

Az adatkezelőnek, amennyiben az adatkezelése valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, szükséges az adatkezelést megelőzően elvégeznie adatvédelmi hatásvizsgálatot. A Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: NAIH) az Európai Parlament és a Tanács (EU) 2016/679 Rendelete (a továbbiakban: GDPR) 35. cikkének (4) bekezdése szerinti adatkezelési műveletek típusainak a jegyzékét, amelyekre nézve az adatkezelőnek kötelező hatásvizsgálatot lefolytatnia, az alábbi pontokban részletezve teszi közzé.

A NAIH felhívja az adatkezelők figyelmét arra, hogy a közzétett listában szereplő adatkezelési műveleteken túl az adatkezelőknek általános kötelezettsége az általa folytatott adatkezelések vonatkozásában az adatvédelmi kockázatok felmérése és a megfelelő kockázatkezelés. A listán szereplő adatkezelések nem jelentik azt, hogy csak ezekben az esetekben kell az adatkezelőnek hatásvizsgálatot lefolytatnia. Ha az adatkezelés a GDPR 35. cikkének (1), illetve (3) bekezdésében található feltételeknek megfelel, úgy az adatkezelő köteles hatásvizsgálatot lefolytatni.

A GDPR 35. cikkének (1), illetve (3) bekezdésében írt kötelező eseteken túl – figyelembe véve a GDPR 35. cikkének (10) bekezdésében írt kivételeket – az alábbi adatkezelési műveletek esetében köteles az adatkezelő adatvédelmi hatásvizsgálatot lefolytatni:

1. Ha egy természetes személy **biometrikus adatainak** kezelése módszeres megfigyelésre irányul.
2. Ha kiszolgáltatott helyzetben lévő érintettekkel – különös tekintettel a gyermekekre, munkavállalókra, idős, mentális betegségben szenvedőkre – kapcsolatos **biometrikus adat** kezelése történik.
3. Ha az adatkezelés egy természetes személy **genetikai adatainak** egyéb különleges adatokhoz vagy fokozottan személyes jellegű adatokhoz történő hozzákapcsolásával jár.

4. Ha egy természetes személy **genetikai adatai** kezelésének célja a természetes személy értékelése vagy pontozása¹.
5. **Pontozás.** Az adatkezelés célja, hogy az érintett bizonyos tulajdonságait felmérje, és annak eredménye kihatással van az érintett részére nyújtott, illetve nyújtandó szolgáltatás létrejöttére vagy minőségére.
6. **Hitelképesség értékelése.** Az adatkezelés célja, hogy az érintett hitelképességét felmérje a személyes adatok nagy számú, illetve módszeres értékelése útján.
7. **Fizetőképesség értékelése.** Az adatkezelés célja, hogy az érintett fizetőképességét felmérje a személyes adatok nagy számú, illetve módszeres értékelése útján.
8. **Harmadik személytől gyűjtött adatok további felhasználása.** Az adatkezelés célja, hogy a harmadik személytől begyűjtött személyes adatokat felhasználják az érintettre vonatkozó szolgáltatás visszautasítására vagy megszüntetésére vonatkozó döntés meghozatalánál.
9. **Diákok, hallgatók személyes adatainak értékelésre való felhasználása.** Az adatkezelés célja a diákok, hallgatók felkészültségének, teljesítményének, alkalmasságának, illetve mentális állapotának rögzítése, valamint vizsgálata és az adatkezelés nem jogszabályon alapul, függetlenül attól, hogy az oktatás alap-, közép- vagy felsőfokú.
10. **Profilozás.** Az adatkezelés célja személyes adatok nagy számú, illetve módszeres értékelése révén végzett profilozás, különösen ha az az érintett munkahelyi teljesítményére, gazdasági helyzetére, egészségi állapotára, személyes preferenciáira vagy érdeklődési körére, megbízhatóságra vagy viselkedésre, tartózkodási helyére vagy mozgására vonatkozó jellemzők alapján történik.

¹ Lásd a 29. cikk szerinti adatvédelmi munkacsoport WP 248 számú Iránymutatása szempontrendszerének 1. pontját

11. **Csalás elleni fellépés.** Az adatkezelés célja hitelreferencia-, pénzmosás és a terrorizmus finanszírozása elleni vagy csalásellenes adatbázis felhasználása ügyfelek szűrésére.
12. **Okosmérők.** Az adatkezelés célja közműszolgáltatók által telepített „okosmérők” alkalmazása (fogyasztási szokások nyomon követése).
13. **Joghatással vagy hasonló jelentős hatással járó automatizált döntéshozatal.** Az adatkezelés célja a természetes személy tekintetében joghatással bíró vagy a természetes személyt hasonlóképpen jelentős mértékben érintő döntések meghozatala, amely adatkezelés adott esetben egyének kirekesztését vagy hátrányos megkülönböztetését eredményezheti.
14. **Módszeres megfigyelés.** Érintettek nagyszámú és módszeres megfigyelése jellemzően közterületeken vagy nyilvános helyeken történő kamerarendszerek, drónok felhasználásával, illetve bármely más új technológia használatával (Wi-Fi tracking, Bluetooth tracking, testkamera).
15. **Helymeghatározási adatok** kezelése, ha az módszeres megfigyelésre vagy profilalkotásra utal.
16. **Munkavállaló munkájának megfigyelése.** Munkavállalók munkájának megfigyelése. Az adatkezelés célja a munkavállaló munkájának megfigyelése során a munkavállaló személyes adatainak nagy számú és módszeres feldolgozása, illetve értékelése.² Például GPS megfigyelő autóban történő elhelyezése, kamerás megfigyelés lopás vagy csalás elleni fellépés céljából.
17. **Különleges adatok nagy számban való kezelése.** A GDPR (91) preambulumbekkezdése alapján a személyes adatok kezelése nem tekinthető nagymértékűnek, ha az adatkezelés egy adott szakorvos, egészségügyi szakember betegei vagy egy adott ügyvéd ügyfelei személyes adataira vonatkozik.

² Lásd a 29. cikk szerinti adatvédelmi munkacsoport WP 248 számú Iránymutatása szempontrendszerének 1. és 3. pontját

18. **Nagyszámú személyes adatok kezelése bűnüldözési célból**
19. **Kiszolgáltatott helyzetben** lévő érintettekkel kapcsolatos, nagy számban kezelt adatok eredeti céltól eltérő kezelése: pl. gyermekek, idősek, mentális betegségben szenvedők esetében.
20. **Gyermekek** személyes adatainak kezelése profilozás, automatikus döntéshozatal, vagy **marketing céljából**, vagy közvetlenül részükre kínált, információs társadalommal összefüggő szolgáltatások ajánlása vonatkozásában.
21. **Új technológiai** megoldások használata az adatkezelés során. Ideértve az érzékelővel ellátott eszközök által előállított adatok interneten vagy más csatornán keresztül történő nagyszámú kezelése (pl.: okos televízió, okos háztartási eszközök, okos játékok stb.), és amelyek adatokat szolgáltatnak a természetes személy fizetőképességére, egészségére, személyes érdeklődési körére, megbízhatóságára vagy viselkedésére, tartózkodási helyére és amelyek alapján profilalkotás történik.
22. **Egészségügyi adatokra vonatkozó adatkezelések.** Nagy számban kezelt adatok tekintetében a kórházak, egészségügyi ellátó intézmények, magán-egészségügyi szolgáltatók vagy nagyszámú páciensi körrel rendelkező természetgyógyászok által kezelt különleges adatok vonatkozásában. Ideértve a nagyobb sportlétesítmények, edzőtermek által a tagoktól felvett egészségügyi adatok kezelése
23. Amikor több adatkezelő **egy egész ágazat által közösen használt alkalmazást, rendszert, eszközt, illetve platformot** tervez létrehozni, amelyben különleges adatokat is kezelnek.
24. Az adatkezelés célja a különböző forrásokból származó adatok **összevonása, egymással való megfeleltetése** vagy **összehasonlítása.**

Az adatvédelmi hatásvizsgálat eredményéről előzetesen konzultálni kell a felügyeleti hatósággal, ha az érintettek jogait és szabadságait érintő kockázatok adatkezelő által történt értékelését követően az adatkezelő nem tud megfelelő intézkedéseket hozni a kockázatok elfogadható szintre való csökkentésére, azaz a fennmaradó kockázatok továbbra is jelentősek.

Az adatkezelőknek folyamatosan értékelniük kell az adatkezelési tevékenységeiből eredő kockázatokat, hogy felismerjék, ha az adatkezelés valamely fajtája „valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve”. Az adatvédelmi hatásvizsgálat egy folyamat, különösen akkor, ha az adatkezelési művelet dinamikus és állandóan változik. Az adatvédelmi hatásvizsgálatot nem egyetlen alkalommal, hanem folyamatosan kell végezni.