NEMZETI FEJLESZTÉSI KÖZPONT

A Nemzeti Fejlesztési Központot vezető államtitkár
6./2025. (IV. 17.) államtitkári rendelkezése

a személyes adatok védelméről, valamint a Nemzeti Fejlesztési Központ adatvédelmi és adatbiztonsági szabályzatáról

Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény 25/A. § (3) bekezdésére tekintettel – a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről szóló, 2016. április 27-i (EU) 2016/679 európai parlamenti és tanácsi rendelet 24. cikk (2) bekezdésében foglaltak alapján – a Nemzeti Fejlesztési Központ által kezelt személyes adatok védelme érdekében a következőképpen rendelkezem:

1. Általános rendelkezések

1. § (1) A szabályzat célja, hogy a Nemzeti Fejlesztési Központ (a továbbiakban: NFK) meghatározza a személyes adatok kezelése során irányadó adatvédelmi és adatbiztonsági előírásokat, ezáltal biztosítva tevékenységével összefüggésben a személyes adatok védelméhez fűződő jog érvényesülését, illetve az NFK által kezelt személyes adatok jogosulatlan felhasználásának megakadályozását.
(2) A szabályzat hatálya az NFK valamennyi szervezeti egységére, munkatársára, továbbá az NFK-val szerződéses jogviszonyban álló adatfeldolgozóra kiterjed.
(3) A szabályzat rendelkezéseit alkalmazni kell az NFK szervezeti egységei által folytatott adatkezelési műveletekre – ideértve a munkavégzéssel összefüggésben az NFK munkatársai által birtokolt adathordozókon, és számítógépes eszközökön tárolt személyes adatokat –, az adatok megszerzésétől vagy a szervezeti egységnél történő keletkezésétől azok törléséig, illetve megsemmisítéséig, az adatkezelés teljes folyamatára kiterjedően, függetlenül az adatok megjelenési formájától, valamint attól, hogy az adatok valamely nyilvántartási rendszer vagy irat részét képezik-e.
(4) A szabályzat rendelkezéseit érvényre kell juttatni az NFK adatkezelési tevékenységében állandó vagy eseti jelleggel résztvevő vagy abban közreműködő, az NFK érdekkörében adatfeldolgozóként vagy közös adatkezelőként eljáró természetes és jogi személyekkel, jogi személyiséggel nem rendelkező szervezetekkel kötendő szerződésekben, megállapodásokban.
(5) A szabályzat hatálya nem terjed ki a közhitelű nyilvántartásból történő, törvényben szabályozott adatszolgáltatásra.
(6) Jogszabály eltérő rendelkezése hiányában a szabályzatot kell alkalmazni a minősített adathordozóban szerepeltetett személyes adatok kezelése során.

2. Értelmező rendelkezések

2. § A szabályzat alkalmazásában

a) adatállomány: az egy nyilvántartásban kezelt adatok összessége;

b) adatbirtokos: az NFK önálló szervezeti egységének vezetője, aki - önállóan vagy másokkal együtt - az adat kezelésének célját meghatározza, az adatkezelésre - beleértve a felhasznált eszközt - vonatkozó döntéseket meghozza és végrehajtja, vagy az általa megbízott adatfeldolgozóval végrehajtatja,

c) adatfeldolgozás: az adatkezelő megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által végzett adatkezelési műveletek összessége;

d) adatfeldolgozó: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely - törvényben vagy az Európai Unió kötelező jogi aktusában meghatározott keretek között és feltételekkel - az adatkezelő megbízásából vagy rendelkezése alapján személyes adatokat kezel;

e) adatkezelés: az alkalmazott eljárástól függetlenül az adaton végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adat további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép);

f) adatkezelés jogalapja: főszabály szerint az érintett hozzájárulása vagy törvényben elrendelt kötelező adatkezelés;

g) adatkezelő szerv: az NFK;

h) adat tárolására alkalmas eszköz: az NFK munkatársainak a munkavégzéséhez használt, illetve birtokába adott számítástechnikai eszköz, valamint adathordozó, amely alkalmas adatok megőrzésére és tárolására;

i) adatvédelmi incidens: az adatbiztonság olyan sérelme, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisülését, elvesztését, módosulását, jogosulatlan továbbítását vagy nyilvánosságra hozatalát, vagy az azokhoz való jogosulatlan hozzáférést eredményezi;

j) címzett: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely részére személyes adatot az adatkezelő, illetve az adatfeldolgozó hozzáférhetővé tesz;

k) EGT-állam: az Európai Unió tagállama és az Európai Gazdasági Térségről szóló megállapodásban részes más állam, továbbá az az állam, amelynek állampolgára az Európai Unió és tagállamai, valamint az Európai Gazdasági Térségről szóló megállapodásban nem részes állam között létrejött nemzetközi szerződés alapján az Európai Gazdasági Térségről szóló megállapodásban részes állam állampolgárával azonos jogállást élvez;

l) érintett: bármely információ alapján azonosított vagy azonosítható természetes személy;

m) harmadik személy: olyan természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely nem azonos az érintettel, az adatkezelővel, az adatfeldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére irányuló műveleteket végeznek;

n) hozzájárulás: az érintett akaratának önkéntes, határozott és megfelelő tájékoztatáson alapuló egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy az akaratát félreérthetetlenül kifejező más magatartás útján jelzi, hogy beleegyezését adja a rá vonatkozó személyes adatok kezeléséhez;
o) nemzetközi szervezet: a nemzetközi közjog hatálya alá tartozó szervezet és annak alárendelt szervei, továbbá olyan egyéb szerv, amelyet két vagy több állam közötti megállapodás hozott létre vagy amely ilyen megállapodás alapján jött létre;
p) nyilvánosságra hozatal: az adat bárki számára történő hozzáférhetővé tétele;
q) személyes adat: a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről szóló, 2016. április 27-i (EU) 2016/679 európai parlamenti és tanácsi rendelet (a továbbiakban: GDPR) szerinti adat, különösen a név, a cím, a személyazonosító igazolvány/útlevél száma, a javadalmazással kapcsolatos információk, a kulturális azonossággal kapcsolatos információk, az internetprotokoll-cím.

3. Az adatvédelmi tevékenység felügyelete, irányítása

3. § (1) A személyes adatok védelméről az NFK-t vezető államtitkár (a továbbiakban: államtitkár) az adatvédelmi tisztviselő útján gondoskodik.
(2) Az államtitkár közvetlenül felügyeli az adatvédelmi tisztviselő tevékenységét, az adatvédelmi tisztviselői feladatok ellátása tekintetében.
(3) Az államtitkár az adatvédelemmel kapcsolatos feladatai körében
a) adatvédelemmel kapcsolatos vizsgálatot rendelhet el,
b) kiadja az NFK adatvédelemmel kapcsolatos belső szabályait vagy szabályzatát.

4. Az adatkezelő szerv vezetőjének feladatai

4. § Az államtitkár, az adatkezelő szerv vezetőjeként felel az általa vezetett adatkezelő szerv vonatkozásában:
a) az adatvédelmi és adatbiztonsági intézményrendszer kiépítéséért és működtetéséért,
b) a személyes adatok védelméhez és az információszabadsággal kapcsolatos követelmények érvényesüléséhez szükséges személyi, tárgyi és technikai feltételek biztosítását célzó, hatáskörébe tartozó intézkedések meghozataláért,
c) az NFK munkatársainak adatvédelmi oktatásáért és rendszeres továbbképzéséért,
d) a rendszeres adatvédelmi ellenőrzésért, az ellenőrzés során esetlegesen feltárt hiányosságok vagy jogszabálysértő körülmények megszüntetéséért, a személyi felelősség megállapításához szükséges eljárás kezdeményezéséért, ennek érdekében a hatáskörébe tartozó eljárások lefolytatásáért,
e) az érintett jogainak gyakorlásához, valamint tájékoztatásához szükséges feltételek biztosításáért,
f) az adatvédelmi hatásvizsgálatok lefolytatásáért és rendszeres felülvizsgálatáért, valamint az ahhoz szükséges feltételek biztosításáért,

g) az adatvédelmi feladatok ellátására alkalmas adatvédelmi tisztviselő kijelöléséért, nevének és elérhetőségének a Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: Hatóság) részére történő bejelentéséért,
h) az adatvédelmi tisztviselő feladatainak végrehajtásához, a személyes adatokhoz és az adatkezelési műveletekhez való hozzáféréshez, valamint az adatvédelmi tisztviselő szakértői szintű ismereteinek fenntartásához szükséges feltételek és források biztosításáért, valamint
i) az adatvédelmi tevékenységgel kapcsolatos közzétételi kötelezettség teljesítéséért.

5. Az adatvédelmi tisztviselő

5. § (1) Az NFK adatvédelmi tisztviselőjét az államtitkár az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) 25/L. §-ában foglaltak alapján jelöli ki.
(2) Adatvédelmi tisztviselőnek csak olyan személy jelölhető ki, aki a GDPR-ban és az Infotv-ben foglalt feltételeknek megfelel.
(3) Nem lehet adatvédelmi tisztviselő, aki az adatkezelő szervnél adatkezeléssel kapcsolatos döntések meghozatalára jogosult személy, vagy annak a Polgári Törvénykönyvről szóló 2013. évi V. törvény szerinti hozzátartozója.
6. § (1) Az adatvédelmi tisztviselő nevéről és elérhetőségéről az NFK munkatársait tájékoztatni kell.
(2) Az adatvédelmi tisztviselő feladatainak ellátása céljából, az ahhoz szükséges mértékben a minősítéssel védett iratokba betekinthet.
(3) Az adatvédelmi tisztviselő számára az államtitkár hozzáférést biztosít a feladatai végrehajtásához szükséges elektronikus rendszerekhez, iratokhoz, egyéb adathordozókhoz, valamint biztosítja a szakmai ismeretei naprakészen tartásához szükséges feltételeket, rendelkezésére bocsátja a szükséges jogosultságokat és erőforrásokat.
(4) Az adatvédelmi tisztviselő a GDPR-ban és az Infotv-ben foglaltak alapján a következő feladatokat látja el:
a) elősegíti az NFK mint adatkezelő és adatfeldolgozónál a személyes adatok kezelésére vonatkozó jogi előírások teljesítését és az érintettek jogainak érvényesülését,
b) ellátja a GDPR 37. cikke alapján a hivatali szervezet vezetőjének felelősségi körébe tartozó adatvédelmi tisztviselő tevékenységet, tájékoztatást és szakmai tanácsot nyújt az NFK adatkezeléseiben résztvevők részére,
c) koordinálja a személyes adatok megfelelő védelmi szintjének kialakítására, fenntartására vonatkozó irányelvek, belső szabályozók, nyilvántartás, valamint adattérkép kidolgozását, véleményezi a tervezett adatkezelési műveleteket és kapcsolódó szerződéseket,
d) figyelemmel kíséri és ellenőrzi a személyes adatok kezelésére vonatkozó jogi előírásoknak és belső szabályoknak való megfelelést, részt vesz az adatkezelést érintő döntések meghozatalában, az érintettek joggyakorlásának biztosításában,
e) szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, nyomon követi a hatásvizsgálat elvégzését,
f) együttműködik az adatkezelés jogszerűségével kapcsolatos eljárások lefolytatására jogosult szervekkel és személyekkel,

g) javaslatot tesz a belső adatvédelmi és adatbiztonsági szabályzat tartalmára a Jogi Főosztálynak,
h) kezdeményezi a hivatali szervezet vezetőjénél a személyes adatok kezelésével összefüggő bejelentések és adatvédelemmel összefüggő incidensek kivizsgálását, megválaszolását és a Hatóság felé történő bejelentését, amely felé kapcsolattartó pontként működik, egyidejűleg elősegíti az érintettet megillető jogok gyakorlását,
i) közreműködik az adatvédelmi incidensek kivizsgálásában, vezeti az NFK adatvédelmi incidens nyilvántartását, és a vizsgálat eredménye alapján a jogszabályi feltételek fennállása esetén bejelenti azt a Hatóság részére,
j) nyilvántartást vezet az érintettnek a személyes adatai kezelésével kapcsolatos hozzáférésre, helyesbítésre, törlésre, tiltakozásra, valamint korlátozásra vonatkozóan benyújtott és elutasított kérelméről, az elutasítás indokairól,
k) vezeti a személyes adat kezelésével összefüggő egyéb nyilvántartásokat,
l) részt vesz a Hatóság által szervezett képzéseken,
m) részt vesz az NFK képviseletében az adatvédelmi tisztviselők konferenciáján.
(5) Az adatvédelmi tisztviselő a GDPR-ban és az Infotv-ben rögzítetteken túl, kizárólag a következő feladatokat látja el:
a) az államtitkár által jóváhagyott ellenőrzési tervet készít, a tervben foglaltak szerint ellenőrzi az adatkezelő szervnél az adatvédelmi és adatbiztonsági követelmények megtartását, valamint
b) az adatkezeléssel kapcsolatos előírások megszegésének észlelése esetén az adatvédelmi tisztviselő felhív a jogszerű állapot haladéktalan helyreállítására, és a hiányosságokat - amennyiben emiatt adatvédelmi érdek sérelmet szenvedne, úgy közvetlenül - jelzi az államtitkárnak, indokolt esetben kezdeményezi a felelősség megállapításához szükséges eljárás lefolytatását.
7. § (1) Az NFK szervezeti egységei és munkatársai kötelesek együttműködni az adatvédelmi tisztviselővel.
(2) Az NFK munkatársai a személyes adatai kezeléséhez és jogai gyakorlásához kapcsolódó valamennyi kérdésben a hivatali út betartása nélkül, közvetlenül fordulhatnak az adatvédelmi tisztviselőhöz.

6. A személyes adatok kezelésére vonatkozó elvek

8. § Az NFK a személyes adatok kezelése során az alábbi elveket alkalmazza:
1. Jogszerűség, tisztességes eljárás és átláthatóság elve: a személyes adatok kezelésére csak és kizárólag a megfelelő jogalap megléte esetén kerülhet sor. Az adatkezelésre vonatkozó jogszabályok betartásán túl, az NFK az adatkezelés során tiszteletben tartja az érintettek személyes adataikhoz fűződő jogát és az emberi méltóságát. Az NFK az adatkezelést átláthatóan végzi, az adatkezelésről hatékony és teljes körű tájékoztatást nyújt az érintettek részére.
2. Célhoz kötöttség elve: az NFK kizárólag előre meghatározott, jogszerű célból kezel adatokat, a céllal, célokkal összeegyeztethető módon.
3. Adattakarékosság elve: az NFK kizárólag annyi és olyan személyes adatot kezel, amely a meghatározott cél teljesüléséhez szükséges, és az adatkezeléskor meghatározott cél

megvalósulását követően - kivéve, ha jogszabály ezzel ellentétesen rendelkezik, vagy az adattárolás olyan adatkezelési cél elérése érdekében lehetséges, amely összeegyeztethető az eredeti adatkezelési céllal - a személyes adatokat töröli.

4. Pontosság elve: az NFK az általa kezelt személyes adatok pontosságát az adatbirtokos folyamatos felülvizsgálata és az érintett helyesbítéséhez való joga gyakorlásának biztosításával garantálja.

5. Korlátozott tárolhatóság elve: az NFK a személyes adatot tartalmazó dokumentumot az adatkezelési cél elérését vagy az adatkezelési idő leteltét követően - kivéve, ha jogszabály ezzel ellentétesen rendelkezik, vagy az adattárolás olyan adatkezelési cél elérése érdekében lehetséges, amely összeegyeztethető az eredeti adatkezelési céllal - törli vagy anonimizálja, amely révén az érintett a továbbiakban nem azonosítható.

6. Integritás és bizalmas jelleg elve: az NFK biztosítja a jogosultak számára, hogy az adatokhoz hozzáférjenek, továbbá az adatbiztonságért felelős önálló szervezeti egység felügyeletével gondoskodik a személyes adatok védelméről.

7. Elszámoltathatóság elve: az NFK valamennyi személyes adat kezelésével összefüggő tevékenységét visszakövethető módon dokumentálja, és ezáltal biztosítja az adatkezeléssel kapcsolatosan megtett intézkedések átláthatóságát.

7. Az érintett jogai és az érintett jogainak érvényesítésével összefüggő feladatok

9. § Az érintettnek joga van írásban tájékoztatást kérni az NFK által kezelt személyes adatai vonatkozásában

a) a személyes adatok köréről,

b) az adatkezelés jogalapjáról,

c) az adatkezelés céljáról,

d) a címzettek vagy címzettek kategóriáiról, akikkel, illetve amelyekkel a személyes adatokat közölték vagy közölni fogják,

e) az adattárolás időtartamáról, valamint

f) az adatok forrására vonatkozó minden elérhető információról, ha az adat nem az érintettől származik.

10. § Az érintett az államtitkárhoz, vagy az adatvédelmi tisztviselőhöz címzett kérelemben írásban kérheti, hogy

a) az NFK helyesbítse, illetve kiegészítse valamely kezelt személyes adatát,

b) az NFK korlátozza vagy törölje személyes adatait, valamint

c) a rá vonatkozó, általa az adatkezelő szerv rendelkezésére bocsátott, bármilyen formában rögzített személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja.

11. § Az NFK a 9. és 10. §-ban foglalt kérelemnek az adatvédelmi tisztviselő útján - a GDPR 12. cikk (3) és (4) bekezdésének figyelembevételével - indokolatlan késedelem nélkül, de legfeljebb egy hónapon belül eleget tesz.

12. § Az érintettet megillető jogok kizárólag akkor gyakorolhatók - az érintettek adatainak védelmét szolgáló adatbiztonsági követelményeket szem előtt tartva -, ha a kérelmező megfelelő azonosítása, illetve kérelme tartalmának hitelesítése megtörtént. Nem biztosítható ezen jogok gyakorlása különösen az elektronikus aláírással nem hitelesített vagy a kérelmező

személyének azonosítását nem biztosító elektronikus levél, valamint telefax útján érkezett kérelmek esetén. Elektronikusan benyújtott kérelem esetén a megfelelő azonosítás a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól szóló 2023. évi CIII. törvény 34. §-a szerint valósul meg.

13. § Az NFK az érintett részére nyújtandó bármely értesítést és tájékoztatást könnyen hozzáférhető és olvasható formában, lényegre törő, világos és közérthetően megfogalmazott tartalommal teljesíti. Az NFK az információt írásban, elektronikus úton, illetve az érintett kérelmére szóban is megadhatja, amennyiben az érintett személyazonossága igazolt. A szóbeli információátadásról azonnali feljegyzést kell készíteni, amelyet elektronikus úton az adatvédelmi tisztviselő részére meg kell küldenie a szervezeti egységnek jelszóval védetten.

14. § (1) Az érintett hozzáférési jogának gyakorlása során a tájékoztatást és az adatról kért első másolatot díjmentesen kell biztosítani, kivéve, ha az érintett kérelme - annak ismétlődő jellege vagy jogszabály alapján, illetve a Hatóság joggyakorlata értelmében - túlzó. Ez esetben - eltérő jogszabályi rendelkezés hiányában - az NFK a tájékoztatás és adatszolgáltatás teljesítéséért a számviteli politikai önköltségszámítási szabályzatában meghatározottaknak megfelelő költségtérítést állapíthat meg.

(2) Az érintett hozzáférési jogának gyakorlása során megküldött tájékoztatókról és adatokról az önálló szervezeti egység tárgyévre vonatkozóan, az 1. melléklet szerinti tartalommal anonim nyilvántartást vezet.

(3) A (2) bekezdés szerinti nyilvántartást az önálló szervezeti egység tárgyévet követő év január 31. napjáig megküldi az adatvédelmi tisztviselőnek.

8. Az adatkezelési tevékenységek nyilvántartása

15. § (1) A 2. melléklet szerinti adatkezelési tevékenységek nyilvántartását és az adatkezelői nyilvántartást az adatvédelmi tisztviselő vezeti.

(2) Az adatkezelési tevékenységek nyilvántartásába az adatbirtokos az adatvédelmi tisztviselő által meghatározott módon és formában szolgáltat adatokat a 3. melléklet szerinti táblázat kitöltésével.

(3) Az adatkezelési tevékenységek nyilvántartásába az adatkezelő szervezeti egység vezetője a következő adatokat küldi meg az adatvedelem@nfk.gov.hu e-mail-címre:

a) az előkészített, megváltozott és megszűnt adatkezelések esetén a 3. melléklet szerinti adatokat,

b) hatásvizsgálat elvégzése esetén a 11. alcím szerinti adatokat, valamint

c) a jogszabályi rendelkezés alapján adatvédelmi hatásvizsgálattal kötelezően vizsgálandó adatkezelési tevékenységek 4. melléklet szerinti hatásvizsgálatát, ha az adatkezelő az NFK.

(4) Az adatvédelmi tisztviselő az adatvédelmi hatásvizsgálatról szóló összefoglaló jelentés alapján az adatkezelést bevezeti a 2. melléklet szerinti adatkezelési tevékenységek nyilvántartásába.

9. Az adattovábbítás és az adattovábbítási nyilvántartás

16. § Az NFK önálló szervezeti egysége az adattovábbítás feltételeinek meglétét minden egyes személyes adattal összefüggésben köteles ellenőrizni, így különösen azt, hogy az igényelt adatokra vonatkozóan az adatok kezelőjének minősül-e.

17. § Adatvédelmi szempontból az adattovábbítás jogszerű, ha

a) a személyes adatot kezelő szerv vagy személy jogosult annak továbbítására,

b) az adattovábbítás címzettje (adatkérő) pedig rendelkezik az adat kezeléséhez szükséges jogalappal vagy az érintett írásos - a vonatkozó jogszabályi elvárásoknak megfelelő tartalmú - hozzájárulásával, és

c) az adatkérés célja mindezzel összhangban van.

18. § (1) Harmadik személy vagy szerv által benyújtott adattovábbítási kérelem elbírálása - törvényben kötelezően előírt adattovábbítás esetét kivéve - az NFK hivatali szervezete vezetőjének vagy az általa kijelölt vezetőnek a hatáskörébe tartozik, amellyel kapcsolatban kikérheti az adatvédelmi tisztviselő véleményét.

(2) Az adattovábbítás abban az esetben teljesíthető, ha tartalmazza:

a) az adattovábbítási igény célját,

b) az adattovábbítási igény jogalapját,

c) a kért adatok körének pontos meghatározását, valamint

d) az érintett személy azonosításához szükséges adatokat, több személyre vonatkozó adatigénylés esetén az érintettek azonosításához szükséges csoportképző ismérveket.

(3) Az adattovábbítás történhet kérelem alapján egyedi adatszolgáltatással, továbbá - törvény ilyen tartalmú rendelkezése vagy erre vonatkozó megállapodás alapján - közvetlen hozzáférés biztosításával.

19. § (1) Ha olyan adat továbbítására kerül sor, amellyel kapcsolatban az adattovábbítást végző szervezeti egység - a GDPR vagy Infotv. által biztosított jogait érintő - adatkezelési korlátozást jelzett, az adatkezelési korlátozást szerepeltetni kell az 5. melléklet szerinti adattovábbítási nyilvántartásban.

(2) Papíralapú adattovábbítási nyilvántartást kell vezetni manuális adatkezelések esetén olyan elektronikus információs rendszerek esetében, ahol a folyamatos és zárt rendszerben történő naplózás nem biztosított. A papíralapú adattovábbítási nyilvántartás tartalmazza

a) az adatkezelés célját,

b) az érintett adatokat,

c) az adatkezelést folytató személy azonosítását lehetővé tevő adatokat, és

d) az elvégzett adatkezelési műveleteket.

10. Az adatvédelmi hatásvizsgálat lefolytatása és az előzetes konzultáció kezdeményezése

20. § (1) Az adatbirtokos előzetes hatásvizsgálatot végez - a 4. mellékletben foglaltak szerint - a tervezett vagy folyamatban lévő adatkezelésnél,

a) ha 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,

b) az adatkezelés kockázatának megváltoztatása esetén, vagy
c) lényeges körülmény - különösen az adatkezelés technológiájának - megváltoztatása esetén.
(2) Az adatbirtokos köteles az előkészített adatkezelés esetén a 2. melléklet szerinti adatkezelési tevékenységek nyilvántartásáról szóló dokumentumot, és a 9. és a 10. melléklet szerinti adatbiztonsági és a felelősségi körökre vonatkozó adatlapot kitölteni, és azt az adatvédelmi tisztviselőnek megküldeni. Az adatvédelmi tisztviselő a megküldött dokumentumokat az adatkezelési tevékenységek nyilvántartásába bejegyezi.

21. § (1) Az adatbirtokos a kockázatelemzési feladata kapcsán, a 4. mellékletben foglalt kérdések megválaszolása előtt
a) köteles kikérni
aa) a döntés végrehajtásáért felelős szakterület véleményét,
ab) az elektronikus információs rendszer biztonságáért felelős önálló szervezeti egység vezetője vagy az elektronikus biztonságért felelős személy véleményét,
ac) a rendszerek üzemeltetésében részt vevő szervezetek véleményét, valamint
ad) az adatvédelmi tisztviselő véleményét,
b) kikérheti a tervezett, illetve megváltozott adatkezelés által érintett személyek véleményét.
(2) Az adatbirtokos írásban rögzíti annak tényét, ha
a) - az adatkezeléssel várhatóan érintett személyek jogaira és szabadságaira nézve - valószínűsíthetően magas kockázatot nem azonosít a tervezett adatkezelés annak körülményeire, így különösen céljára, az érintettek körére, az adatkezelési műveletek során alkalmazott technológiára tekintettel, vagy
b) megállapítást nyer, hogy az adatkezelés az adatvédelmi hatásvizsgálat lefolytatása alóli mentesítést tartalmazó valamely jogszabályban meghatározott kivételi körbe tartozik.
22. § (1) Az adatbirtokos - a döntése alapjául szolgáló legfontosabb szempontokat írásban megjelölve - adatvédelmi hatásvizsgálat lefolytatását kezdeményezi az államtitkárnál,
a) ha a kockázatelemzés során a 20. § (1) bekezdés a) pontja szerinti magas kockázatot valószínűsít, vagy
b) jogszabályi rendelkezés alapján adatvédelmi hatásvizsgálattal kötelezően vizsgálandó adatkezelési tevékenység esetén.
(2) Az államtitkár az adatbirtokos javaslatára elrendeli az adatvédelmi hatásvizsgálat lefolytatását vagy írásban rögzíti mellőzésének okait, és az adatvédelmi tisztviselő kapcsolódó álláspontját. Az adatvédelmi hatásvizsgálat lefolytatásáig, vagy az annak elmaradásával kapcsolatos okok írásban történő rögzítéséig az adatkezelésről szóló döntés nem hozható meg.
(3) Az adatvédelmi hatásvizsgálat lefolytatásában az adatkezelés által érintett személyek vesznek részt. Az adatvédelmi hatásvizsgálat lefolytatását az adatvédelmi tisztviselő támogatja.
(4) Az adatvédelmi hatásvizsgálat során keletkezett iratok az adatkezelő szerv döntését előkészítő adatokat tartalmaznak, ezért azokon „Nem nyilvános!" jelzést kell elhelyezni. Ha a hatásvizsgálat során kezelt adatok egy részének esetében azok minősítésére vonatkozó jogszabályi feltételek fennállnak, akkor az adatkezelő szerv vezetője dönt a szükséges iratok minősítéssel történő védelméről és annak szintjéről. Az adatbirtokos az adatvédelmi hatásvizsgálat eredményeiről minősített adatot nem tartalmazó, „Nem nyilvános!" jelzéssel ellátott összefoglaló jelentést készít.
(5) Az adatvédelmi hatásvizsgálatról szóló összefoglaló jelentést az államtitkár hagyja jóvá.

(6) Ha az adatvédelmi hatásvizsgálat arra az eredményre jut, hogy a tervezett adatkezelés jelentette kockázat nem mérsékelhető a rendelkezésre álló technológiák és a végrehajtási költségek szempontjából észszerű módon - vagy ha azt jogszabály kötelezően előírja -, akkor az adatkezelő szerv előzetes konzultációt kezdeményez a Hatóságnál.

11. Az adatvédelmi incidens észlelése és az adatvédelmi incidens kezelése

23. § (1) Az NFK adatkezelése során és az adatfeldolgozónál bekövetkezett adatvédelmi incidenst észlelő személynek a tájékoztatást haladéktalanul az adatvédelmi tisztviselőhöz és az informatikai rendszerek informatikai biztonságáért felelős szervezeti egység vezetőjéhez kell megtenni. A tájékoztatásnak a 6. melléklet szerinti adatokat kell tartalmaznia.
(2) Az NFK-hoz külső észlelő személytől származó, az NFK adatkezelésére vagy az adatfeldolgozóra vonatkozó adatvédelmi incidens gyanújának tárgyában érkezett tájékoztatást haladéktalanul továbbítani kell az adatvédelmi tisztviselőnek és az informatikai rendszerek informatikai biztonságáért felelős szervezeti egység vezetőjének.
(3) Ha az NFK ellenőrzésre jogosult munkatársa vagy szervezeti egysége a feladata ellátása során adatvédelmi incidens bekövetkezését feltételezi, haladéktalanul értesíti az adatvédelmi tisztviselőt és az informatikai rendszerek informatikai biztonságáért felelős szervezeti egység vezetőjét.
(4) Az adatvédelmi tisztviselő és az informatikai rendszerek informatikai biztonságáért felelős szervezeti egység vezetője megvizsgálja, hogy
a) a tájékoztatás alapján fennáll-e az adatvédelmi incidens,
b) az adatvédelmi incidens az informatikai rendszert érintően következett-e be, valamint
c) mely szervezeti egységeket kell bevonni, illetve szükséges-e közös intézkedések megtétele.
(5) Adatvédelmi incidens különösen:
a) a személyes adatokat tároló informatikai rendszerhez vagy szoftverhez történő jogosulatlan hozzáférés,
b) a személyes adatok jogosulatlan titkosítása, amelynek következtében a személyes adatokhoz - akár átmenetileg - nem lehet hozzáférni, vagy az NFK által végzett adatkezelések során felhasználni,
c) az NFK munkatársának jogosulatlan vagy a jogosultsági szintjét meghaladó hozzáférése a személyes adatokhoz, vagy a munkatárs által jogosulatlanul végrehajtott adatkezelési művelet,
d) személyes adatok vétlen vagy szándékos, felhatalmazás nélküli nyilvánosságra hozatala,
e) személyes adatokat tartalmazó dokumentum más számára történő hozzáférhetővé tétele,
f) személyes adatokat tartalmazó postai küldemény téves címzetthez 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, amelynek következtében a személyes adatokhoz - akár átmenetileg - nem lehet hozzáférni vagy felhasználni.
(6) Az adatvédelmi tisztviselő és az informatikai rendszerek informatikai biztonságáért felelős szervezeti egység vezetője - amennyiben az incidens megállapítható - a döntés előkészítésére

szolgáló anyagot megküldi az adatbirtokos számára. Ha az adatbirtokos nem állapítható meg, akkor az üzemeltetést végző szervezet az incidenskezelési eljárásnak megfelelően jár el.
(7) Ha nem állapítható meg adatvédelmi incidens, de egyéb incidens bekövetkezése igen, akkor a feladat- és hatáskört figyelembe véve kerül sor a további eljárás lefolytatására.
(8) Az adatbirtokos vizsgálja a feladat- és hatáskörébe tartozó, nem informatikai rendszert érintő adatvédelmi incidens gyanújával érintett tájékoztatásokat.

24. § (1) Ha az adatvédelmi incidens a rendelkezésre álló adatok alapján egyértelműen megállapítható, az adatbirtokos a 6. melléklet szerint bejelentett adatokat megküldi az adatvédelmi tisztviselőnek, aki a tudomásszerzést követő 72 órán belül intézkedik - munkacsoport bevonásával - az erre rendszeresített elektronikus felületen a hatósági nyilvántartásba való bejelentésről.
(2) Ha a rendelkezésre álló adatok alapján az adatbirtokos egyértelműen nem tudja megállapítani az adatvédelmi incidens bekövetkezését, de feltételezhető, hogy az esemény magas kockázattal járt, az adatvédelmi tisztviselő és az informatikai rendszerek informatikai biztonságáért felelős szervezeti egység vezetőjének közös álláspontját kéri az ügyben.
(3) A vizsgálat az adatvédelmi tisztviselő véleményének, szakértői tanácsának kikérésével és annak figyelembevételével történik.
(4) Az adatvédelmi tisztviselő és az informatikai rendszerek informatikai biztonságáért felelős szervezeti egység vezetője a tájékoztatást megvizsgálja, a tájékoztatótól, valamint az adatfeldolgozótól szükség esetén további adatszolgáltatást kér, amelyet az érintettek kötelesek haladéktalanul teljesíteni.
(5) Az adatvédelmi tisztviselő és az informatikai rendszerek informatikai biztonságáért felelős szervezeti egység vezetője gondoskodik az elsődleges intézkedések megtételéről. Ha a vizsgálat során az adatvédelmi tisztviselő és az informatikai rendszerek informatikai biztonságáért felelős szervezeti egység vezetője megállapítja az érintettek jogaival és szabadságaival kapcsolatban a magas kockázat fennállását, akkor a 7. melléklet szerinti adatokat az adatvédelmi tisztviselő a munkacsoport közreműködésével a Hatóság részére a tudomásszerzést követő 72 órán belül megküldi az erre rendszeresített elektronikus felület igénybevételével.
(6) Az adatvédelmi incidens bekövetkezése esetén a munkacsoport döntése alapján az adatvédelmi tisztviselő tájékoztatja a 8. mellékletben meghatározott adatokról az incidenssel érintetteket.
(7) Az adatvédelmi tisztviselő az adatbirtokos által megküldött 6. melléklet szerinti adatvédelmi incidenst bevezeti az NFK adatvédelmi incidens nyilvántartásába.

12. Az adatfeldolgozás

25. § (1) Az NFK - adatkezelési tevékenységével összefüggésben - adatfeldolgozót vehet igénybe. Az adatfeldolgozó az adatkezelési műveletekhez kapcsolódó technikai feladatokat végzi, és e minőségében gyakorolja az adatkezelő NFK által átruházott jogosultságokat, teljesíti kötelezettségeit, és vezeti a 3. melléklet szerinti adatfeldolgozói nyilvántartást.
(2) Az adatfeldolgozásra vonatkozó megállapodást írásba kell foglalni. Amennyiben az adatfeldolgozóként igénybe venni kívánt szervre vagy személyre az utasítás hatálya nem

terjed ki, akkor a megállapodásban kell érvényesíteni az adatfeldolgozóval szemben e címben foglalt előírásokat.
(3) Adatfeldolgozó igénybevétele esetén az adatkezelés céljának meghatározására, az adatkezelésre vonatkozó érdemi döntések meghozatalára az adatkezelő jogosult.
(4) Az adatfeldolgozó a tevékenységi körén belül, illetve az adatkezelő által meghatározott keretek között felelős a személyes adatok feldolgozásáért, megváltoztatásáért, törléséért, továbbításáért és nyilvánosságra hozataláért, továbbá minden olyan jogsértésért, amit az adatkezelő utasításának vagy az adatfeldolgozással összefüggésben kötött megbízási szerződésben foglaltak megszegésével okozott.
(5) Az adatfeldolgozó köteles a 3. melléklet szerinti 1. Adatfeldolgozók nyilvántartása, valamint az 2. Adatfeldolgozói tevékenységek nyilvántartásának a vezetésére.

13. Adatbiztonsági előírások

26. § (1) Az adatkezelő szerv, illetve tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról.
(2) Az elektronikusan kezelt adatállományok tekintetében biztosítani kell, hogy a különböző nyilvántartásokban tárolt adatok - törvény eltérő rendelkezése hiányában - közvetlenül ne legyenek összekapcsolhatóak.
(3) A személyes adatokat kezelő nyilvántartások adatbiztonsági felmérése során az adatkezelő szerv, illetve tevékenységi körében az adatfeldolgozó az adatkezelések tekintetében a 9. melléklet szerinti adatbiztonsági adatlapot vesz fel.
27. § Az informatikai adatbiztonsági előírások részletes meghatározását külön szabályzat tartalmazza.

14. Záró rendelkezések

28. § Az önálló szervezeti egységek vezetői, a feladatkörükben a szabályzat hatálybalépését megelőzően elkészített adatfeldolgozói szerződésekről a jelen utasítás hatálybalépését követő 15 napon belül tájékoztatják az adatvédelmi tisztviselőt.
29. § Az önálló szervezeti egységek vezetői a jelen utasítás hatálybalépését követő 15 napon belül kijelölik a szervezeti egység azon munkatársát, akinek feladatát képezi az adatvédelmi tisztviselővel történő kapcsolattartás. Az igények intézésére több személy kijelölése is lehetséges.
30. § Ez az államtitkári rendelkezés az aláírását követő napon lép hatályba.

Budapest, 2025. április „17.”

Nemzeti Fejlesztési Központ Európai Uniós Fejlesztésekért Felelős Államtitkár

dr. Ágostházy Szabolcs Imre

1. melléklet

Adatlap a szervezeti egységek részére az érintett hozzáférési jogának gyakorlására vonatkozó anonim nyilvántartáshoz

A kitöltő szervezeti egység:		
Az érintett saját adataira vonatkozó kérelmek:		
A kérelem jellege:		
Teljesített	Részben teljesített	Elutasított
Tájékoztatás iránti kérelem saját nyilvántartott személyes adatról		
Tájékoztatás iránti kérelem arról, hogy az érintett személyes adatát kinek továbbították		
Helyesbítés iránti kérelem		
Törlés iránti kérelem		
Az érintett személyes adatára vonatkozó részben teljesített, illetve elutasított kérelmek indokolása:		

2. melléklet

Adatkezelési tevékenységek nyilvántartása

1. Gyakorlati útmutató az adatkezelési tevékenységek nyilvántartásához

1. Az adatkezelés megnevezése: a nyilvántartásban történő keresés lehetővé tétele céljából röviden kell megnevezni. A nyilvántartásnak az adatkezelést létrehozó törvény által meghatározott elnevezését kell megjelölni, amennyiben azonban rendelkezik egy általánosan használt fantázianévvel, akkor ezt az elnevezést is fel kell tüntetni. Az azonos adattartalommal rendelkező adatkezeléseket egységes elnevezéssel kell szerepeltetni.
2. Az adatkezelő nevét, címét, székhelyét, telefonszámát, e-mail-címét kell beírni.
3. Csak akkor kell kitölteni, ha van közös adatkezelő, illetve van az adatkezelőnek képviselője.
4. Értelemszerűen kitöltendő.
5. Az adatkezelés céljának rövid megfogalmazása.
6. Hozzájárulás vagy GDPR 6. cikk (1) bekezdésében foglalt jogalapok valamelyike.
Pontosan meg kell jelölni a fentieken kívül azt is, hogy milyen jogszabály (jogszabályhelyet is kérjük feltüntetni) által meghatározott feladat teljesítése érdekében van erre szükség. Ilyen esetben a feladatmeghatározást tartalmazó ágazati jogszabály megfelelő hivatkozási alapnak tekinthető.
7. Az érintettek kategóriái lehetnek: azon csoportok, amelyek tagjainak személyes adataival a Nemzeti Fejlesztési Központ adatkezelést végez. (Pl. az adatkezeléssel érintett személyek / nagykorú állampolgárok / gyermekek, egyéni vállalkozók, gépjármű üzemben tartói stb.)
8. Például: személyes adat, különleges adat, bűnügyi személyes adat, nemzeti adatvagyon, minősített adat.
9. Címzettek: akikkel a személyes adatot közölték vagy közölni fogják, ideértve a harmadik országbeli címzetteket vagy nemzetközi szervezeteket.
10. Harmadik ország: minden olyan ország, ami nem EU- és EGT-tag.
11. Ha jogszabály másképp nem rendelkezik, az adatokat az adatkezelés céljának elérésével, illetve az érintett kérésére törölni kell.
12. A kezelt adatok forrásának megjelölése (pl. érintett hozzájárulása, más adatkezelőtől adatátvétel).
Más adatkezelőtől történő adatátvétel esetén az adatokat továbbító adatkezelő adatvédelmi nyilvántartási számát is meg kell jelölni.
13. Lásd GDPR 32. cikk (1) bekezdése.
14. Ha az adatkezelés a Hatóság részére már bejelentésre került.

2. Adatkezelési tevékenységek nyilvántartása

2. Adatkezelési tevékenységek nyilvántartása	
1. Az adatkezelés megnevezése:	
2. Az adatkezelő szerv neve és elérhetősége:	
3. A közös adatkezelő és az adatkezelő szervezeti egység megnevezése	
4. Az adatvédelmi tisztviselő neve és elérhetősége:	
5. Az adatkezelés célja:	
6. Az adatkezelés jogalapja:	
7. Az érintett személyek köre:	
8. A személyes adatok kategóriái:	
9. A címzettek kategóriái:	
10. Harmadik országba történő adattovábbítás - harmadik ország vagy nemzetközi szervezet megnevezése:	
11. Az adatkategóriák törlési határideje:	
12. Az adatok forrása:	
13. Az adatbiztonsággal összefüggő szervezeti és technikai intézkedések általános leírása:	
14. Hatóság száma:	
15. Adatkezelési tájékoztató van-e? (Ha hozzájárulás a jogalap, feltétlenül szükséges készíteni.)	Lehetséges válaszok: 1. Nincs rá szükség, mert jogszabályi tájékoztatás van. 2. Nincs, azonban feltétlenül szükséges lenne. (Indoklás) 3. Igen, van.
16. Elsődleges adattárolási hely: (ideértve az adatbiztonsági kockázatokat, javaslatokat is, ha vannak)	
17. Vannak-e együtt tárolt adatok?	Igen/Nem.
18. A célhoz kötöttség elve érvényesül-e? (Indoklással, szükség esetén javaslattal!)	1. Igen, az 5. pontnak megfelelően. 2. Nem vagy csak részben. (Nem válasz esetén indoklás, javaslat szükséges.)
19. Az adattakarékosság elve érvényesül-e? (Indoklással, szükség esetén javaslattal!)	1. Igen, a személyes adatok az adatkezelés céljának megfelelnek, relevánsak és szükségesek.

	2. Nem. (Nem válasz esetén indoklás, javaslat szükséges.)
20. A pontosság elve érvényesül-e? (Indoklással, szükség esetén javaslattal!)	1. Igen, a személyes adatok pontosak, naprakészek. 2. Nem. (Nem válasz esetén indoklás, javaslat szükséges.)
21. A korlátozott tárolhatóság elve érvényesül-e? (Indoklással, szükség esetén javaslattal!)	1. Igen, a személyes adatok kezelésére csak a cél eléréséhez szükséges ideig kerül sor, amelyet jogszabály állapít meg. 2. Igen, a személyes adatok kezelésére csak a cél eléréséhez szükséges ideig kerül sor, amelyet az adatkezelő határoz meg. (Hozzájárulás esetén.) 3. A személyes adatok kezelésére közérdekű archiválás, tudományos és történelmi kutatás vagy statisztikai célból az eredeti adatkezelési céltól eltérő ideig kerül sor. (Az első kettővel is alkalmazható.) 4. Nem. (Nem válasz esetén indoklás, javaslat szükséges.)
22. Az adatbiztonság elve érvényesül-e? (Indoklással, szükség esetén javaslattal!)	1. Igen, a személyes adatok megfelelő biztonsága biztosított. 2. Nem. (Nem válasz esetén indoklás, javaslat szükséges.)
23. A tájékoztatás megfelelő-e, tartalmazza-e valamennyi kötelező elemet? (Indoklással, szükség esetén javaslattal!)	1. A tájékoztatás a törvényi előírásnak megfelelő. 2. Az adatkezelés hozzájáruláson alapul. A tájékoztatás megfelelő. 3. Az adatkezelés nem az érintett hozzájárulásán alapul. A tájékoztatás megfelelő. 4. Az adatkezelés..... alapul, tájékoztatás nincs/nem megfelelő. (Nem válasz esetén indoklás, javaslat szükséges.)
24. A törlés, elfeledtetés joga gyakorolható-e? (Indoklással, szükség esetén javaslattal!)	Ezek a jogok nem gyakorolhatóak, ha a jogalap jogi kötelezettség teljesítése, vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlása keretében végzett feladat végrehajtása. 1. Igen, gyakorolható. 2. Nem. (Nem válasz esetén indoklás, javaslat szükséges.)
25. A korlátozás joga gyakorolható-e? (Indoklással, szükség esetén javaslattal!)	Az érintett ezzel a jogával a kötelező és a hozzájáruláson alapuló adatkezelések esetében is élhet. A kötelező esetben csak akkor, ha az adatok pontosságát vitatja, a GDPR-ban szereplő felsorolás többi pontja szerint nem. 1. Igen. 2. Igen, de mivel az adatkezelés jogalapja jogszabályon alapul,

	csak az adatok pontosságát vitathatja. 3. Nem. (Nem válasz esetén indoklás, javaslat szükséges.)
26. Az adathordozhatóság joga gyakorolható-e? (Indoklással, szükség esetén javaslattal!)	Csak a hozzájáruláson vagy szerződésen alapuló adatkezelések esetén alkalmazható. További feltétel, hogy az adatkezelés automatizált módon történjen. Nem alkalmazható a közérdekű és a közhatalmi feladatok keretében végzett adatkezeléseknél! 1. Igen. 2. Nem. (Nem válasz esetén indoklás, javaslat szükséges.)
27. A tiltakozás joga gyakorolható-e? (Indoklással, szükség esetén javaslattal!)	Az érintett csak kivételes esetben, a közérdekű és a közhatalmi feladatok keretében végzett adatkezelések, és a jogos érdeken alapuló adatkezelések esetén élhet ezzel a joggal. [GDPR 6. cikk (1) e) és f) pont] 1. Igen, mert a jogalap .....! 2. Nem. (Nem válasz esetén indoklás, javaslat szükséges.)
28. Van-e adatfeldolgozási megállapodás az adatfeldolgozóval?	

3. Az adatkezelői nyilvántartás

2. Az adatkezelői nyilvántartás **Szervezeti egység megnevezése:**	
Adatkezelő neve és elérhetősége, valamint az adatkezelő képviselőjének a neve és elérhetősége;	
Adatvédelmi tisztviselő neve és elérhetősége	
Adatkezelés megnevezése /a tevékenység, amely során adatkezelés történik/	
Az adatkezelés célja	
Adatkezelési művelet jogalapja	
Érintettek köre	
Kezelt személyes adatok kategóriái	
Személyes adatok különleges kategóriái (Infotv. 3. §), vagy a GDPR 10. cikke szerinti bűnügyi adatok kategóriái	
A tevékenység folyamata során a személyes adatokat tartalmazó dokumentumokat megismerő személyek	
Személyes adatok továbbítása esetén az adattovábbítás címzettjei (ideértve a harmadik országbeli címzetteket és nemzetközi szervezeteket is)	
Adatkezelés technikai jellemzője	
Tárolás időtartama, törlési határidő	
Adatbiztonsági intézkedés /technikai, szervezési intézkedések, vonatkozó normatív utasítások megjelölése/	
Adatfeldolgozó igénybevétele esetén neve, elérhetősége	

3. melléklet
Adatszolgáltatási táblázat az adatkezelési tevékenységek nyilvántartásába

1. Adatfeldolgozókról vezetett nyilvántartás

1. Adatfeldolgozó neve, elérhetőségei, képviseletre jogosult neve, és adatvédelmi tisztviselőjének a neve és elérhetőségeik.
2. Megbízó adatai:
3. Adatfeldolgozó neve, címe, telefonszáma, e-mail címe, adatvédelmi tisztviselő elérhetősége:
4. Adatfeldolgozás célja: GDPR. 31. cikk (1) bekezdés b) pont
5. Az adatkezelő nevében végzett adatfeldolgozási tevékenységek kategóriái pl.: gyűjtés, rögzítés, rendszerezés, tárolás, lekérdezés, betekintés, felhasználás, továbbítás, korlátozás, törlés, megsemmisítés, stb.

Gyűjtés	
Rögzítés	
Rendszerezés	
Tárolás	
Lekérdezés	
Betekintés	
Felhasználás	
Továbbítás	
Korlátozás	
Törlés	
Megsemmisítés	
Egyéb:	

6. Amennyiben al-adatfeldolgozót vesz igénybe annak a neve, az általa végzett rész -feladat, elérhetőségei, képviselőjének, valamint ha van adatvédelmi tisztviselőjének neve és elérhetőségei.
7. GDPR. 30. cikk (1) bekezdés d) pontja alapján a címzettek kategóriái, akikkel a személyes adatokat közlik.
8. Harmadik országba történő adattovábbítás vagy nemzetközi szervezet részére.
9. Az adatbiztonság vonatkozásában végrehajtott technikai, szervezési intézkedésekről történt leírások: Adatbiztonságnak a tesztelése, A tárolt adatok bizalmas jellegének a megőrzése, titkosítás és álnevesítés.

2. Adatfeldolgozói tevékenységek nyilvántartás

Adatfeldolgozói tevékenységek nyilvántartása	
1. Az adatkezelés megnevezése:	
2. Az adatfeldolgozó(k) szervezeti egység megnevezése és elérhetősége(i):	
3. Az adatkezelési tevékenységek kategóriái:	
4. Adatvédelmi tisztviselő neve és elérhetősége:	
5. Harmadik országba történő adattovábbítás - harmadik ország vagy nemzetközi szervezet megnevezése:	
6. Az adatbiztonsággal összefüggő szervezeti és technikai intézkedések általános leírása:	
7. Elsődleges adattárolási hely: (ideértve az adatbiztonsági kockázatokat, javaslatokat is, ha vannak)	
8. Vannak-e együtt tárolt adatok?	
9. A célhoz kötöttség elve érvényesül-e? (Indoklással, szükség esetén javaslattal!)	
10. Az adattakarékosság elve érvényesül-e? (Indoklással, szükség esetén javaslattal!)	
11. A pontosság elve érvényesül-e? (Indoklással, szükség esetén javaslattal!)	
12. A korlátozott tárolhatóság elve érvényesül-e? (Indoklással, szükség esetén javaslattal!)	
13. Az adatbiztonság elve érvényesül-e? (Indoklással, szükség esetén javaslattal!)	
14. A tájékoztatás megfelelő-e, tartalmazza-e valamennyi kötelező elemet? (Indoklással, szükség esetén javaslattal!)	
15. A törlés, elfeledtetés joga gyakorolható-e? (Indoklással, szükség esetén javaslattal!)	
16. A korlátozás joga gyakorolható-e? (Indoklással, szükség esetén javaslattal!)	
17. Az adathordozhatóság joga gyakorolható-e? (Indoklással, szükség esetén javaslattal!)	
18. A tiltakozás joga gyakorolható-e? (Indoklással, szükség esetén javaslattal!)	
19. Ha adatfeldolgozók vagyunk, van-e adatfeldolgozási megállapodás az adatkezelővel?	

4. melléklet

Előzetes kockázatelemzési kérdőív az adatkezelési tevékenységek hatásvizsgálatához

Első rész: Szükséges-e a hatásvizsgálat lefolytatása? Előzetes adatvédelmi kockázatelemzés

1. Használ vagy fejleszt-e olyan informatikai rendszert, amely személyes adatokat kezel?
Igen □ Nem □
2. Szükséges-e személyes adatokat gyűjteni a szolgáltatás működtetéséhez?
Igen □ Nem □
3. Megvalósul-e a korábbiaktól eltérő célú adatkezelés már meglévő személyes adatokkal kapcsolatban?
Igen □ Nem □
a) Alkalmaz új adatköröket gyűjtő technológiát, amely jelentős mértékben megváltoztatja az adatkezelést?
Igen □ Nem □
b) Ha releváns szervezeti változás következik be:
ba) az egyesülés, beolvadás vagy egyéb szervezeti átalakulás hatással van-e az adatbázisokra?
Igen □ Nem □
bb) ez a változás eredményezi új adatok kezelését vagy új nyilvánosságra hozatali eljárásokat?
Igen □ Nem □
c) Ha ez az információ már korábban be lett gyűjtve:
ca) érint-e új vagy nagy létszámú érintett csoportot?
Igen □ Nem □
cb) rögzít-e ezen felül további személyes adatot?
Igen □ Nem □
4. A szolgáltatás korlátozza-e az érintettek személyes adataikhoz való hozzáféréséhez fűződő jogait?
Igen □ Nem □
5. Tervezi-e egymást követő 12 hónapból álló időszak során nagyszámú érintettekre vonatkozó személyes adatainak kezelését?
Igen □ Nem □
6. Megvalósul-e különleges adatok, tartózkodási helyre utaló adatok, illetve gyermekekre vagy munkavállalókra vonatkozó, széleskörű nyilvántartási rendszerekben tárolt adatok kezelése?
Igen □ Nem □
7. Megvalósul-e profilalkotás, amelyre az érintett személy tekintetében joghatással bíró vagy az egyént hasonlóan jelentős mértékben érintő intézkedések épülnek?
Igen □ Nem □
8. Megvalósul-e egészségügyi ellátás nyújtására, járványügyi kutatásokra, mentális vagy fertőző betegségekre irányuló felmérésekre vonatkozó személyes adatok kezelése, amennyiben az adatok feldolgozására meghatározott egyénekre széles körben vonatkozó intézkedések vagy döntések meghozatala érdekében kerül sor?
Igen □ Nem □

9. Megvalósul-e nyilvánosság számára hozzáférhető területek (közterületek) nagyarányú, automatizált nyomon követése?
Igen □ Nem □
10. Megvalósul-e olyan adatkezelés, amely során a személyes adatok megsértése várhatóan hátrányosan érintené az érintett személyes adatainak, magánéletének, jogainak vagy jogos érdekeinek védelmét?
Igen □ Nem □
11. Az adatkezelő vagy adatfeldolgozó fő tevékenységei olyan eljárásokat foglalnak-e magukban, amelyek jellegüknél, alkalmazási területüknél, illetve céljaiknál fogva az érintettek rendszeres és rendszerszerű megfigyelését igénylik?
Igen □ Nem □
12. A személyes adatokat olyan jelentős számú személy számára teszi-e hozzáférhetővé, amely észszerűen elvárható módon nem korlátozható?
Igen □ Nem □
13. Létrejön-e új azonosító vagy hozzáférési jogosultságot ellenőrző rendszer, például biometrikus azonosítás?
Igen □ Nem □
14. Megfigyelés alatt állnak-e az érintettek helyváltoztatás, másokkal való kommunikáció vagy egyéb magatartás tanúsítása közben?
Igen □ Nem □
15. Megvalósul-e automatizált adatfeldolgozás?
Igen □ Nem □
16. Személyes adatok védelmének növelése érdekében előír-e (ha volt ilyen) a korábbinál magasabb szintű adatbiztonsági követelményeket?
Igen □ Nem □
17. Személyes adatokkal való visszaélés megelőzése érdekében bevezetésre kerülnek-e új vagy módosított előírások?
Igen □ Nem □
18. Személyes adatok tárolásával kapcsolatban bevezetésre kerülnek-e új vagy módosított előírások?
Igen □ Nem □
19. Megvalósul-e tudományos kutatási vagy statisztikai célból történő adatkezelés?
Igen □ Nem □
20. Az adatkezelés kiterjed-e különleges adatokra?
Igen □ Nem □
21. Megvalósul-e bármilyen más, magánszférát érintő magatartás?
Igen □ Nem □
22. Végeztek-e már korábban hatásvizsgálatot? Ha a válasz igen, csatolja a dokumentumot!
Igen □ Nem □

Második rész: Előzetes hatásvizsgálat

1. Ki a tájékoztatásra kötelezett személy (név, telefonszám, e-mail-cím)? (Ha van adatvédelmi tisztviselő, akkor az ő adatai.)
2. Mutassa be a szolgáltatás működését, felépítését!

3. Ki az adatkezelő (név, telefonszám, e-mail-cím, postai cím)?
4. Mi az adatkezelés pontos címe/helye/webhelye? (Csak akkor töltse ki, ha az eltér az adatkezelő címétől!)
5. Mi az adatkezelés célja, módja és jogalapja?
6. Mi az adatkezelés időtartama?
7. Kíván-e adatfeldolgozót igénybe venni? Ha igen, mutassa be részletesen az adatfeldolgozó személyét (kapcsolattartó, adatkezeléssel összefüggő tevékenység, adatfeldolgozó címe, adatfeldolgozás helye, technológiája stb.)!
8. Melyek a kezelni kívánt adatkörök?
9. Határozza meg a gyűjteni kívánt adatok mennyiségét, illetve az érintett személyek számát (hozzávetőlegesen)!
10. Melyek az adatfelvétel formái? Megvalósulhat az adatgyűjtés személy azonosítására alkalmas igazolvány segítségével is? Ha igen, fejtse ki! 11. Az adatszolgáltatás önkéntes? Ha igen, az érintettek megfelelő mértékben tájékoztatva vannak-e a kezelt adatok köréről, illetve jogaikról?
12. Az érintetteknek van-e lehetőségük arra, hogy adataik kizárólag meghatározott célokra történő felhasználásához nyújtsanak hozzájárulást? Ha igen, hogyan?
13. Megvalósul-e harmadik országba irányuló adattovábbítás? Ha igen, írja le a továbbítandó adatok fajtáit, a továbbítás címzettjének adatait, valamint az adattovábbítás jogalapját!
14. Fejtse ki, milyen lépéseket tesz az adatok biztonságának megőrzése érdekében!
15. Ha megfelelő szintűnek vélt az adatok biztonsága, milyen eszközök óvják az azonosítatlan hozzáféréstől?
16. A megfelelő védelmi eszközöket használja azonosítatlan hozzáférés megakadályozása érdekében? Fejtse ki álláspontját!
17. Van egyéb közlendő információja?

Harmadik rész: Előzetes hatásvizsgálathoz kapcsolódó további analízis

1. Hogyan biztosítja az érintettek jogainak érvényesítését? 2. Fejtse ki azokat az Ön által is ismert, alternatív megoldásokat, amelyek az eredeti eljáráshoz képest a cél elérése mellett kisebb mértékben érintenék a magánszférát!
3. Milyen módszerekkel kívánja csökkenteni az azonosított kockázati tényezőket?
4. Hogyan ellenőrzi az adatok teljességét?
5. Megfelelően naprakészek-e a gyűjtött adatok? Ha igen, támassza alá válaszát!
6. Kifejtett és részletezett az adatok természete?
7. Kinek van hozzáférési joga (lehetősége) a személyes adatokhoz?
8. Mi alapján kerülnek kiválasztásra azok a személyek, akik rendelkeznek ezzel a joggal?
9. A személyes adatokhoz való hozzáférés feltételei, módja, korlátai rögzítve vannak?
10. Milyen eszközök biztosítják az adatkezelés céljától eltérő felhasználás megakadályozását?
11. Hozzáférhet-e más rendszer a saját rendszerben kezelt adatokhoz? Ha igen, fejtse ki!
12. Az adatkezelés idejének lejárta után milyen módon kerülnek törlésre az adatok? Hogyan lesz dokumentálva az adattörlés?

5. melléklet
Adattovábbítási nyilvántartás

Az Adatkezelő neve és elérhetősége, képviselője neve és elérhetősége, az adatvédelmi tisztviselő neve és elérhetősége, szükség esetén a közös adatkezelő, valamint az adatfeldolgozó neve és elérhetősége, képviselője neve és elérhetősége	
Az adattovábbítás dátuma	
Az érintett beazonosításához szükséges adatok	
Az adattovábbítás célja	
Az adattovábbítás jogalapja	
Az átadott adatok köre	
Az adattovábbítás címzettje	

6. melléklet

Adatlap az adatvédelmi incidens adatvédelmi tisztviselő és az informatikai rendszerek informatikai biztonságáért felelős szervezeti egység vezetőjére részére történő bejelentéséhez

1. Az adatvédelmi incidenst bejelentő tájékoztató adatai:
Név:
.....
.....
E-mail-cím:
.....
.....
Cím:
.....
.....
Telefonszám:
.....
.....
Kapcsolattartó megnevezése, elérhetősége (telefonszám, e-mail):
.....
.....
.....
.....
.....
.....
1.1. Az adatkezelőn kívüli felek részvétele az adatvédelmi incidenssel érintett szolgáltatásban.
1.2. Részt vesz-e az adatkezelőn kívül más az adatvédelmi incidenssel érintett szolgáltatásban:
.....
.....
.....
.....
.....
.....
1.3. Az adatkezelőn kívüli fél megnevezése és minősége:
.....
.....
.....
.....
.....
.....

2. Az adatvédelmi incidenssel kapcsolatos időpontok:
Kezdő időpont:
.....
.....
Záró időpont:
.....
.....
Az adatvédelmi incidens továbbra is fennáll:
.....
.....
Az incidensről való tudomásszerzés időpontja:
.....
.....
Az incidens észlelésének módja:
.....
.....
Az adatfeldolgozó általi értesítés időpontja:
.....
.....
A késedelmes tájékoztatás indokai:
.....
.....
.....
.....
.....
.....
.....
.....
Egyéb megjegyzések az incidens időpontját illetően:
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

3. Az adatvédelmi incidens adatai (kérem, húzza alá a megfelelő választ, amennyiben szükséges, fejtse ki a részleteket):
3.1. Sérülés jellege:
- bizalmas jelleg:
- integritás:
- rendelkezésre állás:
3.2. Az adatvédelmi incidens jellege (kérem, húzza alá a megfelelő választ, amennyiben szükséges, fejtse ki a részleteket):
- eszköz elvesztése vagy ellopása:
- informatikai rendszer feltörése (hackelés):
- papíralapú dokumentum nem megfelelő módon történő megsemmisítése:
- papíralapú dokumentum elvesztése, ellopása vagy olyan helyen hagyása, amely nem minősül biztonságosnak:
- rosszindulatú számítógépes programok (pl. zsarolóprogram):
- elektronikus hulladék (a személyes adatok rajta maradnak az elavult eszközön):
- személyes adatok téves címzett részére történő küldése:
- levél elvesztése vagy jogosulatlan felnyitása:
- adathalászat:
- személyes adatok nagy nyilvánosság előtti jogellenes közzététele:
- személyes adatok jogosulatlan szóbeli közlése:
- egyéb:
.....
.....
.....
.....
.....
.....
4. Az adatvédelmi incidens okai (kérem, húzza alá a megfelelő választ, amennyiben szükséges, fejtse ki a részleteket):
- szervezeten belüli, rosszhiszeműnek nem minősülő cselekmény (belső szabályzat megsértése által):
- szervezeten belüli, rosszhiszemű cselekmény:
- külső, rosszhiszeműnek nem minősülő cselekmény:
- külső, rosszhiszemű cselekmény:
- egyéb:
.....
.....
.....
.....
.....
.....

5. Az adatvédelmi incidenssel érintett személyes adatok köre:
5.1. Személyes adatok (kérem, húzza alá a megfelelő választ, amennyiben szükséges, fejtse ki a részleteket):
- személyazonossághoz kapcsolódó adatok:
- elérhetőségi adatok:
- azonosító adatok:
- személyi szám:
- hivatalos okmányok:
- helymeghatározó adatok:
- gazdasági, pénzügyi adatok:
- büntetett előélettel, bűncselekményekkel vagy büntetéssel, intézkedéssel kapcsolatos adatok:
- különleges adatok:
5.2. Különleges adatok (legalább egy kiválasztása kötelező):
- faji eredetre, nemzetiséghez tartozásra vonatkozó adatok:
- politikai véleményre vonatkozó adatok:
- vallásos vagy más világnézeti meggyőződésre vonatkozó adatok:
- érdekképviseleti szervezeti tagságra vonatkozó adatok:
- szexuális életre vonatkozó adatok:
- egészségügyi adatok:
- genetikai adatok:
- biometrikus adatok:
- még nem ismert:
- egyéb:
.....
.....
.....
.....
.....
.....
5.3. Az adatvédelmi incidenssel érintett személyes adatok becsült száma:
.....
6. Az érintettek jellege (kérem, húzza alá a megfelelő választ, amennyiben szükséges, fejtse ki a részleteket):
- alkalmazottak:
- felhasználók:
- feliratkozók:
- hatósági eljárás vagy intézkedés alá vont, vagy azok által érintett személyek:
- még nem ismert:
- egyéb:
.....
.....
.....
.....

.....

.....

6.1. Az incidenssel érintett adatalanyok részletes leírása (pl. adatbázisokban szereplő munkavállalók leírása):

.....

.....

.....

.....

.....

.....

6.2. Az adatvédelmi incidenssel érintettek becsült száma:

.....

.....

7. Az incidens előtt alkalmazott intézkedések leírása (pl. tűzfal, vírusellenőrzés, adatszivárgás elleni védelmi rendszer):

.....

.....

.....

.....

.....

.....

8. Következmények:

8.1. Bizalmas jelleg sérülése (kérem, húzza alá a megfelelő választ, amennyiben szükséges, fejtse ki a részleteket):

- Szélesebb körű hozzáférés, mint ami szükséges, vagy amihez az érintett hozzájárult:
- Az adat összekapcsolhatóvá vált az érintett egyéb adatával:
- Az adatot más célokból történő, tisztességtelen módon történő kezelése lehetséges:
- egyéb:

.....

.....

.....

.....

8.2. Integritás sérülése (kérem, húzza alá a megfelelő választ, amennyiben szükséges, fejtse ki a részleteket):

- Az adat módosíthatóvá vált annak ellenére, hogy archivált vagy elavult volt:
- Az adatot valószínűsíthetően módosították egyébként pontos adatokra, és azokat eltérő célokra használhatták:
- egyéb:

.....

.....

.....

.....

8.3. Rendelkezésre állás sérülése (kérem, húzza alá a megfelelő választ, amennyiben szükséges, fejtse ki a részleteket):

- Az érintettek számára történő kritikus szolgáltatásnyújtás képességének módosulása:
- egyéb:

.....

.....

.....

.....

8.4. Az érintetteket ért fizikai, anyagi vagy nem vagyoni károk, vagy egyéb jelentős következmények:

8.5. Az incidens valószínűsíthető hatásai az érintettekre (kérem, húzza alá a megfelelő választ, amennyiben szükséges, fejtse ki a részleteket):

- személyes adatok feletti rendelkezés elvesztése:
- érintett jogainak korlátozása:
- hátrányos megkülönböztetés:
- személyazonosság-lopás:
- személyazonossággal való visszaélés:
- pénzügyi veszteség:
- álnevesítés engedély nélküli feloldása:
- jó hírnév sérelme:
- szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülése:
- egyéb:

.....

.....

.....

.....

.....

.....

8.6. A valószínűsíthető következmények súlyossága (kérem, húzza alá a megfelelő választ, amennyiben szükséges, fejtse ki a részleteket):

- elhanyagolható:
- korlátozott:
- jelentős:
- maximális:

9. Az incidens orvoslására megtett intézkedések:

9.1. Megtett intézkedések (az adatvédelmi tisztviselő vagy a bizottság tölti ki). A megtett védelmi intézkedések leírása:

.....

.....

.....

.....

.....

.....

.....

.....

9.2. Az érintettek tájékoztatása (kérem, húzza alá a megfelelő választ, amennyiben szükséges, fejtse ki a részleteket):
A tájékoztatás tervezett időpontja:
- még nincsen eldöntve:
- a tájékoztatás hiányának indokai:
- tényleges ideje, tartalma:
- érintetteknek javasolt intézkedések:
- intézkedések leírása, amelyek alapján az érintettek tájékoztatására nem került sor:
- tájékoztatott érintettek száma:
- az érintett tájékoztatásának formája:
- az érintetteknek szóló tájékoztatás tartalma:
- nyilvánosan közzétett információk vagy hasonló intézkedés:

.....
.....
.....
.....
.....
.....
.....
.....

10. Egyéb:

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

11. Egyéb bejelentések:

.....
.....
.....
.....
.....
.....

Más hatóságoknak (EU tagállami) vagy tagállamnak bejelentette-e az adatvédelmi incidenst?

.....
.....

.....
.....
.....
.....

7. melléklet

Adatlap az adatvédelmi incidens Hatóság részére történő bejelentéséhez

Az adatvédelmi incidensek bejelentése
(GDPR 33. cikk)

1. Az adatkezelő (bejelentő adatai)
Név:
.....
.....
Ország:
.....
.....
Irányítószám és hely:
.....
.....
Utcanév és házszám:
.....
.....
2. Az adatvédelmi tisztviselő/kapcsolattartó neve:
.....
.....
Elérhetősége:
.....
.....
3. Az incidens időpontja
Kezdete:
.....
.....
Tudomásra jutás időpontja:
.....
.....
4. Az incidens jellege
Az incidens leírása (nem jár kockázattal, kockázattal jár, magas kockázattal jár):
.....
.....
.....
.....
.....
.....
5. Az incidensben érintett adatok
Az adatok kategóriáinak leírása (különleges, bűnügyi adatok kiemelése):
.....
.....

.....

.....

6. Az incidensben érintett személyek kategóriái

Az érintettek csoportjának leírása:

.....

.....

.....

.....

.....

.....

.....

.....

7. A megelőzésre tett védelmi intézkedések

Az incidens megelőzésére tett védelmi intézkedések rögzítése:

.....

.....

.....

.....

.....

.....

.....

.....

8. Az incidens következményei

Az érintettre gyakorolt bekövetkezett hatások leírása (fizikai, vagyoni, nem vagyoni):

.....

.....

.....

.....

.....

.....

.....

.....

9. Az incidens valószínűsíthető következményei

Az érintettre gyakorolt lehetséges hatások leírása (fizikai, vagyoni, nem vagyoni):

.....

.....

.....

.....

.....

.....

.....

.....

10. Megtett intézkedések

A megtett védelmi intézkedések leírása:

.....

.....

.....

.....

.....

.....

.....

.....

Az érintettek tájékoztatása (tájékoztatás ideje, tartalma, érintetteknek javasolt intézkedések):

.....

.....

.....

.....

.....

.....

Egyéb:

.....

.....

.....

.....

.....

.....

8. melléklet

Tájékoztató az érintett részére adatvédelmi incidens esetén

Az érintett tájékoztatása az adatvédelmi incidensről
(GDPR 34. cikk)

1. Az adatvédelmi incidens időpontja:

.....
.....

2. Jellege:

.....
.....
.....
.....
.....
.....
.....
.....

3. Az adatvédelmi tisztviselő/kapcsolattartó neve:

.....
.....

Elérhetősége:

.....
.....

4. Az adatvédelmi incidensből eredő valószínűsíthető következmény(ek):

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

5. Az adatvédelmi incidens kezelésével kapcsolatban tervezett, illetve megtett intézkedések (ideértve a hátrányos következmények enyhítését célzó intézkedéseket):

.....
.....
.....
.....
.....
.....
.....
.....

.....

.....

6. Az érintett számára javasolt intézkedések megtétele a bekövetkezett kár enyhítése érdekében:

.....

.....

.....

.....

.....

.....

.....

.....

9. melléklet
Adatbiztonsági adatlap

A személyes adatokat kezelő nyilvántartások adatbiztonsági felmérése
(ADATLAP)

Az adatlap fókuszában a GDPR szerinti személyes adatokat kezelő nyilvántartások felmérése és a hatásvizsgálat elvégzésével összefüggésben a magas kockázatú adatkezelés megállapítása áll, a GDPR 29. cikke alapján létrehozott adatvédelmi munkacsoport (17/HU WP 248 rev.01) iránymutatásai alapján.

A személyes adatokat kezelő nyilvántartások adatbiztonsági felmérésének súlyponti kérdései a nyilvántartások bizalmassága, sértetlensége és rendelkezésre állása oly módon, hogy a felmérés eredményei alapján megállapítható legyen, hogy az adatkezelés a GDPR alkalmazásában „valószínűsíthetően magas kockázattal jár"-e, valamint a kockázatok kezelését célzó alkalmazott védelmi intézkedések és mechanizmusok (szervezeti intézkedések) biztosítják-e az érintettek és más személyek jogait és jogos érdekeit figyelembe vevő garanciákat.

A felmérés során számba vesszük, hogy az „adatkezelések" során jelenleg milyen személyi, adminisztratív, fizikai és elektronikus védelmi intézkedéseket alkalmaznak az adatbiztonsági kockázatok csökkentése érdekében.

Készült: 202.....-n a(z) (adatkezelő szerv megnevezése) hivatalos helyiségében.

Adatkezelő szerv megnevezése:

Ikt. szám:

Jelen vannak:

.....

nyilvántartást kezelő szervezeti egység vezetője

.....

felmérést végző bizottság tagja

.....

felmérést végző bizottság tagja

A NYILVÁNTARTÁS MEGNEVEZÉSE: .....

I. A NYILVÁNTARTÁS JELLEGÉNEK FELMÉRÉSE			
Felmérési kérdés	Igen/Van	Nem/Nincs	Megjegyzés
1. A nyilvántartás papíralapú.			
2. A nyilvántartás elektronikus.			
3. A nyilvántartáshoz kapcsolódik papíralapú adathordozó, amely személyes adatokat tartalmaz.			
4. A nyilvántartás alapja irodai alkalmazás (office-termékek).			
5. A nyilvántartás alapja célszoftver (erre a célra fejlesztett speciális alkalmazás).			
II. A NYILVÁNTARTÁS SZEMÉLYI FELTÉTELEI			
Felmérési kérdés	Igen/Van	Nem/Nincs	Megjegyzés
6. A nyilvántartás kezelését az adatkezelővel (adatfeldolgozóval) munkaviszonyban álló személy(ek) kezeli(k).			
7. A nyilvántartásokat kezelő személy(ek) rendelkezik/nek egyéb, személyi biztonságot fokozó ellenőrzéssel (erkölcsi bizonyítvány, nemzetbiztonsági ellenőrzés).			
8. A nyilvántartást kezelő személy(ek) rendszeresen részt vesz(nek) a nyilvántartások kezelésével összefüggő adatvédelmi és adatbiztonsági szabályokat feldolgozó továbbképzéseken.			
9. A nyilvántartást kezelő személy(ek) rendszeresen részt vesz(nek)-e a nyilvántartások kezelésével összefüggő adminisztratív (nyilvántartó rendszer) kezelési (iratkezelési) szabályok betartásával összefüggő képzéseken.			
III. A NYILVÁNTARTÁS FIZIKAI BIZTONSÁGI FELTÉTELEI			
Felmérési kérdés	Igen/Van	Nem/Nincs	Megjegyzés
10. A nyilvántartás és az azokhoz kapcsolódó személyes adatokat tartalmazó adathordozókhoz való illetéktelen (jogellenes) hozzáférést késleltető fizikai biztonsági eszközöket (beléptető rendszer, riasztó rendszer, biztonsági rács, biztonsági ajtó, páncélszekrény, zárható irodabútor) használnak.			
11. A nyilvántartás és az azokhoz kapcsolódó személyes adatokat tartalmazó adathordozók fizikai			

megsemmisülését megakadályozó biztonságtechnikai (tűzjelző, tűzálló páncélszekrény) rendszereket használnak.			
12. A nyilvántartást kezelő szervezeti egység objektumába a beléptetés ellenőrzött (beléptető rendszer, vendégnyilvántartás, csomagátvizsgálás) a portaszolgálatnál.			
13. A nyilvántartást kezelő szervezeti egységnél az objektumőrség (portaszolgálat) 24 órás rendelkezésre állású.			
14. A nyilvántartást kezelő szervezeti egység irodái munkaidő után zártak, a kulcsdobozokat munkaidőn túl a portaszolgálatnál tárolják.			
15. A nyilvántartást kezelő szervezeti egység irodáiban a takarítás ellenőrzött körülmények között (személyes felügyelet mellett) történik.			
16. A nyilvántartást kezelő szervezeti egység nyilvántartásokat kezelő rendszerének perifériái (fénymásoló, nyomtató) munkaidőn túl nem elérhetőek (nem a folyosón vannak elhelyezve) az illetéktelenek és a jogellenes tevékenység végrehajtására készülő személyek számára.			
17. A nyilvántartást kezelő szervezeti egység feldolgozó helyiségébe a belépés ellenőrzött, és illetéktelen személyek csak kísérettel (felügyelet mellett) tartózkodhatnak a helyiségben.			
IV. A NYILVÁNTARTÁS ADMINISZTRATÍV BIZTONSÁGI FELTÉTELEI			
Felmérési kérdés	Igen/Van	Nem/Nincs	Megjegyzés
18. A nyilvántartást kezelő szervezeti egységek (papíralapú vagy elektronikus) nyilvántartási rendszere alkalmas a személyes adatok nyomon követhető nyilvántartására.			
19. A nyilvántartás rekordjai, adategységei egyedi azonosítóval rendelkeznek.			
20. Az adatokhoz való hozzáférés (gyűjtés, módosítás, továbbítás) naplózott és a hiteles nyomon követés utólag is biztosított.			
21. A nyilvántartásból történő adatszolgáltatások (belső és külső átadások) naplózottak, utólag is hitelesen nyomon követhetőek.			

22. A nyilvántartás vezetésére használt (papír, elektronikus) rendszer/alkalmazás iratkezelési vagy egyéb tanúsítvánnyal rendelkezik.			
V. A NYILVÁNTARTÁS ELEKTRONIKUS BIZTONSÁGI FELTÉTELEI			
Felmérési kérdés	Igen/Van	Nem/Nincs	Megjegyzés
23. A nyilvántartás elektronikus kezelését végző szervezet biztonsági szintbe (1-5) történő besorolása megtörtént.			
24. Az elektronikus nyilvántartás (elektronikus információs rendszer) legalább 3-as biztonsági osztályba történő besorolása megtörtént.			
25. A nyilvántartást biztosító elektronikus információs rendszer adatainak és naplóinak biztonsági mentése és a mentések biztonságos tárolása megoldott.			
26. A nyilvántartást biztosító elektronikus információs rendszer rendelkezésre állása 24/7-es (folyamatos).			
27. A nyilvántartást biztosító elektronikus információs rendszer rendelkezésre állása napi 8 órában, munkaidőben biztosított.			
28. A nyilvántartást biztosító elektronikus információs rendszer redundáns adattárolása, rendszerüzemeltetési környezete biztosított.			
29. A nyilvántartást biztosító elektronikus információs rendszer redundáns (szünetmentes) tápellátása biztosított.			
30. A nyilvántartás alapját képező elektronikus információs rendszerrel összefüggő hitelesítés és jogosultság-ellenőrzés (autentikáció és autorizáció) biztosított.			
31. A nyilvántartást biztosító elektronikus információs rendszerben történő tranzakciók (felhasználói tevékenység) naplózottak.			
32. A nyilvántartást biztosító elektronikus információs rendszer biztonsági eseményei naplózottak.			
33. A naplófájlokat a biztonsági mentés tartalmazza.			
34. A nyilvántartást biztosító elektronikus információs rendszer biztonságos üzemeltetése hálózatvédelmi szoftverrel biztosított.			

35. A nyilvántartást biztosító elektronikus információs rendszer biztonságos üzemeltetése adatlopás elleni védelemmel (szoftverrel) biztosított.			
36. A nyilvántartást biztosító elektronikus információs rendszer biztonságos üzemeltetése tűzfalvédelemmel biztosított.			
37. A nyilvántartások adatainak kezelése titkosított adathordozón (pl. BitLocker meghajtó titkosítás) történik.			

Kmf.

.....

nyilvántartást kezelő szervezeti egység vezetője

....

felmérést végző bizottság tagja felmérést végző bizottság tagja

Készült: ..... példány/..... lap

Kapják:

10. melléklet
Felelősségi körökre vonatkozó adatlap

Felelősségi és feladatkörök meghatározása

	Nyilvántartás neve:	Név	Telefonszám	E-mail
1.	Döntéshozó személy az adatkezelő (államtitkárság, helyettes államtitkárság) részéről:			
	Kapcsolattartó személy az adatkezelő részéről:			
2.	Döntéshozó személy az adatbirtokos (főosztály) részéről:			
	Kapcsolattartó személy az adatbirtokos részéről:			
3.	Döntéshozó személy az adatfeldolgozó részéről:			
	Kapcsolattartó személy az adatfeldolgozó részéről:			