van szükség, ha a javasolt feldolgozás magában foglalja az alábbiakat:

* *a természetes személyekkel kapcsolatos személyes szempontok szisztematikus és kiterjedt értékelése, amely az automatizált feldolgozáson alapul, beleértve a profilalkotást is, és amelyen a döntések alapulnak, és amelyek a természetes személyre nézve joghatásokat váltanak ki, vagy hasonló módon jelentős hatást gyakorolnak a természetes személyre;*
* *a 9. cikk (1) bekezdésében említett különleges adatkategóriák vagy a 10. cikkben említett büntetőítéletekkel és bűncselekményekkel kapcsolatos személyes adatok széles körű feldolgozása; vagy*
* *egy nyilvánosan elérhető terület szisztematikus nyomon követése nagy léptékben.*

*Megjegyzés: A 9. cikk (1) bekezdése olyan személyes adatok feldolgozására utal, amelyek faji vagy etnikai származást, politikai véleményeket, vallási vagy filozófiai meggyőződést vagy szakszervezeti tagságot, valamint a genetikai adatok feldolgozását, a biometrikus adatokat használ a természetes személy egyedi azonosítása céljából, az egészségre vonatkozó adatok vagy a természetes személy szexuális irányultságával kapcsolatos adatok.*

Általában az Adatkezelő határozza meg, hogy az adatvédelmi hatásvizsgálatok szükségesek-e azoknál a projekteknél, ahol az alábbiak közül egy, vagy több feltétel teljesül:

1. az élő személyekről szóló információk gyűjtése és feldolgozása először történik
2. az élő személyekkel kapcsolatos információk megosztásra kerülnek olyan emberekkel vagy szervezetekkel, akik korábban nem jutottak hozzá az információkhoz
3. a meglévő személyes adatok felhasználásának megváltoztatása
4. olyan új technológia alkalmazása, amely a személyes adatokat gyűjti vagy használja, pl. biometrikus adatok
5. a meglévő személyes adatokat használják az automatizált folyamat részeként történő döntéshozatalhoz
6. észszerűen elvárható, hogy az egyén a projekt bármely nézőpontját vagy a magánszemélyek érintett adatait láthassa

Ha bizonytalanság áll fenn egy konkrét projekt esetén, akkor az adatvédelmi tisztviselővel (DPO) szükséges konzultálni, illetve további útmutatást adhat a felügyeleti hatóság (a NAIH) is.

Az adatvédelmi hatásvizsgálat teljes környezetét is ismertetni kell, és indokolni kell a hatásvizsgálat szükségességét.

A hatásvizsgálat hatókörét egyértelműen meg kell határozni. Ilyenek lehetnek például:

* földrajzi fekvés
* szervezeti egységek
* üzleti folyamatok
* informatikai szolgáltatások, rendszerek, hálózatok
* ügyfelek, termékek vagy szolgáltatások

A hatókör alóli bármilyen kivételt fel kell sorolni az okok megjelölésével.

## A személyes adatok felhasználásának dokumentálása

A projekthez kapcsolódó személyes adatokról és azok tervezett feldolgozásáról részletesen össze kell gyűjteni és dokumentálni a következőket:

* A feldolgozás céljait
* Miért szükséges a feldolgozás a célok eléréséhez?
* Annak vizsgálatát, hogy a feldolgozás arányban van-e az elérendő célokkal
* A tárolandó és feldolgozandó adatelemek pontos definíciója
* Az adatok megszerzésének módja
* Az adatok feldolgozásának módja
* Az adatok megőrzésének időtartama
* Az adat tárolás módja
* Az adatok lehetséges jövőbeni felhasználási módjai
* Az adatok átadása, illetve az átadás feltételei
* Ki és hogyan fér hozzá az adatokhoz?

Az alábbi dokumentumok segíthetnek ezen információk összegyűjtésében:

* *Adatvédelmi hatásvizsgálat értékelés kérdőíve*
* *Személyes adat térkép*

## A kockázatok azonosítása

Az adatalany “jogai és szabadságai”, főleg a magánélet védelmére vonatkoznak, de magukban foglalhatják a következőket is:

* szólásszabadság
* a gondolat szabadsága
* a mozgás szabadsága
* a megkülönböztetés tilalma
* a szabadsághoz való jog, vallásszabadság

A feldolgozás körülményeitől függően más hatásokat is figyelembe lehet venni.

Az összegyűjtött, feldolgozott és feldolgozandó személyes adatok kockázatainak azonosítása a következő lépésekből áll.

### A kockázati forgatókönyvek azonosítása

A kockázatok azonosítása csoportos megbeszélések és az érdekeltekkel folytatott interjúk során történik.

Érdekelt felek lehetnek általában:

* Az egyes feldolgozásokért felelős vezetők
* Az adott feldolgozást végzők képviselői
* A feldolgozás inputját adó személy vagy szervezet (ideértve az adatalanyt is)
* A feldolgozás eredményének címzettjei
* Lényeges ismeretekkel rendelkező harmadik felek
* A feldolgozáshoz támogatást nyújtók képviselői
* Bárki más, aki hasznos információt tudni adni a kockázat azonosítás során

Az azonosított kockázatokat írásban részletesen rögzíteni kell. A dokumentumnak tartalmaznia kell az előfordulás valószínűségét és a kiváltott hatás nagyságát. Minden kockázathoz felelőst kell rendelni.

## A kockázatok elemzése

A természetes személyek jogait és szabadságait érintő - változó valószínűségű és súlyosságú - kockázatok származhatnak a személyes adatok kezeléséből, amelyek fizikai, vagyoni vagy nem vagyoni károkhoz vezethetnek, különösen, ha az adatkezelésből hátrányos megkülönböztetés, személyazonosság-lopás vagy személyazonossággal való visszaélés, pénzügyi veszteség, a jó hírnév sérelme, a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülése, az álnevesítés engedély nélkül történő feloldása, vagy bármilyen egyéb jelentős gazdasági vagy szociális hátrány fakadhat; vagy ha az érintettek nem gyakorolhatják jogaikat és szabadságaikat, vagy nem rendelkezhetnek saját személyes adataik felett; vagy ha olyan személyes adatok kezelése történik, amelyek faji vagy etnikai származásra, vagy politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utalnak, valamint ha a kezelt adatok genetikai adatok, egészségügyi adatok vagy a szexuális életre, büntetőjogi felelősség megállapítására, illetve bűncselekményekre, vagy ezekhez kapcsolódó biztonsági intézkedésekre vonatkoznak; vagy ha személyes jellemzők értékelésére, így különösen munkahelyi teljesítménnyel kapcsolatos jellemzők, gazdasági helyzet, egészségi állapot, személyes preferenciák vagy érdeklődési körök, megbízhatóság vagy viselkedés, tartózkodási hely vagy mozgás elemzésére vagy előrejelzésére kerül sor személyes profil létrehozása vagy felhasználása céljából; vagy ha kiszolgáltatott személyek - különösen, ha gyermekek - személyes adatainak a kezelésére kerül sor; vagy ha az adatkezelés nagy mennyiségű személyes adat alapján zajlik, és nagyszámú érintettre terjed ki.

Az érintett jogait és szabadságait érintő kockázat valószínűségét és súlyosságát az adatkezelés jellegének, hatókörének, körülményeinek és céljainak függvényében kell meghatározni. A kockázatot olyan objektív értékelés alapján kell felmérni, amelynek során szükséges megállapítani, hogy az adatkezelési műveletek kockázattal, illetve nagy kockázattal járnak-e.

A kockázatelemzés egy számszerű érték hozzárendelését jelenti a valószínűséghez, illetve a hatáshoz. A kapott értékeket összeszorozva lehet meghatározni a kockázat besorolási szintjét, ami lehet magas, közepes vagy alacsony.

### A valószínűség vizsgálata

Meg kell határozni a kockázat bekövetkezésének valószínűségét. Figyelembe kell venni, hogy történt-e már ilyen esemény a szervezetben, hasonló szervezetekben, a közigazgatás más területein, stb., és hogy van-e ok, lehetőség vagy képesség a fenyegetés megvalósulására.

Az egyes kockázatok valószínűségét egy numerikus skálával kell ábrázolni 1-től (alacsony) 5-ig (magas). Az egyes kategóriák meghatározását az alábbi táblázat tartalmazza. A kockázat valószínűségének felmérésekor figyelembe kell venni a meglévő ellenőrzési folyamatokat. Szükségessé válhat a meglévő ellenőrzési folyamatok hatékonyságának értékelése.

|  |  |  |
| --- | --- | --- |
| **Fokozat** | **Megnevezés** | **Meghatározás** |
| 1 | Valószínűtlen | Sohasem történt ez előtt, és nincs ok az gondolni, hogy ez most valószínűbb |
| 2 | Nem valószínű | Bekövetkezhet, de valószínűleg nem fog |
| 3 | Valószínű | Valószínűbb, hogy bekövetkezik a kockázat, mint hogy nem |
| 4 | Nagyon valószínű | Kicsi a lehetősége, hogy nem következik be a kockázat, a korábbi előfordulási gyakoriság, vagy a jelenlegi feltételek alapján |
| 5 | Majdnem biztos | Vagy már rendszeresen felmerülő a kockázat, vagy egy ismert ok miatt nagy valószínűséggel bekövetkezik  |

*Táblázat 1 – Kockázat valószínűség fokozatok*

### Hatásvizsgálat

Meg kell becsülni, hogy egy adott kockázat milyen hatással lehet az érintett jogaira, szabadságaira. Figyelembe kell venni a meglévő ellenőrzési folyamatokat, amelyek csökkentik a kockázat hatását.

A következő területekre gyakorolt hatás kell figyelembe venni (legalább):

* pénzügy
* egészség és munkavédelem
* hírnév
* jogi, szerződéses vagy szabályozási kötelezettségek
* egyéb lehetséges hatások

Az egyes kockázatok hatását egy numerikus skálával kell értékelni 1-től (alacsony) 5-ig (magas).

### Kockázat besorolás

A valószínűség és a hatás becslése alapján a két kapott számot összeszorozva kapjuk meg a kockázat mértékét.

Minden kockázat az alábbi intervallumok szerint kerül besorolásra:

* Magas – 12 vagy több
* Közepes – 5-től 10-ig
* Alacsony – 1-től 4-ig



1. *Ábra – Kockázati mátrix*

## Kockázatok értékelése

A kockázatértékelés célja annak eldöntése, hogy a kockázatok elfogadhatóak-e, vagy szükséges a kezelésük. Ehhez figyelembe kell venni a Kockázati mátrixban definiált értékeket.

A kockázati mátrixban található zöld értékek jelzik, hogy a kockázat az elfogadható mérték alatt van. A narancsárga és a piros területek jelzik, hogy a kockázat átlépte az elfogadható szintet, ezért annak kezelésére van szükség.

A kockázatokat priorizálni kell besorolásuk alapján, először a magas kockázati besorolással rendelkezőket célszerű kezelni.

## Kockázatkezelési terv

Azoknál a kockázatoknál, ahol a kockázat meghaladja az elfogadhatóság mértékét, kockázat kezelési terv kidolgozására van szükség.

A kockázatkezelés célja, hogy a kockázat mértékét elfogadható szintre csökkentse. Ez nem mindig lehetséges, előfordul olyan eset, amikor a kockázat mértéke bár csökken, továbbra is az elfogadható szint felett marad. Az adatkezelő, dönthet úgy, hogy elfogadja egy adott esetben a magasabb értéket is. Ebben az esetben a döntést írásban rögzíteni kell az indoklással együtt.

### Kockázatkezelési lehetőségek

A következő lehetőségek állnak rendelkezésre az elfogadható szintet meghaladó kockázatok mértékének csökkentésére:

1. ***A kockázat mértékének megváltoztatása*** – olyan ellenőrzések alkalmazása, ami csökkenti a kockázat valószínűségét vagy hatását
2. ***A kockázat elkerülése*** – olyan intézkedéssel, ami miatt a kockázat megszűnik
3. ***A kockázat megosztása*** – a partnerekkel a kockázat megosztása

A döntési folyamat során meg kell határozni melyik cselekvési irány követendő az adott körülmények ismeretében. A döntés során az alábbiakat figyelembe kell venni

* Üzleti stratégia
* Szabályozási és jogszabályi feltételek
* Technikai feltételek
* Szerződéses feltételek

A kockázatkezelő feladata, hogy minden érdekelt féltől beszerezze a szükséges információkat, és konzultáljon a legjobb megoldásról.

### Az ellenőrzési módszerek kiválasztása

Megfelelő információbiztonsági intézkedéseket kell hozni a kockázatok kezelése érdekében. Ennek érdekében jól működő információbiztonsági rendszert kell kialakítani (ISO 27001 szabvány vagy a 2013 évi L. törvény alapján).

### Adatvédelmi hatásvizsgálati jelentés

Az adatvédelmi hatásvizsgálat az alábbiakat részletezi:

* A javasolt adatkezelési műveletek és a személyes adatok leírása
* Az adatkezelés célja, amennyiben szükséges az adatkezelő jogos érdekének a leírásával
* Az adatkezelés szükségességének és arányosságának értékelése
* Az érintettek jogait és szabadságait érintő kockázatok elemzése
* A kockázatok kategorizálása: melyek elfogadhatóak, melyek kezelendőek
* A kockázatok priorizálása
* Kockázatkezelők megnevezése
* Ajánlott kockázatkezelési lehetőségek
* Bevezetendő ellenőrzések
* Az elvégzendő tevékenységek felelőse
* A tevékenységek ütemezése
* Az ellenőrzések elvégzése utáni fennmaradó kockázati szintek

## A menedzsment jóváhagyása a fennmaradó kockázatokhoz

A hatásvizsgálat folyamán minden egyes szakaszban tájékoztatni kell a vezetést az elért eredményekről és döntésekről, többek között a fennmaradó kockázatokról is. A menedzsment jóváhagyja az adatvédelmi hatásvizsgálati jelentést, és eldönti, hogy részletesen, vagy összefoglalva teszi e közzé.

A menedzsmentnek és az érintett kockázatkezelőnek a jelentést alá kell írnia.

## Előzetes konzultáció a felügyeleti hatósággal

Ha az adatvédelmi hatásvizsgálat megállapítja, hogy az adatkezelés az adatkezelő által a kockázat mérséklése céljából tett intézkedések hiányában valószínűsíthetően magas kockázattal jár, a személyes adatok kezelését megelőzően a felügyeleti hatósággal (NAIH) konzultálni kell. A konzultációhoz az alábbi információkat kell megadni:

* Az adatkezelő, ha vannak, a közös adatkezelők és adatfeldolgozók felelősségi köreit
* Az adatkezelés céljait és módjait
* Az érintettek jogainak és szabadságainak védelmében hozott intézkedéseket és garanciákat
* Az adatok védelme érdekében végrehajtandó ellenőrzéseket
* Az adatvédelmi tisztviselő elérhetőségét
* Az adatvédelmi hatásvizsgálat másolatát

A felügyeleti hatóságnak nyolc hét áll a rendelkezésére, hogy elbírálja a javasolt feldolgozást (ez további hat héttel hosszabbítható). Ha szükséges, a felügyeleti hatóság közli, hogy milyen lépéseket kell tenni, hogy a feldolgozás megfeleljen a GDPR-ban előírtaknak.

## Kockázatkezelési intézkedések végrehajtása

A kockázatkezelési terv jóváhagyása után, az abban leírt intézkedésekkel kapcsolatos eseményeket napi szinten követni és dokumentálni kell. Amennyiben bármely intézkedés késik, vagy akadályozva van, a menedzsmentnek meg kell állapítania ennek következményeit, és meghatározni a következő lépést. Ha az érintett kockázat jelentős hatással van a feldolgozásra, akkor tanácsot kell kérni az adatvédelmi tisztviselőtől (DPO) és/vagy a felügyeleti hatóságtól (NAIH).

## Kockázatellenőrzés és jelentés

Az új és régi ellenőrzések hatékonyságához teljesítménymutatókat kell kidolgozni, hogy az ellenőrzések sikerességét mérni lehessen.

Ezeket az indikátorokat folyamatosan figyelni és jelenteni, hogy a trendeket azonosítani lehessen.

## Rendszeres felülvizsgálat

Az éves felülvizsgálat mellett, folyamatosan értékelni kell a kockázatokat, hogy az azokhoz kapcsolódó ellenőrzések is megfelelőek legyenek. Amennyiben jelentős változások következnek be a feldolgozási folyamatban, akkor felül kell vizsgálni a kockázatokat.

## Szerepkörök és felelősségek

A kockázatkezelés során fontos, hogy a szerepköröket és felelősségeket azonosítsák. A szerepkörök és felelősségek áttekintésére jó megoldás a RACI mátrix (Responsible – felelős, Accountable – jóváhagyó, Consulted – tanácsadó, Informed- informálandó)

### RACI mátrix

Az alábbi táblázat definiálja a felelősségeket:

R= Responsible A= Accountable C= Consulted I= Informed

| **Szerep:** | **Értékelést vezető** | **Kockázat kezelő** | **Felsővezetés** |
| --- | --- | --- | --- |
| **Lépés** |
| Szükségletek és összefüggések definiálása | R | C | A |
| A személyes adatok használatának leírása | R | C | A |
| A kockázatok azonosítása | C | R | A |
| A kockázatok elemzése | C | R | A |
| Kockázatértékelés | C | R | A |
| Kockázatkezelési terv definiálása | R | C | A |
| Menedzsment jóváhagyás a fennmaradó kockázatokra | C | C | A/R |
| Kockázatkezelési terv bevezetése | R | R | A/R |
| Ellenőrzés és jelentés | R | I | A |
| Rendszeres felülvizsgálat  | R | C | A |

1. *Táblázat - RACI mátrix*