GENERALI ÖNKÉNTES NYUGDÍJPÉNZTÁR

GENERALI EGÉSZSÉG- ÉS ÖNSEGÉLYEZŐ PÉNZTÁR

ADATVÉDELMI HATÁSVIZSGÁLAT

DPIA

Tartalom

1 Fogalmak és meghatározások

Rövidítés/Fogalom	Magyarázat/Meghatározás
Adatkezelő	Az a természetes vagy jogi személy, aki/amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy más adatkezelőkkel közösen meghatározza.
Adatfeldolgozó	az a természetes vagy jogi személy, amely az adatkezelő nevében személyes adatokat kezel.
Adatvédelmi hatásvizsgálat vagy DPIA	Hatásvizsgálat arra vonatkozóan, hogy a tervezett adatkezelési műveletek a személyes adatok védelmét hogyan érintik, amennyiben az adatkezelés valamely – különösen új technológiákat alkalmazó – típusa –, figyelemmel annak jellegére, hatókörére, körülményére és céljaira, valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve.
Érintett	Olyan azonosítható 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.
Igazságügyi adatok	A büntetőjogi felelősség megállapítására, illetve bűncselekményekre, vagy ezekhez kapcsolódó biztonsági intézkedésekre vonatkozó személyes adatok.
Személyes adat	Azonosított vagy azonosítható természetes személyre („érintett”) közvetlen vagy közvetett módon vonatkozó bármely információ.
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.
Különleges adat	A személyes adatok különleges kategóriáiba tartozó minden adat, azaz a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a genetikai adatok, a természetes személyek egyedi azonosítását célzó biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok.
Egyszerűsített adatvédelmi hatásvizsgálat	Egyszerűsített adatvédelmi hatásvizsgálat annak felmérésére, hogy az adatkezelés magas kockázatot hordoz-e.

2 Bevezető

A jelen mellékletet együtt kell értelmezni a személyes adatok védelméről szóló szabályzattal, amely meghatározza a Személyes adatok kezelésére vonatkozó előírásokat.

3 A SZABÁLYOZÁS HÁTTERE

A GDPR 35. cikke alapján, ha az Adatkezelő a természetes személyek jogaira és szabadságaira nézve valószínűsíthetően magas kockázattal járó adatkezelést tervez, úgy az Adatkezelést megelőzően Adatvédelmi hatásvizsgálatot kell végeznie.

Bizonyos esetekben az Adatkezelőnek ki kell kérnie az érintetteknek vagy képviselőiknek a véleményét a tervezett Adatkezelésről.

Ha az Adatvédelmi hatásvizsgálat megállapítja, hogy az adatkezelés valószínűsíthetően magas kockázattal jár, a személyes adatok kezelését megelőzően konzultálnia kell a felügyeleti hatósággal.

4 Az adatvédelmi hatásvizsgálat (DPIA)

Az Adatvédelmi hatásvizsgálat (DPIA) célja annak garantálása, hogy az olyan adatkezelési műveleteket, amelyek valószínűsíthetően magas kockázattal járnak a természetes személyek jogaira és szabadságaira nézve, az érintett pénztár megfelelő kockázatcsökkentő intézkedésekkel kezeli.
Annak eldöntésére, hogy az egyes Adatkezelési műveletek magas kockázatot hordoznak-e, Egyszerűsített Adatvédelmi hatásvizsgálatot kell lefolytatni.
Az adatkezelési tevékenység megkezdése előtt a felügyeleti hatósággal konzultálni kell minden olyan esetben, ahol a bevezetett kockázatcsökkentő intézkedések elégtelennek bizonyulnak a kockázat [elfogadható szintre történő] csökkentésére, vagyis a fennmaradó kockázat továbbra is magas. Meghatározott körülmények esetén a pénztár köteles kikérni az érintettek vagy képviselőik véleményét a tervezett adatkezelésről.

Az adatvédelmi hatásvizsgálat azért is fontos eszköz, mert ennek lefolytatásával igazolható, hogy a pénztár a megfelelő intézkedések bevezetésével eleget tett a GDPR vonatkozó előírásainak. Fontos azonban, hogy az adatvédelmi hatásvizsgálat lefolytatása nem minden esetben kötelező.

Kötelező az adatvédelmi hatásvizsgálat lefolytatása többek között az alábbi esetekben:

- természetes személyekre vonatkozó egyes személyes jellemzők olyan módszeres és kiterjedt értékelése, amely automatizált adatkezelésen – ideértve a profilalkotást is –alapul, és amelyre a természetes személy tekintetében joghatással bíró vagy a természetes személyt hasonlóképpen jelentős mértékben érintő döntések épülnek;
- Igazságügyi adatok vagy Különleges adatok nagy számban történő kezelése esetén
- Nyilvános helyek nagymértékű és módszeres megfigyelése esetén
- Ha azt a felügyeleti hatóság előírja.

Nem kötelező az adatvédelmi hatásvizsgálat lefolytatása többek között az alábbi esetekben:

- -Az Adatkezelés valószínűsíthetően nem jár magas kockázattal az Érintettek jogaira és szabadságaira nézve;
- -Ha az adatkezelés a jellegét, hatókörét, körülményét és céljait tekintve nagyon hasonlít olyan adatkezelésre, amelyről már készült adatvédelmi hatásvizsgálat. Ilyen esetekben felhasználhatók a hasonló adatkezelés adatvédelmi hatásvizsgálatának eredményei.
- -Ha az 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;
- -Ha az adatkezelés szerepel azoknak az adatkezelési műveleteknek a helyi Felügyeleti Hatóság által összeállított jegyzékében, amelyekre vonatkozóan nem kell adatvédelmi hatásvizsgálatot végezni.

5 Folyamatok és eljárások

5.1 EGYSZERŰSÍTETT ADATVÉDELMI HATÁSVIZSGÁLAT

Bármely feladatkör, amely új, Adatkezeléssel együttjáró projekt vagy tevékenység megkezdését tervezi, köteles felmérni, hogy az adott adatkezelési művelet valószínűsíthetően magas kockázattal jár-e az Érintettek jogaira és szabadságaira nézve.

Ennek megállapítására Egyszerűsített adatvédelmi hatásvizsgálatot köteles lefolytatni az új projekt elindítását illetve az új tevékenység megkezdését megelőzően. Az Egyszerűsített DPIA elvégzéséhez szükséges sablont az jelen szabályozás 1. számú melléklete tartalmazza.

Az Egyszerűsített DPIA során meg kell határozni a tervezett Adatkezelési műveletek főbb jellemzőit, és hogy az alábbi kockázati tényezők felmerülnek-e az egyes Adatkezelési műveletek során:

- Értékelés vagy pontozás, ideértve a profilalkotást és az előrejelzést is, különösen "az Érintett munkahelyi teljesítményére, gazdasági helyzetére, egészségi állapotára, személyes preferenciáira vagy érdeklődési körökre, megbízhatóságra vagy viselkedésre, tartózkodási helyére vagy mozgására vonatkozó jellemzők" alapján;
- Joghatással vagy hasonló jelentős hatással járó automatizált döntéshozatal: vagyis olyan adatkezelés, amelynek célja a természetes személy tekintetében joghatással bíró vagy „a természetes személyt hasonlóképpen jelentős mértékben érintő döntések meghozatala;
- Módszeres megfigyelés: vagyis az érintettek megfigyelése, nyomon követése vagy ellenőrzése céljából végzett adatkezelés, többek között a hálózatokon keresztüli adatgyűjtés vagy a nyilvános helyek nagymértékű, módszeres megfigyelése;
- Különleges adatok, Igazságügyi adatok vagy fokozottan személyes jellegű adatok kezelése (például helymeghatározó adatok, amelyek gyűjtése megkérdőjelezi a mozgás szabadságát, pénzügyi adatok, amelyek csalásra használhatók);
- Nagy számban kezelt adatok (figyelemmel az érintettek számára, a kezelt Személyes adatok mennyiségére, az adatkezelési tevékenység időtartamára vagy állandó jellegére, az adatkezelési tevékenység földrajzi kiterjedésére);
- Adatkészletek egymással való megfeleltetése vagy összevonása (például két vagy több, különböző célból végzett adatkezelési műveletből származó adatokkal, az Érintett ésszerű elvárásait meghaladó módon);
- Kiszolgáltatott helyzetben lévő érintettekkel kapcsolatos adatok (például mentális betegségben szenvedők, menedékkérők vagy az idősek, betegek stb.);
- Új technológiai vagy szervezési megoldások innovatív használata vagy alkalmazása, például az ujjlenyomat- és az arcfelismerés együttes használata a hatékonyabb beléptetés érdekében stb;
- Azok az esetek, amikor az adatkezelés önmagában megakadályozza, hogy az Érintettek a jogaikat gyakorolják vagy szolgáltatásokat vegyenek igénybe vagy szerződést érvényesítsenek. Ide tartoznak az Érintettek számára szolgáltatás igénybevételének vagy szerződéskötésnek a lehetővé tételére, módosítására vagy elutasítására irányuló adatkezelési műveletek.

Amennyiben a tervezett Adatkezelési művelet kapcsán a fenti kockázati tényezők közül legalább kettő felmerül, úgy az Adatkezelés valószínűsíthetően magas kockázattal jár az Érintettek jogaira és szabadságaira nézve, és ezért szükség van Adatvédelmi hatásvizsgálatra.

Olyan esetekben, ahol az Egyszerűsített DPIA eredménye alacsony vagy közepes kockázatot mutat, tehát Adatvédelmi hatásvizsgálat lefolytatására nincs szükség, a kockázat [elfogadható szintre történő] csökkentésére kockázatcsökkentő intézkedéseket kell hozni.

Minden egyes Adatkezelési tevékenység esetében az Egyszerűsített adatvédelmi hatásvizsgálat eredményét csatolni kell a Személyes adatok kezelésére vonatkozó nyilvántartáshoz.

5.2 AZ EGYSZERŰSÍTETT ADATVÉDELMI HATÁSVIZSGÁLAT EREDMÉNYEINEK ÉRTÉKELÉSE

Az Egyszerűsített adatvédelmi hatásvizsgálat elvégzése után annak eredményeit az érintett feladatkör felülvizsgálatra megküldi a DPO részére.

A szóban forgó Adatkezelési művelet jellegétől függően a DPO határozhat úgy, hogy a kockázatot magasnak minősíti akkor is, ha a kockázati tényezők közül csak egy merül fel (pl.: Különleges adatok kezeléséről van szó), illetve, hogy a kockázatot nem minősíti magasnak akkor sem, ha legalább két tényező felmerül.

A vizsgálat során a legfontosabb mérlegelendő tényezők közé tartozik – többek között – a kezelt Személyes adatok mennyisége, jellege, az Érintettek száma, valamint az adatkezeléshez használt eszközök.

Amennyiben a kockázat alacsony vagy közepes besorolást kap, tehát adatvédelmi hatásvizsgálat lefolytatására nincs szükség, az érintett feladatkör köteles a DPO-val egyeztetni arról, hogy milyen kockázatcsökkentő intézkedéseket kell alkalmaznia az adatkezelés során.

Amennyiben a DPO ajánlásaitól eltérő intézkedések kerülnek bevezetésre, azt indokolással ellátva megfelelően dokumentálni kell.

5.3 AZ ADATVÉDELMI HATÁSVIZSGÁLAT LEFOLYTATÁSA

Amennyiben az előzetes felmérés alapján a tervezett Adatkezelési művelet magas kockázatot jelent, úgy a jelen Iránymutatás 1. számú mellékletében közzétett dokumentumsablon alapján le kell folytatni az Adatvédelmi hatásvizsgálatot.

Az Adatvédelmi hatásvizsgálat érinthet egyetlen Adatkezelési műveletet, de elvégezhető több, kockázatait tekintve egymáshoz hasonló adatkezelési művelet értékeléséhez is, amennyiben az egyes Adatkezelési műveletek jellegét, hatókörét, körülményeit és céljait megfelelő módon figyelembe veszik.

Az adatvédelmi hatásvizsgálatot – a DPO szakmai iránymutatása mellett – annak a feladatkörnek kell lefolytatnia, amely a projekt vagy a tevékenység végrehajtását tervezi.

Az egyes Adatkezelési műveletek jellemzői alapján, az Adatvédelmi hatásvizsgálat lefolytatásához más feladatkörök segítsége is kérhető.

Amennyiben az Adatkezelést részben vagy teljes egészében Adatfeldolgozó végzi, úgy az érintett Adatfeldolgozó köteles az Adatvédelmi hatásvizsgálat lefolytatásában a Pénztárral együttműködni, és a szükséges információkat átadni. A fentiek okán az Adatfeldolgozókkal kötött szerződéseknek tartalmazniuk kell erre vonatkozó szerződéses rendelkezéseket.

Az adatvédelmi hatásvizsgálatnak legalább a következőkre ki kell terjednie:

- A tervezett Adatkezelési műveletek módszeres leírására és az adatkezelés céljainak ismertetésére, beleértve adott esetben a Pénztár által érvényesíteni kívánt jogos érdeket (pl.: az Adatkezelés jellege, hatóköre, körülményei és céljai, a kezelt Személyes adatok típusa, a Személyes adatokon elvégzendő műveletek leírása, a Személyes adatok tárolásra használt eszköz meghatározása, külső szolgáltatók bevonása, a címzettek meghatározása, EGT-n kívüli adattovábbítás, stb.);
- Az adatkezelés céljaira figyelemmel az adatkezelési műveletek szükségességi és arányossági vizsgálatára (pl.: annak egyértelmű meghatározása, hogy miért van szükség a Személyes adatok kezelésére, és miért nem lehetséges álnevesítési vagy anonimizálási technikák alkalmazása, a Személyes adatok kezelésének jogalapja, az Érintettek jogainak védelmére hozott intézkedések, stb.);
- Az érintettek jogait és szabadságait érintő kockázatok vizsgálatára (pl.: az Érintettek szemszögéből a kockázatok forrását, jellegét, egyediségét és súlyosságát, a Személyes adatokhoz való jogellenes hozzáférés, az adatok nemkívánatos módosítása vagy eltűnése esetén ezeknek az Érintettek jogait és szabadságait érintő hatásait, stb.)
- Az Érintettek jogait és szabadságait érintő kockázatok orvoslására irányuló intézkedések meghatározására, ideértve különösen a Személyes adatok védelmét célzó, a GDPR-ben illetve bármely egyéb vonatkozó adatvédelmi jogszabályban vagy rendeletben előírt garanciákat, biztonsági intézkedéseket és mechanizmusokat, figyelemmel az Érintettek és bármely egyéb személy jogaira és jogos érdekeire (pl.: titkosítási eljárások felhő-alapú megoldásoknál, garanciák határokon átnyúló adattovábbítás(ok) esetén, stb.)
- Az adatvédelmi hatásvizsgálat eredményét minden egyes Adatkezelési tevékenységre vonatkozóan csatolni kell a Személyes adatok kezelésére vonatkozó nyilvántartáshoz.

5.4 AZ ADATVÉDELMI HATÁSVIZSGÁLAT EREDMÉNYEINEK ÉRTÉKELÉSE

Az Adatvédelmi hatásvizsgálat elvégzése után annak eredményeit az érintett feladatkör megküldi a DPO részére, aki a fennmaradó kockázatot szintet minősíti (vagyis azt, hogy az meghatározott kockázatok mérséklését célzó intézkedések után az Érintettek jogait és szabadságait milyen kockázatok érintik)

Az Adatvédelmi hatásvizsgálat eredményeinek értékelését követően a DPO mérlegeli, hogy:

- A meghatározott intézkedések megfelelőek-e a kockázat mérséklésére.
- Ha igen, úgy a feladatkör megkezdheti a projektet illetve tevékenységet azzal a feltétellel, hogy az adatvédelmi hatásvizsgálatban leírt kockázatcsökkentő intézkedéseket megfelelően alkalmazza;
- Az adatvédelmi hatásvizsgálatban megjelölt intézkedések nem megfelelőek a kockázat mérséklésére.

Ebben az esetben a DPO további kockázatcsökkentő intézkedéseket határoz meg, és egyeztet az érintett feladatkörrel arról, hogy ezek bevezetése/alkalmazása lehetséges-e.

Amennyiben ezen intézkedések nem megvalósíthatóak (pl.: a felhő-alapú szolgáltatás szolgáltatója jelentős többletköltségek nélkül nem tudja a Személyes adatok titkosítását elvégezni, vagy a Személyes adatok törlése technikai akadályokba ütközik, stb.), vagy nem lehet meghatározni további kockázatcsökkentő intézkedéseket, úgy előzetes konzultációt kell kezdeményezni a Felügyeleti Hatósággal. Amennyiben a DPO ajánlásaitól eltérő intézkedések kerülnek bevezetésre, azt indokolással ellátva megfelelően dokumentálni kell.

5.5 FELÜGYELETI HATÓSÁGGAL LEFOLYTATANDÓ ELŐZETES KONZULTÁCIÓ

Amennyiben az Adatvédelmi hatásvizsgálat arra a következtetésre jut, hogy a fennmaradó kockázat továbbra is jelentős, akkor az új projekt illetve tevékenység megkezdését megelőzően kötelező konzultálni az Adatvédelmi Felügyeleti Hatósággal.

A konzultáció lebonyolításáért a DPO felelős.

A Felügyeleti Hatóságnak küldendő tájékoztatásnak tartalmazni kell legalább az alábbi információkat az Adatkezelési művelettel kapcsolatban:

- az Adatkezelésben érintett Adatkezelő és az Adatfeldolgozó kötelezettségeit;
- a tervezett Adatkezelés céljait és az ahhoz használni tervezett eszközöket;
- az Érintettek jogainak és szabadságainak védelmét célzó intézkedéseket és garanciákat;
- adott esetben a DPO elérhetőségeit;
- a Pénztár által lefolytatott adatvédelmi hatásvizsgálat másolatát, valamint
- minden egyéb olyan adatot és információt, melyet a Felügyeleti Hatóság kifejezetten kér.

A tervezett projekt illetve tevékenység nem kezdhető meg addig, amíg a DPO nem küld tájékoztatást az érintett feladatkörnek arról, hogy a Felügyeleti Hatóság az Adatkezelési műveletet jóváhagyta.

A feladatkör köteles az Adatkezelést mindenben szigorúan a Felügyeleti Hatóság által meghatározottak szerint végezni. Amennyiben a Felügyeleti Hatóság állásfoglalása kedvezőtlen, úgy a projekt nem kezdhető meg.

5.6 AZ ÉRINTETTEK VÉLEMÉNYÉNEK KIKÉRÉSE

Bizonyos esetekben kikérhető az Érintett adatalanyok véleménye a tervezett Adatkezeléssel kapcsolatban (pl.: a munkavállalók Internet használatának és elektronikus levelező rendszerének széleskörű megfigyelése a munkavállalók hatékonyságának értékelésére, a helyi üzemi tanács/szakszervezet bevonásával), feltéve, hogy ez nem sérti a Pénztár gazdasági érdekeit vagy közérdeket, illetve az Adatkezelési műveletek biztonságát.

A DPO tájékoztatja az érintett feladatkört arról, ha az Érintett adatalanyok megkérdezése szükségesnek tűnik.

5.7 AZ ADATVÉDELMI HATÁSVIZSGÁLAT DOKUMENTÁLÁSA

Az Adatvédelmi hatásvizsgálat lefolytatását megfelelően dokumentálni kell.

A projekt vagy tevékenység elindítását tervező feladatkör köteles mind az Egyszerűsített adatvédelmi hatásvizsgálatot, mind a teljeskörű Adatvédelmi hatásvizsgálatot aláírni és biztonságos módon megőrizni a helyi nyilvántartási előírásoknak megfelelően. Hasonlóképpen, a DPO értékelését és állásfoglalását is megfelelően dokumentálni kell, az ezekről készült dokumentumokat pedig meg kell őrizni a jogszabályban előírt időpontig.

5.8 AZ ADATVÉDELMI HATÁSVIZSGÁLAT FELÜLVIZSGÁLATA

Bizonyos Adatkezelési műveletek időtartama alatt szükséges lehet az adatvédelmi hatásvizsgálat felülvizsgálata és aktualizálása, hogy a vizsgálati megállapítások megfelelően tükrözzék magában az Adatkezelési tevékenységben illetve az Adatkezelési tevékenységből eredő kockázatban bekövetkező változásokat vagy módosításokat (pl.: új technológia alkalmazását kezdte meg, vagy a Személyes adatok felhasználási célja megváltozott, stb.).

A projektet lebonyolító illetve a tevékenységet végző feladatkör tehát köteles a DPIA-t folyamatosan felülvizsgálni és rendszeresen újra értékelni.

6 Folyamatban lévő Adatkezelési műveletek vizsgálata

Annak érdekében, hogy a már folyamatban lévő Adatkezelési műveletek megfelelő értékelése és kezelése biztosított legyen, a Személyes adatokra vonatkozó Adatkezelési nyilvántartás első kitöltésekor Egyszerűsített adatvédelmi hatásvizsgálatot kell lefolytatni minden egyes rögzítésre kerülő adatkezelési művelet vonatkozásában.

Amennyiben az előzetes felmérés alapján az Adatkezelési művelet magas kockázatot jelent, úgy le kell folytatni az Adatvédelmi hatásvizsgálatot.

Ehhez a 4. pontban leírt folyamatot kell végrehajtani.