Adatvédelmi hatásvizsgálat

Az adatvédelmi hatásvizsgálat elvégzésének általános követelményei

- Kezdetektől megjelenjen a **beépített és alapértelmezett adatvédelem**
- Célzott eljárás
- **Elszámoltathatóság alapelvének** való megfelelés
- Valószínűsíthetően **magas kockázat** fennállása
- 2018. május 25-e után vagy az adatkezelés körülményeiben bekövetkezett jelentős változás esetén

Mikor nem kell hatásvizsgálatot végeznünk?

- az adatkezelés valószínűsíthetően nem jár magas kockázattal,
- a felügyeleti hatóság által összeállított és nyilvánosságra hozott adatkezelések listáján szereplő esetekben,
- hasonló adatkezelések esetében, melyek hasonlóan magas kockázattal járnak egy hatásvizsgálat elvégzés is elegendő lehet.
- „adatkezelés jogalapját uniós vagy az adatkezelőre alkalmazandó tagállami jog írja elő, és e jog a szóban forgó konkrét adatkezelési műveletet vagy műveleteket is szabályozza, valamint e jogalap elfogadása során egy általános hatásvizsgálat részeként már végeztek adatvédelmi hatásvizsgálatot...„

Valószínűsíthetően magas kockázat fennállása (35 cikk (3) bek.)

- Automatizált adatkezelése (a profilozás is)
- Személyes adatok különleges kategóriái
- Nyilvános helyek nagymértékű, módszeres megfigyelés

Minél több kritériumnak felel meg az adatkezelés, annál nagyobb a valószínűsége annak, hogy az adatkezelés magas kockázattal jár az érintettek jogaira és szabadságaira nézve, ezért pedig szükségessé teszi az adatvédelmi hatásvizsgálat elvégzését

Valószínűsíthetően magas kockázat

- pénzügyi vállalkozás, amely hitelreferencia-, pénzmosás és a terrorizmus finanszírozása elleni vagy csalásellenes adatbázist használ ügyfelei szűrésére,
- biotechnológiai vállalat, amely közvetlenül a fogyasztóknak kínál genetikai vizsgálatokat, hogy értékelje, és előre jelezze a betegségek kockázatát és az egészségügyi kockázatokat
- új technológiai vagy szervezési megoldások innovatív használata vagy alkalmazása: az ujjlenyomat- és az arcfelismerés együttes használata
- kiszolgáltatott helyzetben lévő érintettekkel kapcsolatos adatok: pl. gyermekek, munkavállalók, idősek, mentális betegségben szenvedők

Hatásvizsgálat alapvető jellemzői

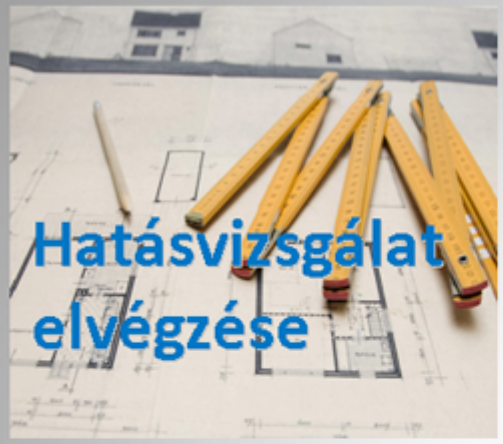
(GDPR)

Hatásvizsgálatot több fajta, különböző módszertan segítségével el lehet végezni, de a hatásvizsgálatnál figyelembe veendő szempontok azonosak

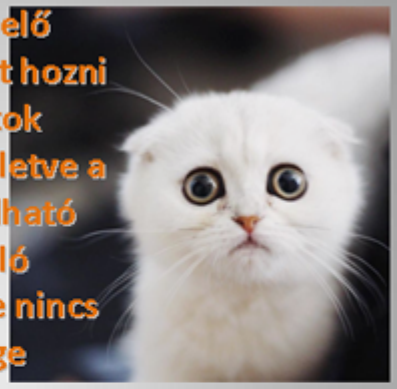
- a tervezett adatkezelési műveletek leírása és az adatkezelés céljának ismertetése;
- szükségesség és arányosság vizsgálata;
- a természetes személyek jogait és szabadságát érintő kockázatok vizsgálata;
- a kockázatok kezelését, valamint a GDPR-ral való összhang igazolását célzó intézkedések.

Megfelelő a hatásvizsgálat ha:

- Adatfeldolgozásról módszeres leírás készült
- Személyes adatok tárolásának időtartamát rögzítették
- Figyelembe vették a jóváhagyott magatartási kódexek előírásait
- Funkcionális leírás készült az adatkezelési műveletről
- Az érintett jogait és szabadságait érintő kockázatokat kezelik
- Érintettek jogait támogató intézkedések
- A személyes adatokhoz használt eszközöket azonosították
- Rendelet betartására irányuló intézkedéseket meghatározták
- Érdekeltek bevonása megtörtént (adatvédelmi tisztviselő és érintettek véleményének kikérése)
- Kockázatokat felmérték



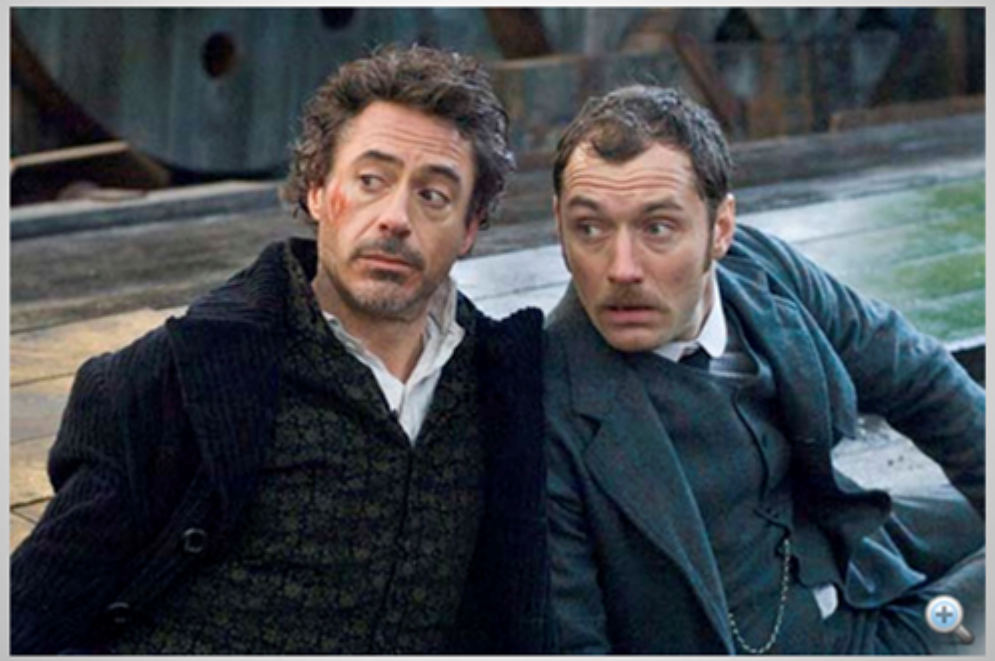
az adatkezelő nem tud megfelelő intézkedéseket hozni a kockázatok enyhítésére, illetve a azok elfogadható szintre való csökkentésére nincs lehetősége



Konzultáció a Hatósággal

Nemzeti Adatvédelmi és Információszabadság Hatóság

Gyakorlati megközelítés



ALAPVETÉS

Egy adatvédelmi hatásvizsgálat alapvetően két nagy részből áll, az adatkezelő értékeli

•Egyrészt az adatvédelmi alapelveknek történő megfelelést, kvázi egy **jogi megfelelőségi elemzést** végez,

•Másrészt az adatbiztonsági intézkedéseket, azaz egy **informatikai biztonsági elemzést** végez.

Mitől jó egy hatásvizsgálat?

- hatásvizsgálat lefolytatásának indoka, strukturált kifejtése
- miért valószínűsíthetően magas az adatkezelés kockázata, illetve milyen kötelező esetkör indokolta annak elvégzését
- kockázati szint meghatározása: a súlyosság és valószínűség:

1. adatvédelem jogi elvei
2. a természetes személyek jogai és szabadságai

- hatásvizsgálati iránymutatásban található szempontrendszer és az információbiztonsági technikai leírások kifejtése, részletezése
- információ-technológiai biztonság kidolgozása
- a belső politikáktól, eljárásoktól és szabályoktól függően érdemes meghatározni és írásba foglalni az egyéb szerep- és felelősségi köröket, például az adatfeldolgozó esetében
- az egyes adatvédelmi alapelvek teljesüléséhez hozzárendelhető kockázatok csökkentéséhez vagy kezelésére szolgáló technikai intézkedések vagy műveletek részletezése

- az adatvédelmi hatásvizsgálat eredményeit a vállalati kockázatkezelési folyamatokba be kell építeni annak érdekében, hogy a felső vezetés nyomon tudja követni a kockázatcsökkentő intézkedések végrehajtását.
- az adatvédelmi tisztviselő, illetőleg az érintettek véleményének beszerzése

- A hatásvizsgálat egy folyamat, nem egyetlen alkalomra szól:

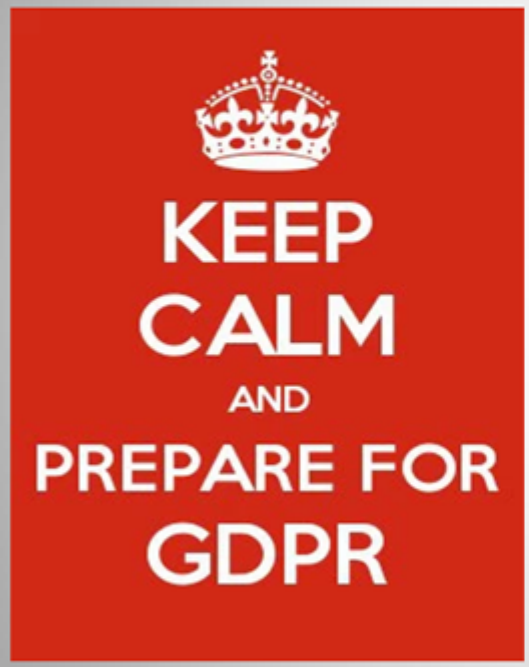
a) A tervezett adatkezelés meghatározása és leírása
b) A meglévő és tervezett intézkedések meghatározása
c) A jogokat és szabadságokat érintő kockázatok vizsgálata
d) A kockázatok kezelésére irányuló intézkedések meghozatala

- Évenkénti felülvizsgálat, vagy jelentősebb változás esetén elvégzendő

Hatásvizsgálat felépítése

- *Tervezett adatkezelés leírása*
- *Szükségesség és arányosság vizsgálata*
- *Megfelelősséget biztosító intézkedések*
- *Érintett adatalanyok jogait és szabadságait érintő kockázatok vizsgálatának leírása*
- *A tervezett kockázatcsökkentő intézkedések leírása*
- *Dokumentálás – mind az eredmények, mind a meghozott döntések vonatkozásában*
- *Felülvizsgálat és nyomon követés*

Köszönöm a figyelmet!



Dr. Nagy Beatrix Havaska

DPO

Szerencsejáték Zrt.

nbhavaska@gmail.com