Szellemi Tulajdon
Nemzeti Hivatala

A Szellemi Tulajdon Nemzeti Hivatala adatvédelmi és adatbiztonsági szabályzata

……	……
készítette:	jóváhagyta:
dr. Hegedüs Krisztina s. k.	Pomázi Gyula s. k.
adatvédelmi tisztviselő	elnök

Hatályos: 2021. július. 9.

TARTALOM

I. ÁLTALÁNOS RENDELKEZÉSEK

I.1. Fogalmak

A Szabályzat alkalmazásában:

a) *érintett*: a személyes adat alapján azonosított vagy – közvetve vagy közvetlenül – azonosítható természetes személy (az adatalany);[1]
b) *személyes adat*: érintettre vonatkozó bármely információ;[2]
c) *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;[3]
d) *adatkezelés*: a személyes adatokon 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;[4]
e) *adattovábbítás*: a személyes adat egy meghatározott harmadik személy számára történő hozzáférhetővé tétele;[5]
f) *nyilvánosságra hozatal*: a személyes adat bárki számára történő hozzáférhetővé tétele;[6]
g) *adattörlés*: a személyes adat felismerhetetlenné tétele oly módon, hogy a helyreállítása többé nem lehetséges;[7]
h) *adatkezelő*: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza;[8]
i) *adatfeldolgozó*: az a természetes vagy jogi személy, illetve bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel;[9]
j) *címzett*: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, akivel vagy amellyel a személyes adatot közlik, függetlenül attól, hogy harmadik fél-e;[10]
k) *harmadik fél*: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely nem azonos az érintettel, az adatkezelővel, az adatfeldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy

[1] L. Általános adatvédelmi rendelet (GDPR) 4. cikk 1. pont.
[2] Uo.
[3] GDPR 9. cikk (1) bekezdés és Infotv. 3. § 3. pont.
[4] GDPR 4. cikk 2. pont.
[5] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (Infotv.) 3. § 11. pont.
[6] Infotv. 3. § 12. pont.
[7] Infotv. 3. cikk 13. pont.
[8] GDPR 4. cikk 7. pont.
[9] GDPR 4. cikk 8. pont.
[10] GDPR 4. cikk 9. pont.

adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére felhatalmazást kaptak;[11]

l) *harmadik ország*: minden, az Európai Gazdasági Térségen kívüli ország;[12]

m) *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;[13]

n) *hozzájárulás*: az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló, egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez;[14]

o) *adatvédelmi incidens*: a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi;[15]

p) *adatbiztonság*: minden olyan technikai vagy szervezési intézkedés, amelynek célja a kezelt személyes adatok biztonságának biztosítása, így különösen azok az intézkedések, amelyek a személyes adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet szolgálják;[16]

q) *álnevesítés*: a személyes adatok olyan módon történő kezelése, amelynek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik, feltéve, hogy az ilyen további információt külön tárolják, és technikai és szervezési intézkedések megtételével biztosított, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni;[17]

r) *személyes adat megsemmisítése*: a személyes adat egyáltalán nem, vagy az adatkezelő számára nem használható formában létezik;[18]

s) *személyes adat elvesztése*: az adatkezelő már nem rendelkezik a személyes adat felett, nem fér hozzá, vagy az nincsen a birtokában;[19]

t) *személyes adat megváltoztatása*: a személyes adat módosult, sérült, vagy már nem hiánytalan;[20]

u) *nemvárt esemény*: minden olyan esemény, amely az adatkezelő kezelésében lévő adatok vagy információk megsemmisítésével, elvesztésével, megváltoztatásával, illetve

---

[11] GDPR 4. cikk 8. pont.
[12] Infotv. 3. § 24. pont.
[13] Infotv. 3. cikk 23. pont.
[14] GDPR 4. cikk 11. pont.
[15] GDPR 4. cikk 12. pont.
[16] GDPR 5. cikk (1) bekezdés f) pont és 32. cikk.
[17] GDPR 4. cikk 5. pont.
[18] A 29. cikk alapján létrehozott Adatvédelmi Munkacsoport iránymutatása az adatvédelmi incidensek (EU) 2016/679 rendelet szerinti bejelentéséről (http://naih.hu/files/wp250rev01_hu.pdf).
[19] Uo.
[20] Uo.

jogosulatlan közlésével vagy az azokhoz való hozzáféréssel jár, ideértve különösen a r)-t) pontokban foglalt eseteket is;

v) *NAIH*: Nemzeti Adatvédelmi és Információszabadság Hatóság;

w) *biometrikus adat:* egy természetes személy testi, fiziológiai vagy viselkedési jellemzőire vonatkozó minden olyan sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását, ilyen például az iriszkép vagy a daktiloszkópiai adat;[21]

x) *fokozottan személyes jellegű adat:* olyan személyes adat, amelynek kezelése fokozza az érintett jogait és szabadságait érintő lehetséges kockázatokat, különös tekintettel az otthoni vagy magánjellegű tevékenységekhez kapcsolódó, az alapvető jog gyakorlására kiható, valamint az olyan adatokra, amelyeket érintő jogsértések egyértelműen súlyos hatást gyakorolnak az érintett mindennapi életére;[22]

y) *profilalkotás:* a személyes adatok automatizált kezelésének bármely olyan formája, amelynek során a személyes adatokat valamely természetes személyhez fűződő bizonyos személyes jellemzők értékelésére használják.[23]

II. A SZELLEMI TULAJDON NEMZETI HIVATALA ADATVÉDELMI RENDSZERE

II.1. Az adatkezelő megnevezése és elérhetőségei

(1) A Szabályzat hatálya alá tartozó adatkezelések tekintetében a Szellemi Tulajdon Nemzeti Hivatala minősül adatkezelőnek (a továbbiakban: Adatkezelő vagy Hivatal).[24]

(2) Az Adatkezelőre vonatkozó adatok:
   a) *megnevezés*: Szellemi Tulajdon Nemzeti Hivatala
   b) *székhely*: 1081 Budapest, II. János Pál pápa tér 7.
   c) *postacím*: 1438 Budapest, Pf. 415.
   d) *e-mail*: sztnh@hipo.gov.hu
   e) *adatvédelmi tisztviselő neve:* dr. Hegedüs Krisztina
   f) *adatvédelmi tisztviselő elérhetőségei:*
      - e-mail cím: krisztina.hegedus@hipo.gov.hu és adatvedelem@hipo.gov.hu
      - telefonszám: +36-1-474-5941 és +36-20-297-1266

(3) Az Adatkezelő a Szabályzat tartalmának kialakítása során figyelembe vette a vonatkozó jogszabályokat, fontosabb nemzetközi ajánlásokat, amelyeket az 1. számú melléklet tartalmaz.

II.2. Az adatvédelmi tisztviselő szerepe

(1) Az Adatkezelő köteles adatvédelmi tisztviselőt kijelölni.[25] Az Adatkezelő adatvédelmi tisztviselőjét a Hivatal elnöke nevezi ki.

---

[21] GDPR 4. cikk 14. pont.
[22] https://www.naih.hu/files/WP248_rev01_hu.pdf
[23] GDPR 4. cikk 4. pont.
[24] GDPR 4. cikk 7. pont.
[25] GDPR 37. cikk (1) bekezdés.

(2) Az adatvédelmi tisztviselő elsősorban a következő feladatokat látja el:
   a) tájékoztat és szakmai tanácsot ad az Adatkezelő vagy bármely adatfeldolgozója, továbbá az adatkezelést végző munkatársak részére a GDPR, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezések szerinti kötelezettségeikkel kapcsolatban,
   b) ellenőrzi a GDPR-nak, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezéseknek, továbbá az Adatkezelő vagy az adatfeldolgozó személyes adatok védelmével kapcsolatos belső szabályainak való megfelelést, ideértve a feladatkörök kijelölését, az adatkezelési műveletekben részt vevő személyek tudatosság-növelését és képzését, valamint a kapcsolódó auditokat is,
   c) kérésre szakmai tanácsot ad az érdekmérlegelési tesztre és az adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomon követi az érdekmérlegelési teszt útmutatás szerinti, illetve az adatvédelmi hatásvizsgálat GDPR 35. cikke szerinti elvégzését,
   d) gondoskodik az Adatkezelő által a tevékenységei körében végzett adatkezelésekkel kapcsolatos adatkezelési tájékoztatók és a jelen Szabályzat naprakészségéről, elérhetőségéről,
   e) figyelemmel kíséri az Adatkezelő által a tevékenységei körében végzett adatkezeléseket,
   f) közreműködik, illetve segítséget nyújt az adatkezeléssel összefüggő döntések meghozatalában, valamint az érintettek jogainak biztosításában,
   g) együttműködik a NAIH-hal,
   h) az adatkezeléssel összefüggő ügyekben kapcsolattartó pontként szolgál a NAIH felé, valamint adott esetben bármely egyéb kérdésben konzultációt folytat vele,
   i) vezeti az adatvédelmi tevékenységek nyilvántartását (belső adatvédelmi nyilvántartás),
   j) vezeti az adatvédelmi incidensek nyilvántartását,
   k) véleményezi a részére megküldött, adatvédelmi kérdéseket érintő belső szabályozási dokumentumok és szerződések tervezetét,
   l) az adatvédelmi kérdésekkel összefüggésben fogadja az Adatkezelő munkatársainak, illetve egyéb érintetteknek a megkereséseit, konzultációs kérdéseit, és azokkal érdemben foglalkozik,
   m) minden évben a Hivatal elnöke által meghatározott időpontig, külön meghatározás hiányában január 15-ig elkészíti az Adatkezelő előző éves adatvédelmi tevékenységéről készült jelentést, amelyet a Hivatal elnöke hagy jóvá,
   n) minden évben a Hivatal elnöke által meghatározott időpontig, külön meghatározás hiányában december 15-ig elkészíti a következő évi munkatervét és ellenőrzési tervét, amelyeket a Hivatal elnöke hagy jóvá.

(3) Az adatvédelmi tisztviselő a fentieken túlmenően ellátja a Szabályzatban részére meghatározott feladatokat, illetve minden olyan feladatot, amellyel a Hivatal elnöke megbízza, kivéve abban az esetben, ha a feladat a GDPR (97) preambulumbekezdésében, vagy a 38. cikk (6) bekezdésében meghatározottak szerint összeférhetetlen az adatvédelmi tisztviselői tevékenység ellátásával.

(4) Az adatvédelmi tisztviselő a Hivatal elnökének tartozik felelősséggel.[26]

[26] GDPR 38. cikk (3) bekezdés.

II.3. A Hivatal elnökének szerepe

A Hivatal elnöke

a) kinevezi a GDPR-ban meghatározott feltételeknek megfelelő személyt adatvédelmi tisztviselőnek,
b) meghatározza és biztosítja a személyes adatok kezelésének és védelmének személyi és tárgyi feltételeit, beleértve a technikai feltételeket is,
c) felel a Hivatal adatvédelmi tevékenységéért, az ellenőrzések során esetlegesen feltárt hiányosságok vagy nem megfelelőségek megszüntetéséért,
d) szükség esetén személyi felelősség megállapítására irányuló eljárást indít vagy kezdeményez,
e) egyetértése esetén jóváhagyja az adatvédelmi tisztviselő éves jelentését, valamint munkatervét és ellenőrzési tervét.

II.4. Az Adatkezelő személyes adatot kezelő szervezeti egysége vezetőjének és az önálló területeket képviselő hivatali munkatársak szerepe

Az Adatkezelő személyes adatot kezelő szervezeti egységének vezetője és az önálló területet képviselő hivatali munkatárs ellátja a jelen Szabályzatban meghatározott feladatokat, így különösen

a) új (vagy új típusú) adatkezeléssel járó tevékenység bevezetése esetén előzetesen konzultál az adatvédelmi tisztviselővel,
b) az adatkezelés során közreműködik az adatvédelmi követelmények betartásában,
c) elvégzi a belső adatvédelmi nyilvántartásba bejelentésre kötelezett adatkezelések bejelentését az adatvédelmi tisztviselő részére,
d) részt vesz a Szabályzat elkészítésében és aktualizálásában,
e) ellenőrzi a számítógépeken, elektronikus adathordozókon a személyes adatok, illetve ezek felhasználásával készült dokumentumok kezelését, a dokumentumok megfelelő tárolását,
f) közreműködik az adatvédelmi tisztviselő feladatai ellátásának segítésében,
g) szükség esetén részt vesz a bekövetkezett adatvédelmi incidensek kivizsgálásában,
h) szükség esetén ő vagy az általa kijelölt munkatársa elvégzi az adatvédelmi hatásvizsgálatot, vagy személyesen vagy kijelölt munkatársa útján részt vesz annak lefolytatásában,
i) gondoskodik az adatvédelmi szabályok végrehajtásának feltételrendszeréről, az irányítása alá tartozó szervezeti egység által kezelt rendszerben található személyes adatok védelméről,
j) intézkedik a nem szabályszerű adatkezelési gyakorlat megszüntetéséről, az eset kivizsgálása érdekében értesíti az adatvédelmi tisztviselőt, informatikai rendszer érintettsége esetén az informatikai és az információbiztonsági vezetőt is,
k) intézkedik az adatvédelmi tisztviselő felé az érintett által hozzá benyújtott, tiltakozási vagy egyéb érintetti jog teljesülése érdekében,
l) betartja és munkatársaival betartatja a II.5. pontban írt kötelezettségeket.

II.5. A személyes adatokat kezelő munkatársak szerepe

Az Adatkezelő azon munkatársa, aki személyes adatok kezelésével kapcsolatos tevékenységet végez, köteles

a) gondoskodni arról, hogy az adatkezelés teljes folyamatában maradéktalanul érvényesüljenek az adatvédelmi előírások;
b) gondoskodni arról, hogy a személyes adatok továbbítása az Adatkezelő szervezetén kívülre lehetőség szerint jelszóval vagy más módon védetten, az azokat hordozó dokumentum metaadat-mentesítését követően valósuljon meg,
c) részt venni az adatvédelmi tisztviselő által tartott vagy szervezett oktatáson, továbbá letenni az esetlegesen ahhoz kapcsolódó vizsgát,
d) ellátni a Szabályzat rendelkezéseire tekintettel rá háruló adatvédelmi feladatokat,
e) adatvédelemmel kapcsolatos kérdés esetén az adatvédelmi tisztviselőhöz fordulni.

II.6. Az információbiztonsági vezető szerepe

Az Adatkezelő információbiztonsági vezetője ellátja a jelen Szabályzatban meghatározott feladatokat, így különösen

a) a jogszabályok és belső szabályzatok előírásainak megfelelően gondoskodik az Adatkezelővel szemben támasztott adatbiztonsági követelmények minél magasabb szintű megvalósításáról,
b) együttműködik az adatvédelmi tisztviselővel az adatvédelmi és adatbiztonsági követelmények érvényesülésében,
c) részt vesz az adatvédelmi incidensek kivizsgálásában;
d) szükség esetén részt vesz az adatvédelmi hatásvizsgálat lefolytatásában.

II.7. Adatfeldolgozók szerepe

Mindazok, akik az Adatkezelő megbízásából az Adatkezelő nevében és helyett személyes adatot kezelnek, kötelesek

a) az adatvédelmi jogszabályokban és az Adatkezelő belső szabályzataiban foglalt adatvédelmi és adatbiztonsági, további egyéb, az adatkezelésre vonatkozó követelményeket betartani,
b) az adatvédelmi tisztviselő által tartott vagy szervezett oktatáson részt venni, az esetlegesen ahhoz kapcsolódó vizsgát letenni,
c) ellátni az e Szabályzat rendelkezéseire tekintettel rájuk háruló adatvédelmi és adatbiztonsági feladatokat,
d) adatvédelemmel kapcsolatos kérdés esetén az adatvédelmi tisztviselőhöz fordulni.

III. AZ ADATKEZELÉS ELVEI

(1) A Hivatal számára alapvető érték, egyben cél is a személyes adatok védelme; ezért az általa folytatott tevékenységekkel összefüggésben végzett adatkezelések vonatkozásában betartja a releváns adatkezelési elveket.

(2) A Hivatal számára kiemelten fontos érték a tisztességesség követelménye.[27] Ennek megfelelően a Hivatal mindenkor tiszteletben tartja az érintettek emberi méltóságát és magánéletét. Tilos minden olyan tevékenység, amely az érintettek magánéletének szükségtelen megzavarásával, illetve az érintettek személyes adatainak rejtett vagy titkos kezelésével jár, továbbá az érintettek titkos megfigyelését eredményezi.

(3) A Hivatal mindenkor eleget tesz a jogszerűség követelményének.[28] A Hivatal az általa folytatott tevékenységekkel összefüggésben végzett adatkezelések során a mindenkor hatályos adatvédelmi előírások betartásával jár el, továbbá eleget tesz a személyes adatok kezelésének jogalapjával kapcsolatos követelményeknek.

(4) A Hivatal törekszik arra, hogy az általa folytatott tevékenységekkel összefüggésben végzett adatkezelések átláthatók legyenek az érintettek számára.[29] A Hivatal e követelményt különösen a tájékoztatáshoz és hozzáféréshez való jog gyakorlásával összefüggésben, valamint az érintettel folytatott kommunikáció során érvényesíti.

(5) A Hivatal az általa folytatott tevékenységekkel összefüggésben végzett adatkezelések során mindenkor a célhoz kötöttség követelményére tekintettel jár el.[30] A Hivatal a személyes adatok kizárólag előre meghatározott, egyértelmű jogszerű cél – jog gyakorlása vagy kötelezettség teljesítése – érdekében kezeli. Az adatkezelésnek mindvégig meg kell felelnie e célnak. Tilos a személyes adatokat a céllal össze nem egyeztethető módon kezelni. Tilos a személyes adatokat előre meghatározott, egyértelmű és jogszerű cél hiányában kezelni.

(6) A Hivatal az általa folytatott tevékenységekkel összefüggésben végzett adatkezelések során csak olyan személyes adatot kezel, amely az adatkezelés célja szempontjából megfelelő és releváns, illetve az adatkezelés célja eléréséhez szükséges (adattakarékosság elve).[31]

(7) A Hivatal az általa folytatott tevékenységekkel összefüggésben végzett adatkezelések során csak olyan személyes adatot kezel, amely pontos és naprakész.[32] A Hivatal köteles minden észszerű intézkedést meghozni az adatkezelés céljai szempontjából pontatlan személyes adatok haladéktalan törlése vagy helyesbítése érdekében.

(8) A Hivatal az általa folytatott tevékenységekkel összefüggésben végzett adatkezelések során biztosítja, hogy a kezelt személyes adatok az érintettek azonosítását csak az adatkezelés céljának eléréséhez szükséges ideig tegyék lehetővé (korlátozott tárolhatóság elve).[33]

(9) A Hivatal megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítja a személyes adatok megfelelő biztonságát, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni

[27] GDPR 5. cikk (1) bekezdés a) pont.
[28] Uo.
[29] Uo.
[30] GDPR 5. cikk (1) bekezdés b) pont.
[31] GDPR 5. cikk (1) bekezdés c) pont
[32] GDPR 5. cikk (1) bekezdés d) pont
[33] GDPR 5. cikk (1) bekezdés e) pont.

védelmét is ideértve (integritás és bizalmas jelleg elve).[34]

(10) A Hivatal biztosítja az általa folytatott tevékenységekkel összefüggésben végzett adatkezelések megfelelőségének igazolásához szükséges dokumentumok rendelkezésre állását és naprakészségét.[35] A Hivatal köteles bizonyítani azt, hogy az általa folytatott tevékenységekkel összefüggésben végzett adatkezelések megfelelnek a vonatkozó adatvédelmi előírásoknak (elszámoltathatóság elve).

IV. AZ ADATKEZELÉS JOGALAPJAI

(1) A személyes adatok kezelése kizárólag akkor és annyiban jogszerű, amennyiben legalább az alábbi feltételek egyike teljesül:
   a) az érintett hozzájárulását adta – beleértve a hozzájárulást félreérthetetlenül kifejező cselekedetet is – személyes adatainak egy vagy több konkrét célból történő kezeléséhez;
   b) az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél, vagy az a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges;
   c) az adatkezelés az Adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges;
   d) az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges;
   e) az adatkezelés közérdekű vagy az Adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges;
   f) az adatkezelés az Adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé, különösen, ha az érintett gyermek.

(2) Különleges adatok[36] esetében az (1) bekezdés a)-f) pontjaiban írtak egyikének fennállta mellett is csak abban az esetben kerülhet sor a személyes adatok kezelésére, amennyiben az adatkezelés jelentős közérdek miatt szükséges, illetve uniós jog vagy tagállami jog alapján, amely arányos az elérni kívánt céllal, tiszteletben tartja a személyes adatok védelméhez való jog lényeges tartalmát, és az érintett alapvető jogainak és érdekeinek biztosítására megfelelő és konkrét intézkedéseket ír elő.

(3) Kétség esetén a jogalap alkalmazhatóságáról az adatvédelmi tisztviselő dönt.

IV.1. Az érintett hozzájárulása

(1) Az érintett hozzájárulása akkor tekinthető az adatkezelés érvényes jogalapjának, amennyiben az az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló, egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez.

[34] GDPR 5. cikk (1) bekezdés f) pont.
[35] GDPR 5. cikk (2) bekezdés.
[36] GDPR 9. cikk

(2) Az érintett hozzájárulása során biztosítani kell, hogy valódi választási lehetőség álljon az érintett rendelkezésére, a beleegyezés tudatossága felől nem lehet kétség. Nem minősül önkéntesnek a hozzájárulás akkor, ha annak következményei aláássák az egyén választási szabadságát.

(3) Az érintett hozzájárulása esetén:
   a) az Adatkezelőnek képesnek kell lennie annak igazolására, hogy az érintett a személyes adatainak kezeléséhez hozzájárult;[37]
   b) az Adatkezelőnek biztosítania kell azt, hogy az érintett a hozzájárulását bármikor indokolás nélkül visszavonhassa, és a hozzájárulás visszavonását ugyanolyan egyszerű módon kell lehetővé tennie, mint annak megadását;[38]
   c) a hallgatás, az előre bejelölt négyzet vagy a nem cselekvés nem minősül hozzájárulásnak;[39]
   d) a hozzájárulás megadása nem tekinthető önkéntesnek, ha az érintett nem rendelkezik valós vagy szabad választási lehetőséggel, illetve nem áll módjában a hozzájárulás anélküli megtagadása vagy visszavonása, hogy ez kárára válna;[40]
   e) nem tekinthető önkéntesnek a beleegyezés, ha nem tesz lehetővé külön-külön hozzájárulást a különböző személyes adatkezelési műveletekhez;[41]
   f) nem tekinthető önkéntesnek a hozzájárulás, ha a szerződés teljesítése (például a szolgáltatás nyújtását) olyan adatkezeléshez való hozzájáruláshoz volt kötve, amely adatkezelés nem szükséges a szerződés teljesítéséhez;[42]
   g) a hozzájárulás nem szolgálhat érvényes jogalapként akkor, ha az érintett és az Adatkezelő között egyértelműen egyenlőtlen viszony áll fenn;[43]
   h) ha az Adatkezelő írásbeli nyilatkozaton keresztül szerzi be az érintett hozzájárulását, akkor a nyomtatványon a hozzájárulás iránti kérelmet egyértelműen és világosan el kell választani a szerződés többi részétől, valamint ezen kérelmet érthető és egyszerű nyelvezettel kell az Adatkezelőnek megfogalmaznia.[44]

(4) A hozzájárulás beszerzése előtt az Adatkezelő – adott esetben a munkatársai vagy a nevében eljáró adatfeldolgozó útján – köteles megfelelő tájékoztatásban részesíteni az érintettet. A tájékoztatás megtörténhet az erre rendszeresített hozzájáruló nyilatkozaton feltüntetett információk megismerése révén is. Ebben az esetben elegendő időt kell biztosítani az érintett számára arra, hogy megismerje a tájékoztatást és megértse a benne foglaltakat.

(5) Az érintett jogosult további információkat és felvilágosítást kérni az Adatkezelőtől – adott esetben a munkatársai vagy a nevében eljáró adatfeldolgozó útján –; a tájékoztatás vagy

[37] GDPR 7. cikk (1) bekezdés.
[38] GDPR 7. cikk (3) bekezdés.
[39] GDPR (32) preambulumbekezdés
[40] GDPR (42) preambulumbekezdés.
[41] GDPR (43) preambulumbekezdés.
[42] GDPR (43) preambulumbekezdés és 7. cikk (4) bekezdés.
[43] GDPR (43) preambulumbekezdés.
[44] GDPR 7. cikk (2) bekezdés.

felvilágosítás megadása kötelező. A tájékoztatás megadásához szükség esetén az adatvédelmi tisztviselő segítséget nyújt.

IV.2. A szerződéses jogalap

(1) Az Adatkezelő és az érintett közötti szerződés létrehozása és teljesítése jogalapot teremthet a személyes adatok kezelésére.[45]

(2) A szerződés megkötése érdekében akkor kezelhetők személyes adatok, ha az alábbi követelmények mindegyike teljesül:
   a) a szerződést az érintettel köti az Adatkezelő;
   b) az érintett bocsátja az adatokat az Adatkezelő rendelkezésére;
   c) az adatok az Adatkezelő és az érintett közötti szerződés megkötéséhez szükségesek.

(3) A szerződés teljesítése érdekében akkor kezelhetők a személyes adatok, ha az alábbi követelmények mindegyike teljesül:
   a) a felek megkötötték azt a szerződést, amelyikben az érintett az egyik fél;
   b) a szerződés érvényes;
   c) az adatkezelés ténylegesen szükséges a szerződés általános célkitűzésének eléréséhez.

(4) A szükségesség követelményének érvényesülése a szerződéses jogalap alkalmazásának előfeltétele.[46] E követelmény nem redukálható pusztán a szerződéses kitételek vizsgálatára, hanem feltételezi az adatvédelmi garanciák, illetve a GDPR-ban meghatározott alapelvek mérlegelését is, különös tekintettel a tisztességes eljárás, a célhoz kötöttség és az adattakarékosság elvére. Ebből következően amennyiben az adatkezelés hasznos, de objektíve nem szükséges a szerződés teljesítéséhez, nem alkalmazható a szerződéses jogalap.

IV.3. Kötelező adatkezelés

(1) Az Adatkezelőre vonatkozó jogi kötelezettség teljesítése is jelentheti az adatkezelés jogalapját.[47]

(2) A jogi kötelezettség teljesítése abban az esetben szolgáltathat jogalapot a személyes adatok kezeléséhez, amennyiben:
   a) azt uniós vagy hazai jogszabály rendeli el;
   b) a rendelkezés közvetlenül az Adatkezelőre vonatkozó kötelezettséget tartalmaz;
   c) a rendelkezés közérdekű célt szolgál;

---

[45] GDPR 6. cikk (1) bekezdés b) pont.

[46] L. az Európai Adatvédelmi Testület 2/2019. számú iránymutatása a személyes adatoknak az általános adatvédelmi rendelet 6. cikke (1) bekezdésének b) pontja szerinti kezeléséről az érintettek részére nyújtott online szolgáltatások összefüggésében (https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_hu.pdf)

[47] GDPR 6. cikk (1) bekezdés c) pont.

d) a rendelkezés arányos az elérni kívánt jogszerű céllal.[48]

(3) Kötelező adatkezelés esetén a kezelendő adatok fajtáit, az adatkezelés célját és feltételeit, az adatok megismerhetőségét, az adatkezelő személyét, valamint az adatkezelés időtartamát vagy szükségessége időszakos felülvizsgálatát az adatkezelést elrendelő törvény vagy önkormányzati rendelet határozza meg.[49]

(4) Ha a kötelező adatkezelés időtartamát vagy szükségessége időszakos felülvizsgálatát törvény, helyi önkormányzat rendelete vagy az Európai Unió kötelező jogi aktusa nem határozza meg, az Adatkezelő az adatkezelés megkezdésétől legalább háromévente felülvizsgálja, hogy az általa, illetve a megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által kezelt személyes adat kezelése az adatkezelés céljának megvalósulásához szükséges-e. Ezen felülvizsgálat körülményeit és eredményét az Adatkezelő dokumentálja, e dokumentációt a felülvizsgálat elvégzését követő tíz évig megőrzi és azt a NAIH kérésére a rendelkezésére bocsátja.[50]

IV.4. Létfontosságú érdek

(1) Az Adatkezelő adatkezelését jogszerűnek kell tekinteni abban az esetben is, amikor az az érintett vagy más természetes személy létfontosságú érdekeinek védelmében történik. Más természetes személy létfontosságú érdekeire hivatkozással személyes adatkezelésre csak akkor kerülhet sor, ha a szóban forgó adatkezelés egyéb jogalapon nem végezhető el.[51]

(2) A létfontosságú érdek védelmét jelentheti különösen az érintett vagy más természetes személy életének, testi épségének, egészségének védelme.

IV.5. Közfeladat ellátása

(1) Amennyiben az adatkezelés az Adatkezelő közérdekű vagy rá ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges, abban az esetben a személyes adatok kezelésének jogalapja a GDPR 6. cikk (1) bekezdésének e) pontja. Az adatkezelések esetében a jogalapot uniós jog, illetve azon nemzeti jog szerint lehet megállapítani, amelynek hatálya alá az Adatkezelő tartozik.

(2) Ezen jogalap alkalmazásának feltétele, hogy az Adatkezelő a közfeladata végrehajtásához szükséges adatkezelési tevékenységét közérdeken alapuló célból hazai vagy uniós jogszabály alapozza meg. Az ilyen feladatellátásnak meg kell felelnie a IV.3. pont (2)-(4) bekezdésében írt kötelezettségeknek.[52]

---

[48] GDPR 6. cikk (3) bekezdés.
[49] Infotv. 5. § (3) bekezdés.
[50] Infotv. 5. § (5) bekezdés.
[51] GDPR (46) preambulumbekezdés.
[52] https://www.naih.hu/files/NAIH_beszamolo_2019.pdf

IV.6. A jogos érdek

(1) Az Adatkezelő – ideértve azt az adatkezelőt is, akivel a személyes adatokat közölhetik – vagy valamely harmadik fél jogos érdeke jogalapot teremthet az adatkezelésre, feltéve, hogy azzal szemben az érintett érdekei, alapvető jogai és szabadságai nem élveznek elsőbbséget, figyelembe véve az Adatkezelővel való kapcsolata alapján az érintett észszerű elvárásait is.[53]

(2) Az (1) bekezdésben írtakkal szemben a jogos érdek nem szolgálhat az adatkezelés jogalapjául, amennyiben az adatkezelést az Adatkezelő – ideértve azt az adatkezelőt is, akivel a személyes adatokat közölhetik – vagy valamely harmadik fél közfeladat ellátásával összefüggésben végzi.[54]

(3) A jogos érdek fennállásának megállapításához minden esetben megvizsgálandó az, hogy az érintett a személyes adatok gyűjtésének időpontjában és azzal összefüggésben számíthat-e észszerűen arra, hogy adatkezelésre az adott célból kerülhet sor.[55] Az érintettek érdekei és alapvető jogai elsőbbséget élvezhetnek az Adatkezelő érdekével szemben, ha a személyes adatokat olyan körülmények között kezelik, amelyek közepette az érintettek nem számítanak adatkezelésre vagy további adatkezelésre.

(4) A jogos érdek jogalapként történő kezeléséhez az szükséges, hogy az Adatkezelő elvégezze az ún. érdekmérlegelési tesztet. Az érdekmérlegelési teszt a következő lépésekből áll:
   a) meg kell határozni az Adatkezelő jogszerű, egyértelmű és valós érdekét;
   b) azonosítani kell az érintettek alapvető jogait és szabadságait, valamint figyelembe kell venni az érintettek elvárásait;
   c) elemezni kell az adatkezelés szükségességét és arányosságát;
   d) olyan intézkedéseket kell meghatározni, amelyek az adatkezelés érintettekre gyakorolt hatásait csökkentik vagy tovább csökkentik.[56]

V. AZ ÉRINTETTI JOGOK

V.1. Előzetes tájékoztatási kötelezettség

(1) Az érintettek részére a személyes adatok megszerzésének időpontjában tájékoztatást kell adni a GDPR 13-14. cikke szerinti tartalommal, különösen a személyes adatok kezelésének tényéről, céljáról, jogalapjáról, a kezelt adatok köréről, az adatkezelés módjáról, időtartamáról vagy az időtartam meghatározásának szempontjairól, az adattovábbítás szabályairól, valamint a felügyeleti hatósághoz címzett panasz benyújtásának jogáról.

(2) Az (1) bekezdés szerinti tájékoztatás mellett, a személyes adatok GDPR 6. cikk (1)

[53] GDPR 6. cikk (1) bekezdés f) pont.
[54] GDPR 6. cikk (1) bekezdés.
[55] GDPR (47) preambulumbekezdés.
[56] L. a 29. cikk alapján létrehozott Adatvédelmi Munkacsoport 06/2014. számú vélemény az adatkezelő 95/46/EK irányelv 7. cikke szerinti jogszerű érdekeinek fogalmáról (https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_hu.pdf).

bekezdésének e) vagy f) pontján alapuló kezelése esetén az érintett figyelmét kifejezetten fel kell hívni a tiltakozáshoz való jog érvényesítésének lehetőségére, és az erre vonatkozó tájékoztatást egyértelműen és minden más információtól elkülönítve kell megjeleníteni.

(3) Az (1)-(2) bekezdés szerinti tájékoztatást:
   a) az álláspályázatot benyújtók számára az álláspályázati felhívás közzétételét szolgáló oldalon a vonatkozó adatkezelési tájékoztató szerinti tartalommal kell nyújtani;
   b) az Adatkezelővel munkaviszonyt, kormányzati szolgálati jogviszonyt létesítők részére a jogviszony létrejöttekor a vonatkozó adatkezelési tájékoztatók szerinti tartalommal kell nyújtani;
   c) az Adatkezelő közfeladatainak ellátásából adódó tevékenysége során a szolgáltatásait igénybe vevőknek a szolgáltatás igénybevételekor a vonatkozó adatkezelési tájékoztató szerinti tartalommal kell nyújtani.

(4) A (3) bekezdés a) és c) pontja szerinti tájékoztatásokat az Adatkezelő honlapján, tömör, átlátható és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva kell elhelyezni.

(5) A (3) bekezdés b) pont szerinti tájékoztatást legkésőbb a jogviszony létesítésekor elektronikus formában kell megadni, melynek megtörténtének igazolása megvalósulhat
   a) az érintett papír alapú nyilatkozatával írásban vagy
   b) a Hivatalban szokott módon (az intranet megfelelő rovatában) közzétett tájékoztatás alábbi adatainak igazolásával:
      a. mikor történt meg a közzététel
      b. erről az érintettek milyen módon kaptak tájékoztatást (intranetes hír, körlevél elnöki értekezletről készült emlékeztető, stb.) .

V.2. A hozzáféréshez való jog

(1) Az érintett kérelmére az adatkezelést végző illetékes munkatárs vagy vezetője az adatvédelmi tisztviselő támogatásával, illetve amennyiben az célszerű, az adatvédelmi tisztviselő maga a kérelem beérkezésétől számított egy hónapon belül tájékoztatást ad az érintett vonatkozásában folyamatban lévő adatkezelés(ek)ről. Szükség esetén, figyelembe véve a kérelem összetettségét és a kérelmek számát, ez a határidő további két hónappal meghosszabbítható. A határidő meghosszabbításáról az Adatkezelő a késedelem okainak megjelölésével a kérelem kézhezvételétől számított egy hónapon belül tájékoztatja az érintettet.

(2) Az érintett jogosult arra, hogy hozzáférést kapjon a személyes adataihoz, illetve a következő információkhoz:
   a) az adatkezelés céljai;
   b) az érintett személyes adatok kategóriái;
   c) azon címzettek vagy címzettek kategóriái, akikkel, illetve amelyekkel a személyes adatokat közölték vagy közölni fogják, ideértve különösen a harmadik országbeli címzetteket, illetve a nemzetközi szervezeteket is;

d) adott esetben a személyes adatok tárolásának tervezett időtartama, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjai;
e) az érintett azon joga, hogy kérelmezheti az Adatkezelőtől a rá vonatkozó személyes adatok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen;
f) a valamely felügyeleti hatósághoz címzett panasz benyújtásának joga;
g) ha az adatokat nem az érintettől gyűjtötték, a forrásukra vonatkozó minden elérhető információ.[57]

(3) A személyes adatokhoz való hozzáférést úgy kell biztosítani, hogy annak során az érintett más személy személyes adatait ne ismerhesse meg. Ez alól kivételt képezhetnek azok a személyes adatok, amelyek mind az érintettre, mind egy másik személyre is vonatkoznak.[58]

(4) Az érintett hozzáféréshez való jogát az Adatkezelő az elérni kívánt céllal arányosan korlátozhatja vagy megtagadhatja, ha ezen intézkedés elengedhetetlenül szükséges harmadik személyek alapvető jogai és szabadságai védelmének biztosításához, beleértve az üzleti titkot és a szellemi tulajdont is. Az e bekezdésben írt korlátozás nem eredményezheti azt, hogy az Adatkezelő az érintettől minden információt megtagadjon.[59]

(5) Ha az Adatkezelő nagy mennyiségű információt kezel az érintettre vonatkozóan, kérheti őt, hogy az információk közlését megelőzően pontosítsa, hogy kérése mely információkra vagy adatkezelési tevékenységekre vonatkozik.[60]

(6) Amennyiben az Adatkezelő a (4) bekezdésben foglaltak szerint megtagadja vagy korlátozza az érintett hozzáférési jogát, erről haladéktalanul írásban tájékoztatja érintettet az intézkedés indokát is megjelölve. A tájékoztatásban az Adatkezelő információt nyújt arról is, hogy az érintett panaszt nyújthat be valamely felügyeleti hatóságnál, és élhet bírósági jogorvoslati jogával.

(7) Az Adatkezelő a Szabályzat 2. számú mellékletében foglalt nyilvántartásban tartja nyilván a hozzáféréshez való jog gyakorlásával kapcsolatos intézkedéseit. Amennyiben az Adatkezelő a (4)-(5) bekezdésekben foglalt intézkedést alkalmaz, az intézkedés jogi és ténybeli indokait is megjelöli.

V.3. A helyesbítéshez való jog gyakorlása

(1) Az érintett kérelmére az adatkezelést végző illetékes munkatárs vagy vezetője szükség esetén az adatvédelmi tisztviselő tanácsának kikérését követően indokolatlan késedelem nélkül helyesbíti az érintettre vonatkozó pontatlan személyes adatokat.[61] Figyelembe véve az adatkezelés célját, az érintett jogosult arra, hogy kérje a hiányos személyes adatok –

[57] GDPR 15. cikk.
[58] GDPR 15. cikk (3)-(4) bekezdés.
[59] GDPR (63) preambulumbekezdés.
[60] GDPR (63) preambulumbekezdés.
[61] GDPR 16. cikk.

egyebek mellett kiegészítő nyilatkozat útján történő – kiegészítését is.

(2) Az Adatkezelő minden olyan címzettet tájékoztat a személyes adatot érintő valamennyi helyesbítésről, akivel, illetve amellyel a személyes adatot közölte, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel. Az érintettet kérelmére az Adatkezelő tájékoztatja e címzettekről.[62]

V.4. A törléshez való jog

(1) Az érintett kérelmére az adatkezelést végző illetékes munkatárs vagy vezetője szükség esetén az adatvédelmi tisztviselő tanácsának kikérését követően indokolatlan késedelem nélkül törli az érintett személyes adatait vagy azoknak az érintett által meghatározott körét, feltéve, hogy az alábbi esetek valamelyike fennáll:

a) a személyes adatokra már nincs szükség abból a célból, amelyből azokat gyűjtötték vagy más módon kezelték;
b) az érintett visszavonja az adatkezelés alapját képező hozzájárulását, és az adatkezelésnek nincs más jogalapja;
c) az érintett tiltakozik az adatkezelés ellen, és nincs elsőbbséget élvező jogszerű ok az adatkezelésre;
d) a személyes adatokat jogellenesen kezelték;
e) a személyes adatokat az Adatkezelő által alkalmazandó uniós vagy tagállami jogban előírt jogi kötelezettség teljesítéséhez törölni kell.[63]

(2) Ha az Adatkezelő nyilvánosságra hozta a személyes adatot, és az (1) bekezdés értelmében azt törölni köteles, az elérhető technológia és a megvalósítás költségeinek figyelembevételével megteszi az észszerűen elvárható lépéseket – ideértve technikai intézkedéseket – a szóban forgó személyes adatokra mutató linkek vagy e személyes adatok másolatának, illetve másodpéldányának törlése érdekében.[64]

(3) Az Adatkezelő minden olyan címzettet tájékoztat a személyes adatot érintő valamennyi törlésről, akivel, illetve amellyel a személyes adatot közölte, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel. Az érintettet kérelmére az Adatkezelő tájékoztatja e címzettekről.[65]

(4) Az Adatkezelő a személyes adatok törlését a jogszerű kérelem ellenére sem végezheti el, amennyiben az adatkezelés szükséges:

a) a véleménynyilvánítás szabadságához és a tájékozódáshoz való jog gyakorlása céljából;
b) a személyes adatok kezelését előíró, az Adatkezelő által alkalmazandó uniós vagy tagállami jog szerinti kötelezettség teljesítése céljából;
c) közérdekből végzett feladat végrehajtása céljából;

[62] GDPR 19. cikk.
[63] GDPR 17. cikk (1) bekezdés.
[64] GDPR 17. cikk (2) bekezdés.
[65] GDPR 19. cikk.

d) közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból, amennyiben az adattörlés valószínűsíthetően lehetetlenné tenné vagy komolyan veszélyeztetné ezt az adatkezelést;
e) jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez.[66]

V.5. Az adatkezelés korlátozásához való jog

(1) Az érintett kérelmére az adatkezelést végző illetékes munkatárs vagy vezetője szükség esetén az adatvédelmi tisztviselő tanácsának kikérését követően korlátozza az adatkezelést, ha az alábbi feltételek valamelyike teljesül:
a) az érintett vitatja a személyes adatok pontosságát, ez esetben a korlátozás arra az időtartamra vonatkozik, amely lehetővé teszi, hogy az adatkezelést végző illetékes ügyintéző, a vezetője vagy az adatvédelmi tisztviselő ellenőrizze a személyes adatok pontosságát;
b) az adatkezelés jogellenes, és az érintett ellenzi az adatok törlését, és ehelyett kéri azok felhasználásának korlátozását;
c) az Adatkezelőnek már nincs szüksége a személyes adatokra adatkezelés céljából, de az érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez; vagy
d) az érintett tiltakozási jogával élt az adatkezelés ellen; ez esetben a korlátozás arra az időtartamra vonatkozik, amíg megállapításra nem kerül, hogy az Adatkezelő jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben.[67]

(2) Ha az adatkezelés az (1) bekezdés alapján korlátozás alá esik, az ilyen személyes adatokat a tárolás kivételével
a) csak az érintett hozzájárulásával, vagy
b) jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez, vagy
c) más természetes vagy jogi személy jogainak védelme érdekében, vagy
d) az Unió, illetve valamely tagállam fontos közérdekéből
lehet kezelni.

(3) Az adatkezelést végző illetékes munkatárs vagy vezetője szükség esetén az adatvédelmi tisztviselő tanácsának kikérését követően az érintettet, akinek a kérésére az (1) bekezdés alapján korlátozták az adatkezelést, az adatkezelés korlátozásának feloldásáról előzetesen tájékoztatja.[68]

(4) Az Adatkezelő minden olyan címzettet tájékoztat a személyes adatot érintő valamennyi adatkezelés-korlátozásról, akivel, illetve amellyel a személyes adatot közölte, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel. Az érintettet kérelmére az Adatkezelő tájékoztatja e címzettekről.[69]

[66] GDPR 17. cikk (3) bekezdés.
[67] GDPR 18. cikk (1) bekezdés.
[68] GDPR 18. cikk (3) bekezdés.
[69] GDPR 19. cikk.

V.6. Az adathordozhatósághoz való jog

(1) Az érintett kérelmére az adatkezelést végző illetékes munkatárs vagy vezetője szükség esetén az adatvédelmi tisztviselő tanácsának kikérését követően biztosítja a személyes adatok hordozhatóságát az alábbi feltételek teljesülése esetén:
   a) a személyes adatokat az érintett bocsátotta az Adatkezelő rendelkezésére;
   b) az adatkezelés jogalapja hozzájárulás vagy az érintett és az Adatkezelő között kötött szerződés;[70]
   c) az adatkezelés automatizált módon történik;[71]
   d) a személyes adatok hordozása nem érinti hátrányosan mások jogait vagy szabadságait.

(2) Az adathordozhatósághoz való jog gyakorlása során az Adatkezelő a személyes adatokat tagolt, széles körben használt, géppel olvasható (elsősorban PDF vagy XML) formátumban köteles az érintett rendelkezésére bocsátani.

(3) Az érintett – abban az esetben, amennyiben az technikailag megvalósítható – kérheti, hogy az Adatkezelő a személyes adatokat közvetlenül egy másik adatkezelő részére továbbítsa. Az Adatkezelő a kérést nem köteles teljesíteni.

(4) Az Adatkezelő emellett az érintett kérelme esetén – a hozzáféréshez való jog érvényesülésének elősegítése érdekében – papír alapon is köteles rendelkezésre bocsátani a személyes adatokat.

V.7. A tiltakozáshoz való jog

(1) Amennyiben az adatkezelés az Adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez vagy közfeladatainak végrehajtásához szükséges, az érintett tiltakozhat a személyes adatai kezelése ellen.

(2) Tiltakozás esetén az Adatkezelő a személyes adatokat nem kezelheti tovább, kivéve, ha bizonyítja, hogy az adatkezelést olyan kényszerítő erejű jogos okok indokolják, amelyek elsőbbséget élveznek az érintett érdekeivel, jogaival és szabadságaival szemben, vagy amelyek jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódnak.[72]

(3) Ha a személyes adatok kezelése közvetlen üzletszerzés érdekében történik, az érintett jogosult arra, hogy bármikor tiltakozzon a rá vonatkozó személyes adatok e célból történő kezelése ellen; ebben az esetben a személyes adatok a továbbiakban e célból nem kezelhetők.[73]

---

[70] GDPR 6. cikk (1) bekezdés a)-b) pontja.
[71] A papír alapú adatkezelések esetében e jog nem gyakorolható, helyette a hozzáférési jog gyakorlásán belül a másolatkiadás joga él.
[72] GDPR 21. cikk (1) bekezdés.
[73] GDPR 21. cikk (3) bekezdés.

V.8. A jogorvoslathoz való jog

(1) Adatkezeléssel kapcsolatos jogainak megsértése esetén az érintett – az adatkezelést végző illetékes munkatárs vagy vezetője útján, illetve közvetlenül – az adatvédelmi tisztviselőhöz fordulhat, aki a panaszt megvizsgálja, és ha az alapos, a Hivatal elnökénél intézkedést, ellenkező esetben a panasz elutasítását kezdeményezi.

(2) Az elutasításról az Adatkezelő az érintettet a kérelem kézhezvételét követő egy hónapon belül írásban tájékoztatja, a kérelem elutasításának ténybeli és jogi indokait is közölve. A kérelem elutasítása esetén az érintettet tájékoztatni kell a bírósági jogorvoslat, továbbá a felügyeleti szervhez fordulás lehetőségéről is. Az elutasított kérelmeket az adatvédelmi tisztviselő dokumentálni köteles.

(3) Ha az érintett továbbra is sérelmezi azt, ahogyan a Adatkezelő kezeli az adatait, vagy közvetlenül felügyeleti hatósághoz szeretne fordulni, akkor bejelentéssel élhet a NAIH-nál (cím: 1055 Budapest, Falk Miksa utca 9-11., levelezési cím: 1363 Budapest, Pf. 9., e-mail: ugyfelszolgalat@naih.hu, honlap: www.naih.hu).

(4) Az érintettnek lehetősége van továbbá személyes adatainak védelme érdekében bírósághoz fordulni, amely az ügyben soron kívül jár el. Ebben az esetben az érintett szabadon választhat, hogy a lakóhelye (állandó lakcím) vagy a tartózkodási helye (ideiglenes lakcím) szerinti törvényszéknél (http://birosag.hu/torvenyszekek) nyújtja-e be keresetét. Az érintett lakóhelye vagy tartózkodási helye szerinti törvényszékek megkereshetők a http://birosag.hu/ugyfelkapcsolati-portal/birosag-kereso oldalon.

VI. ADATBIZTONSÁG

(1) Az Adatkezelő az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre annak biztosítása és bizonyítása céljából, hogy a személyes adatok kezelése a GDPR-ral összhangban történik; ideértve többek között, adott esetben:

a) a személyes adatok álnevesítését és titkosítását;[74]

b) a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítását, integritását, rendelkezésre állását és ellenálló képességét;

c) fizikai vagy műszaki incidens esetén az arra való képességet, hogy a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását kellő időben vissza lehet állítani;

d) az adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedések hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárást.[75]

[74] GDPR 4. cikk 5. pont.
[75] GDPR 32. cikk (1) bekezdés.

(2) A biztonság megfelelő szintjének meghatározásakor kifejezetten figyelembe kell venni az adatkezelésből eredő olyan kockázatokat, amelyek a kezelt személyes adatok véletlen vagy jogellenes megsemmisítéséből, elvesztéséből, megváltoztatásából, jogosulatlan nyilvánosságra hozatalából vagy az azokhoz való jogosulatlan hozzáférésből erednek.[76]

(3) Az Adatkezelő megfelelő technikai és szervezési intézkedéseket hajt végre, amelyek célja egyrészt a Szabályzatban meghatározott adatvédelmi alapelvek hatékony megvalósítása, másrészt a további adatvédelmi garanciák beépítése az adatkezelés folyamatába.[77]

(4) Az Adatkezelő megfelelő technikai és szervezési intézkedéseket hajt végre annak biztosítására, hogy alapértelmezés szerint kizárólag olyan személyes adatok kezelésére kerüljön sor, amelyek az adott konkrét adatkezelési cél szempontjából szükségesek. Ez a kötelezettség vonatkozik a személyes adatok mennyiségére, kezelésük mértékére, tárolásuk időtartamára és hozzáférhetőségükre egyaránt. Ezek az intézkedések különösen azt kell, hogy biztosítsák, hogy a személyes adatok alapértelmezés szerint a természetes személy beavatkozása nélkül ne válhassanak hozzáférhetővé meghatározatlan számú személy számára.[78]

(5) Személyes adatot tartalmazó irat nem hagyható olyan helyen, ahol harmadik személy is hozzáférhet. Az ilyen iratok elzárásáról azokban az irodákban és egyéb helyiségekben is gondoskodni kell, ahol az illetékes munkatársakon kívül más, harmadik személy (akár másik hivatali munkatárs) is megfordulhat.

(6) Az adathordozó képek és dokumentációk elhelyezésének, fizikai védelmének biztonságáról az adatkezelő szervezeti egység vezetője – szükség esetén az adatvédelmi tisztviselővel és az információbiztonsági vezetővel való előzetes konzultáció után – dönt.

(7) A szervezeti egységeknél kialakítandó adatkezelési rendszer környezetének védelméről a helyi adottságok figyelembevételével az illetékes vezetőknek kell gondoskodnia, beleértve az adatbiztonság sérülésének megelőzését is.

(8) A manuálisan kezelt személyes adatok elvesztésének megelőzése érdekében eredeti iratokat csak hivatalos ügyintézés, különösen bírósági vagy nyomozati eljárás során lehet kiadni. Kiadást megelőzően az eredeti iratokról hiánytalan másolatot kell készíteni.

(9) Személyes adatokat ért sérülés vagy megsemmisülés esetén a rendelkezésre álló egyéb adatforrásokból meg kell kísérelni a lehetséges mértékig a károsodott adatok pótlását. A sérült adat pótlásáért annak a szervezeti egységnek a vezetője felelős, ahol az adatsérülés bekövetkezett. Az adatpótlásba be kell vonni azon illetékes adatkezelő munkatársat, aki az adatok rögzítésében közreműködött. A pótolt adatokon vagy dokumentumokon a pótlás tényét fel kell tüntetni.

[76] GDPR 4. cikk 12. pont.
[77] GDPR 25. cikk (1) bekezdés.
[78] GDPR 25. cikk (2) bekezdés.

VII. ELSZÁMOLTATHATÓSÁG

VII.1. Az adatkezelésre és adatfeldolgozásra vonatkozó általános követelmények

(1) Az Adatkezelővel a Szabályzatot hatályba léptető elnöki utasítás 2. §-a szerint jogviszonyban álló személy, aki személyes adat birtokába jut, ilyet munkaköre vagy tisztsége alapján kezel, köteles azokat védeni és őrizni, továbbá minden erőfeszítést megtenni annak érdekében, hogy azok megfelelő védelmét biztosítsa.

(2) A személyes adatokat különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen kell védeni.

(3) Az Adatkezelővel jogviszonyban állók, illetve az Adatkezelő képviseletében eljáró személyek kötelesek titokban tartani minden olyan személyes adatot, amely számukra a jogviszonyukkal vagy feladatellátással összefüggésben vált ismertté.

(4) Az Adatkezelővel bármilyen jellegű jogviszonyban álló, adatkezelést vagy adatfeldolgozást végző személyek felelősséggel tartoznak minden olyan kárért, amely adatkezelési, adatvédelmi kötelezettségük megszegéséből származik.

(5) Ha az adatkezelést az Adatkezelő nevében más végzi, az Adatkezelő kizárólag olyan adatfeldolgozókat vehet igénybe, akik vagy amelyek megfelelő garanciákat nyújtanak az adatkezelés követelményeinek való megfelelést és az érintettek jogainak védelmét biztosító, megfelelő technikai és szervezési intézkedések végrehajtására.

(6) Az adatfeldolgozó által végzett adatkezelést olyan, írásban megkötött szerződésnek kell szabályoznia, amely köti az adatfeldolgozót az Adatkezelővel szemben. Szerződés helyett kivételesen az Adatkezelő alkalmazhat olyan dokumentumot is, amelyből az adatfeldolgozóra egyoldalú kötelezettség hárul. E dokumentumra a szerződésre vonatkozó szabályokat kell alkalmazni.

(7) A szerződésben rögzíteni kell különösen az alábbiakat:
   a) a Hivatal és az adatfeldolgozó megnevezése;
   b) az adatkezelés tárgya;
   c) a kezelendő személyes adatok típusa;[79]
   d) a kezelendő személyes adatok mennyisége (ha lehetséges);
   e) az érintettek kategóriái;[80]
   f) az adatkezelés jellege és célja;
   g) az adatkezelés jogalapja;
   h) az adatkezelés időtartama;
   i) teendők az adatkezelési szolgáltatás nyújtásának befejezés esetén;[81]

[79] A kezelendő adatkörök megnevezése.
[80] Pl. munkatárs, kapcsolattartó
[81] Személyes adat törlése, vagy visszajuttatása az Adatkezelőnek és törlése.

j) az Adatkezelő kötelezettségeit és jogait;
k) azt, hogy az adatfeldolgozó a személyes adatokat kizárólag az Adatkezelő írásbeli utasításai alapján jogosult kezelni – beleértve a személyes adatoknak valamely harmadik ország vagy nemzetközi szervezet számára való továbbítását is –, kivéve, ha az adatkezelést az adatfeldolgozóra alkalmazandó uniós vagy tagállami jog írja elő; ebben az esetben erről a jogi előírásról az adatfeldolgozó az Adatkezelőt az adatkezelést megelőzően értesíti, kivéve, ha az Adatkezelő értesítését az adott jogszabály fontos közérdekből tiltja;
l) az Adatkezelő és az adatfeldolgozó közötti utasításadás, illetve kapcsolattartás módja;
m) a további adatfeldolgozó igénybevételére vonatkozó döntés;
n) azon kikötés, hogy az adatfeldolgozó a további adatfeldolgozó igénybevételére vonatkozóan tiszteletben tartja a jogszabályi előírásokat;[82]
o) titoktartási kötelezettség;
p) adatbiztonsági előírások;[83]
q) közreműködés az adatbiztonsági előírások érvényesítésében, az incidensek kezelésében és a hatásvizsgálatok elvégzésénél;[84]
r) közreműködés az érintetti jogok gyakorlásában;
s) információk nyújtása az Adatkezelőnek és az Adatkezelő ellenőrzési jogosultsága;[85]
t) az Adatkezelő ellenőrzésének kivitelezési módja;
u) a felelősség egyes kérdései;
v) a jogérvényesítési lehetőségek.

(8) Amennyiben szükséges, az Adatkezelő és az adatfeldolgozó további intézkedéseket hoz annak biztosítására, hogy az Adatkezelő vagy az adatfeldolgozó irányítása alatt eljáró, a személyes adatokhoz hozzáféréssel rendelkező természetes személyek kizárólag az Adatkezelő utasításának megfelelően kezelhessék az említett adatokat.

(9) A (7) bekezdésben meghatározott tartalmi elemek gyakorlati alkalmazása érdekében az adatfeldolgozóval kötendő szerződéses rendelkezések általános mintáját az Adatkezelő adatvédelmi tisztviselője állítja össze, illetve szükség esetén módosítja. E rendelkezések mintáját az adatvédelmi tisztviselő tartja nyilván, és teszi hozzáférhetővé a Hivatal intranetjén a munkatársak számára.

VII.2. Az adattovábbításra vonatkozó követelmények

(1) Az Adatkezelő szervezeti rendszerén belül a személyes adatok – a feladat elvégzéséhez szükséges mértékben és ideig – olyan szervezeti egységhez, személyhez továbbíthatók, amelynek/akinek az Adatkezelőnél végzett feladatának ellátásához a személyes adatok megismerése és kezelése szükséges.

[82] GDPR 28. cikk (2) és (4) bekezdés.
[83] GDPR 32. cikk.
[84] GDPR 32-36. cikk.
[85] Az Adatkezelő vagy az általa megbízott más személy, mint ellenőr jogosult az adatkezelés megkezdése előtt, illetve annak folyamatában auditokat végezni, beleértve a helyszíni vizsgálatokat is, amelyek célja az adatfeldolgozó tevékenysége jogszerűségének biztosítása.

(2) Az Adatkezelőnél különböző célra irányuló adatkezelések csak törvényes céloknak megfelelően, indokolt esetben kapcsolhatók össze.

(3) Olyan megkeresés, amely az Adatkezelő által kezelt személyes adat továbbítására irányul, csak kötelező jogszabályi rendelkezés alapján vagy a GDPR 6. és 9. cikkeiben meghatározott egyéb jogalap és körülmény fennállása esetén teljesíthető. Minden más esetben az adattovábbítás teljesítését meg kell tagadni.

(4) Külföldre irányuló adattovábbítás esetén az adattovábbítást végző hivatali munkatársnak vagy vezetőjének külön meg kell győződnie arról, hogy a külföldre történő adattovábbítás GDPR-ban előírt feltételei fennállnak-e. Ennek kapcsán vizsgálandó, hogy az adattovábbítás a GDPR-ban meghatározott valamely jogalapnak megfelelően történik-e, és az adatok megfelelő védelmi szintje az adatokat átvevő személynél vagy szervezetnél biztosított-e. Ha az adattovábbítás az Európai Gazdasági Térség valamely tagállamába irányul, a személyes adatok megfelelő szintű védelmét nem kell vizsgálni.[86]

(5) Személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására sor kerülhet, ha az Európai Bizottság megállapította, továbbá az Európai Unió Hivatalos Lapjában és annak honlapján közzétette, hogy a harmadik ország, a harmadik ország valamely területe, egy vagy több meghatározott ágazata, vagy a szóban forgó nemzetközi szervezet megfelelő védelmi szintet biztosít (megfelelőségi határozat). Az ilyen adattovábbításhoz nem szükséges külön engedély.

(6) A harmadik országba vagy nemzetközi szervezet részére való adattovábbítások (5) bekezdésen túli eseteit a GDPR 46-50. cikkei szabályozzák, azokról szükség esetén az adatvédelmi tisztviselő ad felvilágosítást.

(7) Olyan személyes adatok továbbítására – ideértve a személyes adatok harmadik országból vagy nemzetközi szervezettől egy további harmadik országba vagy további nemzetközi szervezet részére történő újbóli továbbítását is –, amelyeket harmadik országba vagy nemzetközi szervezet részére történő továbbításukat követően adatkezelésnek vetnek alá vagy szándékoznak alávetni, csak abban az esetben kerülhet sor, ha az Adatkezelő és az adatfeldolgozó egyaránt teljesíti a GDPR-ban rögzített feltételeket.

(8) Az adattovábbítás megfelelőségének kérdésében – erre irányuló kérdés esetén – az Adatkezelő adatvédelmi tisztviselője felvilágosítást ad.

(9) Személyes adatok továbbítása során, amennyiben az postai küldeményként történik, biztosítani kell, hogy a küldemény zártan kerüljön feladásra.

(10) Az Adatkezelő vállalja, hogy a személyes adatokat statisztikai célra kizárólag úgy adja át, hogy gondoskodik arról, hogy azokat az érintettel ne lehessen kapcsolatba hozni.

(11) Az Adatkezelő az általa végzett adattovábbításokat a Szabályzat 3. számú mellékletét képező nyilvántartás szerinti tartalommal tartja nyilván.

[86] GDPR 44-50. cikkek.

VII.3. Az adatkezelési tevékenységek nyilvántartása

(1) Az Adatkezelő köteles nyilvántartani minden olyan adatkezelési tevékenységét, amely:
   a) az érintettek jogaira és szabadságaira nézve valószínűsíthetően kockázattal jár;
   b) nem alkalmi jellegű;
   c) különleges adatok vagy bűnügyi személyes adatok kezelésével jár.[87]

(2) Az Adatkezelő az (1) bekezdés szerinti kötelezettségének a 4. számú mellékletben foglaltak szerinti tartalommal tesz eleget.

(3) Az Adatkezelő nevében az (1) bekezdés szerinti nyilvántartást az adatvédelmi tisztviselő vezeti az érintett szervezeti egység vezetője vagy az önálló területeket képviselő munkatárs által rendelkezésre bocsátott információk felhasználásával.

(4) Az adatvédelmi tisztviselő köteles a nyilvántartást a NAIH ez irányú kérésére rendelkezésre bocsátani.

VIII. ADATVÉDELMI HATÁSVIZSGÁLAT

VIII.1. Az adatvédelmi hatásvizsgálat elvégzésének esetkörei

(1) Az adatvédelmi hatásvizsgálat elvégzésének három esetköre lehetséges. Kötelező elvégezni az adatvédelmi hatásvizsgálatot, amennyiben
   a) az adatkezelés szerepel a NAIH GDPR 35. cikk (4) bekezdése alapján kibocsátott listáján,[88]
   b) az adatkezelés, figyelemmel annak jellegére (különösen új technológiát alkalmazó voltára), hatókörére, körülményére és céljaira, valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve,[89]
   c) az Adatkezelő a tervezett adatkezelésre figyelemmel így dönt (eseti döntés).

(2) Kötelező adatvédelmi hatásvizsgálatot végezni, amennyiben az adatkezelés az alábbi kategóriák bármelyikének hatálya alá tartozik:
   a) az érintettekre vonatkozó egyes személyes jellemzők olyan módszeres és kiterjedt értékelése, amely automatizált adatkezelésen alapul, és amelyre joghatással bíró vagy az érintettet hasonlóképpen jelentős mértékben érintő döntések épülnek;
   b) a személyes adatok különleges kategóriái vagy a büntetőjogi felelősség megállapítására vonatkozó határozatokra vagy bűncselekményekre vonatkozó személyes adatok nagy számban történő kezelése; vagy
   c) nyilvános helyek nagymértékű, módszeres megfigyelése.

(3) A (2) bekezdésben írt eseteken túl kötelező adatvédelmi hatásvizsgálatot végezni, amennyiben az adatkezelés az alábbi kategóriák bármelyikének hatálya alá tartozik:

[87] GDPR 9. cikk (1) bekezdés és 10. cikk.
[88] https://naih.hu/files/GDPR_35_4_lista_HU_mod.pdf
[89] GDPR 35. cikk (1) bekezdés.

a) az adatkezelés egy természetes személy egyedi azonosítását célzó biometrikus adatának kezelése módszeres megfigyelésre irányul;
b) az adatkezelés kiszolgáltatott helyzetben lévő érintettek biometrikus adatainak felhasználására irányul;
c) az adatkezelés célja az érintett bizonyos tulajdonságainak felmérése, amelynek eredménye kihatással van az érintett részére nyújtott, illetve nyújtandó szolgáltatás létrejöttére vagy minőségére;
d) az adatkezelés célja harmadik személytől begyűjtött személyes adatok felhasználása az érintettre vonatkozó szolgáltatás visszautasítására vagy megszüntetésére vonatkozó döntés meghozatalánál;
e) az adatkezelés célja személyes adatok nagyszámú, illetve módszeres értékelése révén végzett profilalkotás, 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;
f) 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;
g) az adatkezelés célja az érintettek nagyszámú és módszeres megfigyelése jellemzően közterületeken vagy nyilvános helyeken történő kamerarendszerek, drónok, illetve bármely más új technológia használatával;
h) az adatkezelés helymeghatározási adatok kezelésére irányul, ha az módszeres megfigyelésre vagy profilalkotásra utal;
i) az adatkezelés célja a munkatárs munkájának megfigyelése során a munkatárs személyes adatainak nagyszámú és módszeres feldolgozása, illetve értékelése;
j) az adatkezelés különleges adatok nagy számban való kezelésére irányul;
k) az adatkezelés nagyszámú személyes adat bűnüldözési célú kezelésére irányul;
l) az adatkezelés kiszolgáltatott helyzetben lévő érintettekkel kapcsolatos, nagy számban kezelt adatok eredeti céltól eltérő kezelésére irányul;
m) az adatkezelés gyermekek személyes adatainak kezelésére irányul profilozás, automatizált döntéshozatal vagy marketing céljából, illetve közvetlenül a részükre kínált, információs társadalommal összefüggő szolgáltatások ajánlása vonatkozásában;
n) az adatkezelés új technológiai megoldások használatát vonja maga után;
o) az adatkezelés során több adatkezelő egy egész ágazat által közösen használt alkalmazást, rendszert, eszközt, illetve platformot tervez létrehozni, amelyben különleges adatokat is kezelnek;
p) az adatkezelés célja a különböző forrásokból származó adatok összevonása, egymással való megfeleltetése vagy összehasonlítása.

(4) A (2)-(3) bekezdésekben foglaltakon kívül kötelező adatvédelmi hatásvizsgálatot végezni, amennyiben az adatkezelés az alábbi kategóriák közül legalább kettő hatálya alá tartozik:
a) az adatkezelés célja 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;

b) az adatkezelés joghatással vagy hasonló jelentős hatással járó automatizált döntéshozatalra irányul;
c) az adatkezelés érintettek megfigyelésére, nyomon követésére vagy ellenőrzésére irányul;
d) az adatkezelés különleges adatok vagy fokozottan személyes jellegű adatok kezelésére irányul;
e) az adatkezelés nagyszámú adat kezelésére irányul;
f) az adatkezelés adatkészletek egymással való megfeleltetésére vagy összevonására irányul;
g) az adatkezelés kiszolgáltatott helyzetben lévő érintettekkel kapcsolatos adatok kezelésére irányul;
h) az adatkezelés új technológiai vagy szervezési megoldások innovatív használatára vagy alkalmazására irányul;
i) az adatkezelés önmagában véve megakadályozza, hogy az érintettek a jogaikat gyakorolják, szolgáltatásokat vegyenek igénybe vagy szerződést érvényesítsenek.

(5) Amennyiben az adatkezelés nem esik a (2)-(4) bekezdés hatálya alá, főszabály szerint nem kötelező az adatvédelmi hatásvizsgálat elvégzése. Azonban az Adatkezelő döntése alapján lehetőség van adatvédelmi hatásvizsgálat elvégzésére, amennyiben az adatkezelés vonatkozásában teljesül a (4) bekezdés a)-i) pontjaiban foglalt valamely feltétel.

(6) Nem kell adatvédelmi hatásvizsgálatot végezni, amennyiben az adatkezelés vonatkozásában teljesül valamelyik alábbi feltétel:
a) az adatkezelés valószínűsíthetően nem jár magas kockázattal az érintettek jogaira és szabadságaira nézve;
b) az adatkezelés a jellegét, hatókörét, körülményét és céljait tekintve nagyon hasonlít olyan adatkezelésre, amelyről már készült adatvédelmi hatásvizsgálat;
c) az adatkezelést a NAIH vagy valamely uniós tagállam adatvédelmi felügyeleti hatósága korábban ellenőrizte, és azóta nem történt változás a körülményekben;
d) az adatkezelés – a GDPR 6. cikk (1) bekezdés c) vagy e) pontja alapján – a Hivatalra vonatkozó jogi kötelezettség teljesítéséhez szükséges, az adatkezelés közérdekű vagy az Adatkezelőre ruházott közhatalmi jogosítvány gyakorlása keretében végzett feladat végrehajtásához szükséges –, a jog szabályozza az adott adatkezelési műveletet, és az említett jogalap megállapítása során már készült adatvédelmi hatásvizsgálat;
e) az adatkezelés szerepel az adatkezeléseknek a GDPR 35. cikk (5) bekezdése alapján a NAIH által összeállított jegyzékében.[90]

(7) Jelen rendelkezések alkalmazásában módszeres megfigyelésnek minősül az érintett megfigyelése, nyomon követése vagy ellenőrzése, ha az:
a) adott rendszer szerint fordul elő;
b) előre megszervezett, szervezett vagy módszeres;
c) az adatkezelésre vonatkozó általános terv részeként történik; vagy
d) egy adott stratégia részeként végzik.

(8) Jelen rendelkezések alkalmazásában kiszolgáltatott helyzetben lévő érintettnek minősül az

[90] Az említett jegyzék közzétételére még nem került sor.

érintett, ha közte és a Hivatal közötti kapcsolatban egyenlőtlen helyzet alakul ki, különösen, ha az érintett:
a) gyermek;
b) munkatárs;
c) a lakosság különleges védelmet igénylő, kiszolgáltatottabb helyzetben lévő rétegei közé (mentális betegségben szenvedők, menedékkérők, idősek, betegek stb.) tartozik.

(9) Jelen rendelkezések alkalmazásában nagyszámú adatkezelésnek minősül, amennyiben:
a) az érintettek száma,
b) a kezelt adatok mennyisége vagy az adatfajták köre,
c) az adatkezelési tevékenység időtartama vagy állandó jellege, vagy
d) az adatkezelési tevékenység földrajzi kiterjedése
alapján feltételezhető a személyes adatok nagy számban történő kezelése.

(10) Jelen rendelkezések alkalmazásában joghatással bíró döntésnek minősül az, ha a döntés befolyásolja az érintett törvényes vagy szerződésen alapuló jogait, illetve jogállását.

(11) Jelen rendelkezések alkalmazásában a döntés hasonlóképpen jelentős mértékben érinti az érintettet, amennyiben az:
a) jelentősen befolyásolja az érintett körülményeit, viselkedését vagy választásait;
b) hosszan tartó vagy tartós hatást gyakorol az érintettre;
c) a döntés az érintett személyek kirekesztéséhez vagy hátrányos megkülönböztetéséhez vezethet.

(12) Jelen rendelkezések alkalmazásában automatizált döntéshozatalnak minősül minden olyan eljárás, amelynek keretében technológiai eszközök segítségével, emberi beavatkozás nélkül hoznak döntéseket.

VIII.2. Az adatvédelmi hatásvizsgálatban résztvevő személyek

(1) Az adatvédelmi hatásvizsgálatban az alábbi személyek részvétele kötelező:
a) az adatkezeléssel érintett szervezeti egység vezetője vagy az általa kijelölt munkatárs;
b) az adatvédelmi tisztviselő.

(2) Az adatvédelmi hatásvizsgálatban szükség esetén részt vesznek:
a) az informatikai terület vezetője vagy az általa kijelölt munkatársa;
b) egyéb szervezeti egységek vezetői vagy az általuk kijelölt munkatársak;
c) az információbiztonsági vezető;
d) adatfeldolgozó vagy annak kijelölt munkavállalója;
e) külső szakértő vagy tanácsadó
f) az érintettek vagy képviselőik.

(3) Az adatkezelő szervezeti egység vezetője vagy az általa kijelölt munkatárs köteles:
a) előkészíteni az adatvédelmi hatásvizsgálatot, különös tekintettel a szükséges adatok, információk és tények összegyűjtésére, rendszerezésére;

b) az adatvédelmi hatásvizsgálatot lefolytatni, amelyhez szükség esetén az adatvédelmi tisztviselő közvetítésével igénybe veheti a Hivatallal szerződésben álló külső szakértő vagy tanácsadó segítségét;
c) az adatvédelmi hatásvizsgálat elvégzését megelőzően kikérni az adatvédelmi tisztviselő véleményét, illetve tanácsát, továbbá
d) biztosítani, hogy az adatvédelmi tisztviselő ellenőrizhesse az adatvédelmi hatásvizsgálat lefolytatását, illetve annak eredményét.

(4) Az adatkezelő szervezeti egység vezetője vagy az általa kijelölt munkatárs az adatvédelmi hatásvizsgálat lefolytatása során bármikor tanácsot, információt és felvilágosítást kérhet az adatvédelmi tisztviselőtől az adatvédelmi hatásvizsgálattal összefüggésben, továbbá köteles minden szükséges információt és felvilágosítást megadni az adatvédelmi tisztviselő részére az adatvédelmi hatásvizsgálat lefolytatásával kapcsolatban.

(5) Az adatvédelmi tisztviselő köteles:
a) értékelni az adatvédelmi hatásvizsgálat lefolytatásának szükségességét;
b) dokumentálni az adatvédelmi hatásvizsgálat szükségességének értékelését;
c) kérésre szakmai tanácsot adni az adatvédelmi hatásvizsgálat lefolytatását illetően;
d) nyomon követni és ellenőrizni az adatvédelmi hatásvizsgálat lefolytatását és eredményét;
e) véleményezni az adatvédelmi hatásvizsgálat lefolytatását és eredményét,
f) megőrizni az adatvédelmi hatásvizsgálati dokumentációt.

VIII.3. Az adatvédelmi hatásvizsgálat elvégzésének ideje

(1) Az adatvédelmi hatásvizsgálatot a tervezett adatkezelést megelőzően, legkésőbb a személyes adatok kezelésének megkezdésének időpontjáig el kell végezni.

(2) Annak érdekében, hogy az Adatkezelő eleget tudjon tenni az (1) bekezdésben írt kötelezettségének, az adott tevékenység tervezése során a lehető leghamarabb biztosítani kell annak lehetőségét, hogy az adatvédelmi tisztviselő megvizsgálhassa a tervezett adatkezelési műveletet vagy műveleteket.

(3) Amennyiben az adatvédelmi hatásvizsgálat elvégzése indokolt, azt az adatvédelmi tisztviselő javaslatát követő lehető leghamarabb el kell kezdeni. Az adatvédelmi hatásvizsgálat megkezdésének idejéről tájékoztatni kell az adatvédelmi tisztviselőt.

(4) Amennyiben az adatvédelmi hatásvizsgálat megkezdésének időpontjában nem ismert még minden adatkezelési művelet, a már ismert műveletek tekintetében kell az adatvédelmi hatásvizsgálatot folytatni. A később ismertté váló adatkezelési műveleteket folyamatosan kell az adatvédelmi hatásvizsgálatba bevonni.

(5) Az adatvédelmi tisztviselő köteles rendszeresen, legfeljebb évente egyszer ellenőrizni a korábban elvégzett adatvédelmi hatásvizsgálatok hatálya alá tartozó adatkezeléseket annak megállapítása érdekében, hogy bekövetkezett-e az adatkezelésben olyan változás, amely az adatvédelmi hatásvizsgálat megismétlését teszi szükségessé.

(6) Amennyiben a korábban elvégzett adatvédelmi hatásvizsgálatok hatálya alá tartozó adatkezelés körülményeiben jelentős változás áll be, az adatvédelmi tisztviselő javaslatára az adatvédelmi hatásvizsgálatot vagy annak egy részét meg kell ismételni, és annak alapján a korábban elvégzett adatvédelmi hatásvizsgálat dokumentációját – szükség esetén – ki kell egészíteni vagy módosítani kell.

VIII.4. Az adatvédelmi hatásvizsgálat módszertana

(1) Az adatvédelmi hatásvizsgálatnak legalább a következő elemekre kell kiterjednie:
   a) az adatkezelés módszeres leírása;
   b) az adatkezelés szükségességének és az arányosságának értékelése;
   c) az érintett jogait és szabadságait érintő kockázatok, valamint az azok kezelésére tett intézkedések;
   d) az érintettek (érdekeltek) bevonására vonatkozó információk.

(2) A Hivatal által végzett adatvédelmi hatásvizsgálatnak minden esetben tartalmaznia kell az (1) bekezdésben foglalt tartalmi elemeket, a jelen pontban részletezett módszertannak megfelelően. Az egyes módszertani elemek részletezettségét, kialakítását az adott adatkezelés körülményeihez kell igazítani.

(3) Amennyiben kérdés merül fel az adatvédelmi hatásvizsgálat módszertanának egyes elemeivel kapcsolatban, az érintett szervezeti egység vezetője köteles az adatvédelmi tisztviselő véleményét kikérni.

(4) A hatásvizsgálat keretében be kell mutatni a tervezett adatkezelést. Ennek során ismertetni kell:
   a) az adatkezelést;
   b) az adatkezeléshez kapcsolódó felelősségi viszonyokat;
   c) az adatkezelésre alkalmazandó szabványokat.

(5) Az adatkezelés ismertetése során be kell mutatni:
   a) az adatkezelés célját vagy céljait;
   b) az adatkezelés jogalapját;
   c) az adatkezelés során kezelendő személyes adatokat;
   d) az adatkezelés során kezelendő személyes adatok forrását;
   e) az érintettek kategóriáit;
   f) a személyes adatok tárolásának időtartamát;
   g) az adatkezelés egyéb jellemzőit.

(6) Az adatvédelmi hatásvizsgálat keretében meg kell vizsgálni, hogy az adatkezelés vonatkozásában meghatározásra kerültek-e a GDPR betartására irányuló alábbi intézkedések:
   a) az adatkezelés arányosságát és szükségességét előmozdító intézkedések;
   b) az érintettek jogait támogató intézkedések;
   c) garanciális jelentőségű kiegészítő intézkedések.

(7) Az adatvédelmi hatásvizsgálat keretében meg kell vizsgálni, hogy az érintett jogait és szabadságait érintő kockázatok kezelése megfelelő-e, azaz az adatkezelés vonatkozásában:
   a) megtörtént-e a kockázatok forrásának, jellegének, egyediségének és súlyosságának felmérése az érintettek szemszögéből;
   b) a kockázatok orvoslására irányuló intézkedések meghatározásre kerültek-e.

(8) Az adatvédelmi hatásvizsgálat során részletesen fel kell mérni, értékelni kell és be kell mutatni az adatkezelés által az érintett jogait és szabadságait érintő kockázatokat – elsősorban, de nem kizárólagosan – az alábbi eseményekre tekintettel:
   a) a személyes adatokhoz való jogosulatlan hozzáférés;
   b) a személyes adatok véletlen vagy jogellenes megváltoztatása;
   c) a személyes adatok elvesztése.

(9) A (8) bekezdésben említett események vonatkozásában elemezni kell a kockázatok forrását és valószínűségét. Ebben a vonatkozásban vizsgálandók:
   a) lehetséges belső – véletlen vagy szándékos – magatartások;
   b) lehetséges külső – véletlen vagy szándékos – magatartások;
   c) a kiszolgáló környezet.

(10) A kiszolgáló környezet értékelése során az alábbi tényezőket kell vizsgálni:
   a) az adatkezelés eszközei (papír alapú vagy automatizált módszerekkel történő adatkezelés);
   b) az alkalmazott rendszerek (levelező rendszer, adathordozó stb.);
   c) a kiszolgáló környezet biztonságát védő intézkedések (pl. titkosítás, álnevesítés, tűzfal);
   d) a kiszolgáló környezet ellenállóképessége;
   e) a kockázatok elhárítása érdekében előzetesen tett intézkedések hatékonysága;
   f) a kockázatok bekövetkeztét lehetővé tevő tényezők;
   g) a kockázatok bekövetkeztét befolyásoló egyéb tényezők;
   h) a rendszerszerű működés helyreállításának valószínűsége.

(11) A kockázatforrások alapján a kockázatokat valószínűség szerint kell osztályozni az alábbi szerint:
   a) *csekély valószínűség*: csekély valószínűségűnek minősül az a kockázat, amely csak kivételesen esetben következhet be a fennálló ismeretek alapján;
   b) *korlátozott valószínűség*: korlátozott valószínűségűnek minősül az a kockázat, amely az esetek kis részében következhet be. Ez esetben – a fennálló ismeretek alapján – a kockázatforrások a személyes adatok kezelésére szolgáló eszközöket kihasználó alacsony veszélyt jelentenek;
   c) *nagy valószínűség*: nagy valószínűségűnek minősül az a kockázat, amely az esetek nagy részében bekövetkezhet. Ez esetben – a fennálló ismeretek alapján – a kockázatforrások a személyes adatok kezelésére szolgáló eszközöket kihasználó veszélyt jelentenek;
   d) *maximális valószínűség*: maximális valószínűségűnek minősül az a kockázat, amely csak kivételes esetben nem következik be. Ez esetben – a fennálló ismeretek alapján – a kockázatforrások a személyes adatok kezelésére szolgáló eszközöket kihasználó kiemelt veszélyt jelentenek.

(12) A (8) bekezdésben említett események vonatkozásában figyelembe kell venni a kockázatok hatásait és azok súlyosságát. A kockázatok érintettre gyakorolt hatásai szempontjából figyelembe vehető tényezők:

a) a kezelt személyes adatok;
b) a kockázat következményei.

(13) A kezelt személyes adatok szempontjából vizsgálandók:

a) a személyes adatok kategóriái, különös tekintettel a különleges adatokra;
b) személyes adatok száma;
c) érintettek kategóriái, különös tekintettel az érintettek esetleges kiszolgáltatott helyzetére;
d) az érintettek azonosíthatósága;
e) az érintettek száma.

(14) A következmények szempontjából vizsgálandó az esetleges fizikai károk vagy veszélyek, illetve a vagyoni és nem vagyoni károk. A kockázatok hatásait azok súlyossága szerint kell osztályozni az alábbi szerint:

a) *elhanyagolható következmények/hatás*: elhanyagolható a következmény, ha annak bekövetkezte esetén az érintettek nem szenvednek kárt, vagy néhány kellemetlenséget kell csupán elviselniük, amelyen könnyen túlteszik magukat. Ide tartozhatnak például a jelentéktelen időveszteség, a kéretlen üzenetek fogadása, valamint az enyhébb erkölcsi vagy lelki következmények;
b) *korlátozott következmények/hatás*: korlátozott a következmény, ha az érintettek jelentős kellemetlenségeket tapasztalhatnak, de néhány nehézség ellenére túlteszik magukat rajtuk. Ide tartozhatnak például kisebb anyagi kellemetlenségek, a közigazgatási vagy kereskedelmi szolgáltatások igénybevételétől való eltiltás, az olyan kéretlen üzenetek érkezése, ami árt az érintettek jóhírnevének, valamint a kisebb erkölcsi sérelmek;
c) *jelentős következmények/hatás*: jelentős a következmény, ha az érintettek komoly következményekkel szembesülhetnek, amelyeken ugyan túlteszik magukat, de jelentős és valós nehézségek árán. Ide tartozhatnak például a jelentősebb fizikai vagy pszichikai következmények, a jelentősebb anyagi következmények, valamint a jelentősebb erkölcsi következmények;
d) *súlyos következmények/hatás:* súlyos a következmény, ha érintettek komoly, akár maradandó következményekkel is szembesülhetnek, amelyeken nem tudják túltenni magukat. Ide tartozhatnak például a súlyos fizikai vagy pszichikai következmények, a súlyos anyagi következmények, valamint a súlyos erkölcsi következmények.

(15) Kárnak minősül:

a) ha az adatkezelésből hátrányos megkülönböztetés, személyazonosság-lopás vagy személyazonossággal való visszaélés, pénzügyi veszteség, a jó hírnév sérelme, a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülése, az álnevesítés engedély nélkül történő feloldása, vagy bármilyen jelentős gazdasági vagy szociális hátrány fakadhat;
b) ha az érintettek nem gyakorolhatják jogaikat és szabadságaikat, vagy nem rendelkezhetnek saját személyes adataik felett.

(16) Az adatvédelmi hatásvizsgálat során részletesen fel kell mérni, értékelni kell és be

kell mutatni a kockázatok bekövetkeztének valószínűségét és hatásainak súlyosságát csökkentő – meglévő és tervezett – védelmi intézkedéseket a (8) bekezdésében említett események vonatkozásában. A szükséges, egyben a kockázattal arányos védelmi intézkedések kiválasztásába be kell vonni a Hivatal információbiztonsági vezetőjét.

(17) A (16) bekezdésben említett intézkedések lehetnek:
a) logikai védelmi intézkedések;
b) fizikai védelmi intézkedések;
c) adminisztratív védelmi intézkedések.

(18) Logikai védelmi intézkedés lehet különösen:
a) titkosítás;
b) anonimizálás;
c) az adatok különválasztása;[91]
d) logikai hozzáférés szabályozás;
e) naplózás;
f) archiválás;
g) papír alapú dokumentumok biztonsága;
h) adatminimalizálás.[92]

(19) Fizikai védelmi intézkedés lehet különösen:
a) üzembiztonsági intézkedések;
b) rosszindulatú szoftverek kiszűrése;
c) a munkaállomások kezelése;
d) webhelybiztonság;[93]
e) biztonsági mentések;
f) hardver karbantartás;
g) adatfeldolgozók igénybevétele során alkalmazandó követelmények;
h) hálózatbiztonság;[94]
i) fizikai hozzáférésvédelem;[95]
j) hálózati tevékenységek megfigyelése;[96]
k) hardverbiztonság;[97]

[91] Az adatok különválasztásának minősül az, ha a kezelt személyes adatok egyes kategóriáit, különös tekintettel az azonosító adatokra, elválasztva kerülnek tárolásra és felhasználva.
[92] Adatminimalizálásnak minősül különösen a személyes adatok szűrése, a felesleges személyes adatok eltávolítása, a személyes adatok érzékenységének csökkentése átalakítás révén, a személyes adatok személyazonosításra alkalmas jellegének csökkentése, az adatfelhalmozás korlátozása, a személyes adatokhoz való hozzáférés korlátozása.
[93] Webhelybiztonsági intézkedésnek minősül különösen az ANSSI webhelybiztonsági ajánlásainak alkalmazása.
[94] Hálózatbiztonsági intézkedésnek minősül különösen a tűzfal-, a behatolásérzékelő, illetve az egyéb aktív vagy passzív biztonsági rendszer.
[95] Fizikai hozzáférésvédelmi intézkedésnek minősül a személyes adatok kezelésére szolgáló helyiségek, épületek fizikai védelme, és az annak érvényre juttatását szolgáló belső eljárás.
[96] Hálózati tevékenységek megfigyelésének minősül behatolásészlelő és -megelőző rendszerek által végzett ellenőrzés, illetve a kibertámadás-gyanús tevékenységek észlelése.
[97] Hardverbiztonsági intézkedésnek minősül a szerverek és a munkaállomások fizikai biztonságát befolyásoló védelmi intézkedés.

l) a nem emberi eredetű kockázatokkal szembeni védelem.[98]

(20) Adminisztratív védelmi intézkedés lehet különösen:
a) szervezeti intézkedések;[99]
b) a belső eljárásrendek szabályozása;
c) az adatvédelmi kockázatok kezelése;
d) a beépített adatvédelem érvényesítése;
e) a személyes adatokkal kapcsolatos jogsértések kezelése;
f) a humánerőforrás-menedzsment;[100]
g) a harmadik felekkel való kapcsolatok szabályozása;
h) a belső felügyelet.

(21) Az adatvédelmi hatásvizsgálat során részletes intézkedési tervet kell készíteni, amely tartalmazza:
a) a kockázatok bekövetkeztének valószínűségét és hatásainak súlyosságát csökkentő, tervezett intézkedéseket;
b) az intézkedések elvégzéséért felelős szervezeti egységet, illetve felelős személyt;
c) az intézkedések elvégzésének határidejét.

(22) Az adatvédelmi tisztviselő köteles véleményezni az adatvédelmi hatásvizsgálat elvégzését és eredményét, beleértve az intézkedési terv tervezetét is. Az Adatkezelő az adatvédelmi hatásvizsgálat elvégzése során köteles figyelembe venni az adatvédelmi tisztviselő véleményét, az abban foglalt intézkedéseket – főszabály szerint – haladéktalanul meg kell hozni. Kizárólag dokumentált módon és megfelelő indokolással ellátott vélemény alapján lehet az adatvédelmi tisztviselő javaslataitól eltérni.

VIII.5. Az érdekeltek bevonása

(1) Az adatvédelmi hatásvizsgálat elvégzésébe lehetőség szerint be kell vonni az érdekelt személyeket vagy személyek csoportját (VIII.2. (2) bekezdés d) és f) pontjai).

(2) Az adatkezeléstől függően elektronikus úton vagy papír alapon ki kell kérni az érintettek vagy a képviselőik [101] véleményét az adatvédelmi hatásvizsgálat eredményével kapcsolatban. Az Adatkezelő köteles az érintettek vagy képviselőik véleményét összesíteni, és az indokolt intézkedéseket megtenni. Amennyiben az Adatkezelő nem kíván az érintettek vagy képviselőik véleményének megfelelő intézkedéseket tenni, azt köteles dokumentált módon megindokolni. Az érintettekkel vagy képviselőiekkel való

[98] Nem emberi eredetű kockázatokkal szembeni védelmi intézkedésnek minősül különösen a tűzvédelmi eszközök, a tűzjelző és tűzoltó berendezések, a vízkár elleni védelem eszközei, az áramellátás ellenőrzésére szolgáló eszközök és a kármentesítés eszközei.

[99] Szervezeti intézkedés lehet különösen az adatvédelmi tisztviselő, illetve személy vagy olyan szervezeti egység alkalmazása, aki vagy amely felelős az adatvédelmi jogszabályok és egyéb előírások érvényesítéséért.

[100] Humánerőforrás-menedzsmentnek minősül különösen az adatvédelmi ismereteket bővítő és adatvédelmi tudatosságot növelő mechanizmus, oktatás, tréning.

[101] Az érintettek képviselőinek minősülnek az egyének nagyobb csoportjait képviselő szervezetek, különös tekintettel a munkaügyi és társadalmi érdekképviseleti szervezetekre.

kapcsolattartás során biztosítani kell a szükséges személyes adatok kezelésének jogszerűségét. Az érintettek vagy képviselőik véleményének kikérését csak abban az esetben lehet elhagyni, ha az:

a) az Adatkezelő hivatali érdekeinek védelme, titkossága érdekében szükséges;
b) a közérdek védelme érdekében szükséges;
c) az adatkezelési műveletek biztonságának védelme érdekében szükséges;
d) egyéb okból aránytalan vagy kivitelezhetetlen lenne.

(3) Az adatfeldolgozó segíti az Adatkezelőt az adatvédelmi hatásvizsgálat lefolytatásában. Az adatfeldolgozó köteles:

a) az adatvédelmi hatásvizsgálat lefolytatásához szükséges információkat az Adatkezelő által megjelölt módon és határidőben rendelkezésre bocsátani;
b) az adatvédelmi hatásvizsgálat lefolytatásához szükséges dokumentációt az Adatkezelő által megjelölt módon és határidőben rendelkezésre bocsátani;
c) minden olyan intézkedést meghozni, amely az adatvédelmi hatásvizsgálat sikerességéhez szükséges.

VIII.6. Előzetes konzultáció

(1) Amennyiben az adatvédelmi hatásvizsgálat keretében meghozott intézkedések után fennmaradó kockázatok továbbra is magasak az érintett jogaira és szabadságaira nézve, az Adatkezelő a személyes adatok kezelésének megkezdését megelőzően köteles konzultálni a NAIH-hal. Az előzetes konzultáció kötelezettsége fennállhat abban az esetben is, amennyiben azt a hatályos jogszabályok az Adatkezelő számára előírják.

(2) Az előzetes konzultáció keretében az Adatkezelő tájékoztatja a NAIH-ot:

a) a saját, valamint az adatkezelésben esetlegesen részt vevő közös adatkezelők és adatfeldolgozók feladatköreiről,
b) a tervezett adatkezelés céljairól és módjairól;
c) az érintettek jogainak és szabadságainak védelmében hozott intézkedésekről és garanciákról;
d) az adatvédelmi tisztviselő elérhetőségeiről;
e) az adatvédelmi hatásvizsgálatról;
f) a NAIH által kért minden egyéb információról.

(3) Az Adatkezelő a NAIH előzetes konzultáció során nyújtott tanácsainak, illetve a GDPR 58. cikke szerinti hatáskörei keretében kiadott állásfoglalásában foglaltak megfelelően köteles:

a) módosítani vagy kiegészíteni az adatvédelmi hatásvizsgálatot;
b) módosítani az adatkezelést;
c) módosítani a vonatkozó adatkezelési tájékoztatót vagy a jelen Szabályzatot.

VIII.7. Dokumentálás és hozzáférés

(1) Az adatvédelmi hatásvizsgálati dokumentáció részét képezi:

a) az adatvédelmi hatásvizsgálat szükségességének értékelése;
b) az adatvédelmi hatásvizsgálati jelentés;

c) az előzetesen konzultációra vonatkozó jelentés.

VIII.7.1.Az adatvédelmi hatásvizsgálat szükségességének értékelése

(1) Az Adatkezelő az adatvédelmi hatásvizsgálat szükségességét a Szabályzat 5. számú mellékletében foglalt dokumentumban köteles rögzíteni.
(2) Az adatvédelmi hatásvizsgálat szükségességének értékelésében fel kell tüntetni:
   a) az adatvédelmi hatásvizsgálat elvégzésének indokát (indokait);
   b) az értékelés azonosítószámát;
   c) az értékelést végző személy nevét, szervezeti egységét és beosztását, aláírását;
   d) az értékelésbe bevont további személyek nevét, szervezeti egységét és beosztását, aláírását;
   e) az értékelés elvégzésének idejét.

VIII.7.2. Az adatvédelmi hatásvizsgálati jelentés

(1) Az Adatkezelő az adatvédelmi hatásvizsgálat dokumentálása céljából alkalmazza:
   a) a NAIH által közzétett hatásvizsgálati szoftvert; vagy
   b) a Szabályzat 6. számú mellékletében foglalt adatvédelmi hatásvizsgálati jelentés mintát.

(2) Az említett lehetőségek mindegyike megfelelő eljárásnak minősül, az Adatkezelő a választott módszert nem köteles indokolni.

(3) Az adatvédelmi hatásvizsgálati jelentéshez csatolni kell azokat a mellékleteket, amelyek a benne foglalt tényeket támasztják alá. Az adatvédelmi hatásvizsgálati jelentéshez csatolni kell a VIII.4. pont (22) bekezdése és a VIII.5. pont (2)-(3) bekezdései szerinti véleményeket és dokumentumokat.

VIII.7.3. Az előzetes konzultációra vonatkozó jelentés

(1) Az Adatkezelő az előzetes konzultációval kapcsolatban a Szabályzat 7. számú mellékletében foglalt jelentést készít. Az előzetesen konzultációra vonatkozó jelentésben fel kell tüntetni:
   a) az adatvédelmi hatásvizsgálat azonosítószámát;
   b) a jelentést készítő személy nevét, szervezeti egységét és beosztását, aláírását;
   c) a jelentés készítésébe bevont további személyek nevét, szervezeti egységét és beosztását, aláírását;
   d) az adatvédelmi tisztviselő nevét és aláírását;
   e) a jelentés készítésének idejét.

VIII.7.4. Az adatvédelmi hatásvizsgálati dokumentáció hozzáférhetősége

(1) Az adatvédelmi hatásvizsgálat eredménye – főszabály szerint – nem nyilvános.

(2) Az Adatkezelő mérlegelése alapján az adatvédelmi hatásvizsgálat összefoglalóját:
   a) az érintettek nagyobb csoportja számára hozzáférhetővé teheti, amennyiben az adatkezelés a személyek megfelelő módon meghatározott körét érinti;

b) nyilvánosságra hozhatja, amennyiben az adatkezelés a nyilvánosságot érinti.

(3) Az Adatkezelő az adatvédelmi hatásvizsgálat összefoglalójának hozzáférhetővé tételére vagy nyilvánosságra hozatalára vonatkozó döntését indokolással köteles ellátni. Az összefoglaló nem tartalmazhat olyan információkat, amely a személyes adatok védelmét vagy biztonságát, illetve az Adatkezelő vagy harmadik fél méltányolható érdekét sértené, különös tekintettel a biztonsági kockázatokra vonatkozó adatokra, az üzleti titkokra és a bizalmas adatokra.

IX. AZ ADATKEZELÉS SPECIÁLIS ESETEI

IX.1. A munkatársak adatainak kezelése

(1) Az Adatkezelő valamennyi munkaviszonyt vagy kormányzati szolgálati jogviszonyt létesítő személyt köteles tájékoztatni a munkavégzéssel kapcsolatos adatkezelésekről. A tájékoztatás megismeréséről az érintett írásban nyilatkozik, amennyiben annak igazolása nem a Szabályzat V.1. pontja (5) bekezdésének b) pontja alapján történik.

(2) A bér- és munkaügyi nyilvántartás adatai a foglalkoztatott jogviszonyával kapcsolatos tények megállapítására, a besorolási követelmények igazolására, bérszámfejtésre, társadalombiztosítási ügyintézésre és statisztikai adatszolgáltatásra használhatók fel.

(3) A bér- és munkaügyi nyilvántartás kezelését – a feladatkörük ellátásához szükséges mértékben – az Adatkezelő humánpolitikai ügyekért felelős munkatársai és a bérszámfejtők végzik.

(4) Az Adatkezelő által végzett, a munkatársai személyes adataira vonatkozó adatkezeléssel kapcsolatos feladat- és hatásköröket, továbbá annak körülményeit és jellemzőit az Adatkezelő közszolgálati adatvédelmi szabályzata tartalmazza.

IX.2. Manuálisan kezelt személyes adatok

(1) Az Adatkezelőnek az adatok biztonságát szolgáló intézkedések meghatározásakor és alkalmazásakor tekintettel kell lennie a technika mindenkori fejlettségére. Több lehetséges adatkezelési megoldás közül azt kell választania, amely a személyes adatok magasabb szintű védelmét biztosítja, kivéve, ha az aránytalan nehézséget jelentene.

(2) A manuálisan kezelt személyes adatok biztonsága érdekében az alábbi intézkedéseket kell meghozni és végrehajtani:

a) az irattári kezelésbe vett iratokat jól zárható, száraz, tűzvédelmi és vagyonvédelmi berendezéssel ellátott helyiség(ek)ben kell elhelyezni;
b) a folyamatos aktív kezelésben lévő iratokhoz csak az illetékes ügyintézők férhetnek hozzá, egyebekben az iratokat biztonságosan elzárva kell tartani,

c) az adatkezelések iratainak archiválását rendszeresen el kell végezni, az archivált iratokat a vonatkozó előírásoknak megfelelően kell szétválogatni és irattári kezelésbe venni.

(3) A papíralapú adatkezelés – beleértve az irattározást is –, szabályait az Adatkezelő iratkezelési szabályzata, az (2) bekezdés b) pontja szerinti helyiségek, illetve szekrények kulcsához való hozzáférés rendjét a beléptetésre és benntartózkodásra vonatkozó szabályzat, továbbá az információbiztonsági szabályzat tartalmazza.

IX.3. Elektronikusan kezelt személyes adatok

(1) Amennyiben az Adatkezelő olyan elektronikus rendszerben kezel személyes adatot, amelybe csak az arra felhatalmazott, a rendszerhez hozzáférési jogosultsággal (pl. felhasználónév és jelszó) rendelkező munkatársa léphet be, úgy az illetékes munkatársnak egyéni, titkos jelszóval vagy ahhoz köthető módon kell bejelentkeznie a rendszerbe. Az adatkezelés befejeztével a rendszerből ki kell lépni.

(2) Az adatvédelmi incidensek elkerülése érdekében minden munkatárs kötelessége az egyéni jelszavának védelme, továbbá szabályzatokkal összhangban lévő kezelése.

(3) Az adatkezelésre használt számítógépek adatbevitelre, lekérdezésre alkalmas (lezárás nélküli) állapotban történő, felügyelet nélkül hagyása tilos, azt minden esetben le kell zárni, amennyiben azon az érintett munkatárs nem dolgozik.

(4) Az Adatkezelő kizárólag olyan adatkezelési rendszert alkalmazhat, amely a rendszerbe történt belépést regisztrálja, illetve a rögzített adatokról megállapítható, hogy az adatrögzítés ki által és milyen időpontban történt.

(5) Az elektronikus adatkezelés részletes szabályait az Adatkezelő információbiztonsági szabályzata tartalmazza.

IX.4. A hivatali munkatársakat és egyes adatfeldolgozókat vagy munkatársaikat[102] érintő speciális szabályok (beleértve az ellenőrzéseket is)

IX.4.1. Postai küldemények

(1) A Hivatal címére érkezett postai küldeményt, amennyiben feltételezhető, hogy az személyre szóló – például „s.k.” jelzéssel lett ellátva –, először az érintett személynek kell átadni. Amennyiben ilyen tartalmú levél mégis felbontásra kerül, akkor azt vissza kell zárni, és a felbontás dátumát, valamint a levél tartalmának megismerő személy nevét fel kell rajta tüntetni.

(2) A postai küldemények kezelésének részletes szabályait az iratkezelési szabályzat tartalmazza.

[102] L. a hatályba léptető elnöki utasítás 2. § (1)-(2) bekezdéseit.

IX.4.2.Telefonok használatának ellenőrzése

(1) Az Adatkezelő által a munkatársak és egyes adatfeldolgozók vagy munkatársaik (a továbbiakban jelen IX. fejezet tekintetében: hivatali feladatot ellátó személy) rendelkezésére bocsátott vezetékes- és mobiltelefonokat elsősorban hivatalos célból lehet használni.

(2) Amennyiben az Adatkezelő, mint munkáltató vagy adatkezelő, a munkáltatói vagy adatkezelői ellenőrzéshez való jogára hivatkozva ellenőrizni kívánja a hivatali feladatot ellátó személy telefonhasználatát, akkor ez kizárólag a hivatalos használatra terjedhet ki, az esetleges magáncélú használat ellenőrzése tilos. Nem minősül a magáncélú használat ellenőrzésének, amennyiben az ellenőrzés a hivatali adatvagyon védelméhez, illetve sérelme lehetőségéhez kapcsolódik. Az adatkezelés jogalapja a GDPR 6. cikk (1) bekezdésének e) pontja, tekintettel arra, hogy az ellenőrzés az Adatkezelő közfeladatának megfelelő ellátása érdekében történik. Az ellenőrzést az Adatkezelő által elkészített érdekmérlegelési teszt eredménye alapozza meg, amely tartalmazza az adatkezelésre vonatkozó szükségesség-arányosság elvének érvényesülését. Az ellenőrzésre jogosult munkáltatói jogkör gyakorló vagy hivatali kapcsolattartó (a továbbiakban jelen IX. fejezet tekintetében: ellenőrzést végző személy) köteles a hivatali feladatot ellátó személyt dokumentált módon, a tényleges ellenőrzés megkezdése előtt tájékoztatni, hogy mely, pontosan meghatározott érdek miatt kerül sor az ellenőrzésre, illetve annak körülményeiről.

(3) Az ellenőrzés során főszabály szerint az Adatkezelő biztosítja az eljárás lefolytatásához szükséges munkatársak jelenlétét, illetve az ellenőrzés során a fokozatosság elvének betartásával jár el. Amennyiben az ellenőrzés részben vagy egészben a hivatali feladatot ellátó személyhez köthető híváslista ellenőrzéséhez kapcsolódik, akkor a távközlési szolgáltatótól megkért részletes híváslistát az Adatkezelő átadja a hivatali feladatot ellátó személy részére annak érdekében, hogy az esetleges magáncélú hívásait kiválogassa. Ezt a híváslistát – a távközlési szolgáltatóval kapcsolatot tartó munkatárson kívül – kizárólag a hivatali feladatot ellátó személy ismerheti meg.

(4) A hivatali feladatot ellátó személy a híváslistából a magánhívásai telefonszámát felismerhetetlenné teszi olyan módon, hogy azok utolsó három számjegyét törli, majd átadja azt az ellenőrzést végző személynek.

(5) A telefonhasználat ellenőrzéséről jegyzőkönyvet kell felvenni.

(6) Abban az esetben, ha a hivatali feladatot ellátó személy bármely okból akár csak ideiglenesen (pl. javítás céljára) is visszaadja az általa használt mobiltelefont – akár a jogviszony fennállása vagy az adatfeldolgozói szerződés hatálya alatt, akár annak megszűnésekor –, gondoskodnia kell arról, hogy az eszközön tárolt esetleges magánjellegű adatait – így pl. telefonszámokat, üzeneteket, képeket, filmeket, egyéb formájú és tartalmú adatokat – olyan módon/helyre mentse, ahol azokat a Hivatal más munkatársa nem éri el; majd azokat a készülékről visszaállíthatatlan módon törölnie kell (elsősorban a gyári beállítások visszaállításával). A hivatali feladatot ellátó személy köteles a magánjellegű tartalmak eltávolításáról jelen Szabályzat 8. számú mellékletében foglaltak szerinti

tartalommal írásbeli nyilatkozatot tenni.

(7) A készüléket csak azt követően lehet átadni harmadik személy részére, ha az eszközkiadásért felelős személy annak gyári beállításai visszaállításával vagy más módon biztosítja, hogy azon magánjellegű adat már nem lelhető fel. Az eljárást lefolytató személyt az (5) bekezdésben írtak ellenére esetlegesen megismert magánjellegű adatok tekintetében titoktartási kötelezettség terheli, azt harmadik személy részére nem adhatja át, rá vonatkozó információt nem közölhet.

IX.4.3. E-mail postafiók használatának és ellenőrzésének adatvédelmi szabályai

(1) Az Adatkezelő a feladatellátás céljára rendelkezésre bocsátott (saját névre szóló vagy funkcionális) e-mail postafiókot hivatalos célból adja át a hivatali feladatot ellátó személynek, az e-mail fiók magáncélra nem használható.

(2) Az Adatkezelő informatikai rendszereinek stabil működéséért felelős informatikai főosztályvezető jogosult az egyes e-mail postafiókok tárolókapacitását központilag meghatározni, az e-mailhez csatolt fájlok méretét és formátumát korlátozni, továbbá köteles az ezekkel kapcsolatos információkról a hivatali feladatot ellátó személyeket tájékoztatni, illetve az azok alapjául szolgáló indokokat megadni. E beállításokat, továbbá a Hivatal által meghatározott további felhasználói szabályokat a hivatali feladatot ellátó személyek kötelesek betartani.

(3) A hivatali feladatot ellátó személy további – nem hivatali – e-mail postafiókokat a munkahelyi számítógépen megnyithat és használhat azzal, hogy az ilyen magáncélú használat során az Adatkezelő üzleti érdekeit és jó hírnevét nem sértheti. A Hivatal által működtetett információbiztonsági rendszerek egységesen biztosítják a hivatali rendszereken áthaladó elektronikus adatforgalom védelmét, amiből következően az e bekezdésben írt adatforgalomra is rálátással vannak.

(4) Az Adatkezelő, mint munkáltató vagy adatkezelő a munkáltatói vagy adatkezelői ellenőrzéshez való jogára hivatkozva ellenőrizheti a hivatali feladatot ellátó személy által folytatott hivatalos levelezést a jelen Szabályzatban foglaltak betartásával. Az adatkezelés jogalapja a GDPR 6. cikk (1) bekezdésének e) pontja, tekintettel arra, hogy az ellenőrzés az Adatkezelő közfeladatának megfelelő ellátása érdekében történik.

(5) Az ellenőrzés során az Adatkezelő főszabály szerint biztosítja az ellenőrzéshez szükséges munkatársak személyes jelenlétét, továbbá az ellenőrzés során a fokozatosság elvének betartásával jár el.

(8) Az ellenőrzést az Adatkezelő által elkészített érdekmérlegelési teszt eredménye alapozza meg, amely tartalmazza az adatkezelésre vonatkozó szükségesség-arányosság elvének érvényesülését. Az ellenőrzést végző személy köteles a hivatali feladatot ellátó személyt dokumentált módon, a tényleges ellenőrzés megkezdése előtt tájékoztatni, hogy mely, pontosan meghatározott érdek miatt kerül sor az ellenőrzésre, illetve annak körülményeiről. A hivatali feladatot ellátó személy az ellenőrzés során az e-mail tartalmának megtekintése

előtt köteles jelezni az ellenőrzést végző személynek, ha az adott e-mail nem a hivatali feladatellátásához kapcsolódó személyes adatot tartalmaz. A hivatali feladatellátással kapcsolatos e-mailek tartalmát az Adatkezelő korlátozás nélkül vizsgálhatja.

(6) Amikor a hivatalos e-mail postafiók tartalmát az Adatkezelő ellenőrizni kívánja – a lépcsőzetes ellenőrzési rendszer alapján –, elsősorban a levelek fejlécének listáját jogosult a hivatali feladatot ellátó személytől vagy az informatikai terület kijelölt munkatársától megkérni. A lista tartalmazhatja a postafiókba érkezett és onnan küldött levelek címzettjét, tárgyát, a küldés vagy fogadás időtartamát és az esetlegesen csatolt fájl nevét, méretét. A lista megismerését követően az ellenőrzést végző személy kijelölheti azokat a leveleket, amelyeket a hivatali feladatot ellátó személynek a részére át kell adnia, aki a kérést csak abban az esetben jogosult megtagadni, ha a levél nem hivatali, hanem magánjellegű. A magánjellegű levelek tartalmát az Adatkezelő nem ismerheti meg; a tilalom ellenére folytatott magánjellegű levelezés esetében a levél tartalmának megismerése nem szükséges a hivatali feladatot ellátó személlyel szemben esetlegesen alkalmazandó munkajogi vagy polgári jogi, illetve más jogkövetkezményekhez. Ilyen levelek törlésére az ellenőrzést végző személy jogosult felszólítani a hivatali feladatot ellátó személyt, aki köteles eleget tenni a felszólításnak.

(7) Az Adatkezelő adatszivárgásra vonatkozó megalapozott gyanú esetén, a szükséges információbiztonság biztosítása érdekében jogosult megtekinteni azokat az e-maileket is, amelyeket a hivatali feladatot ellátó személy magánjellegűnek minősített. Az ellenőrzés kizárólag addig tarthat, ameddig az ellenőrzést végző személy azok hivatali- vagy magánjellegéről meg nem győződik. Az ilyen ellenőrzést külön érdekmérlegelési teszt és szükség esetén adatvédelmi hatásvizsgálat kell, hogy megalapozza.

(8) Amennyiben olyan időpontban kellene az e-mail postafiókban tárolt levelek közül a szükséges hivatalos tárgyú leveleket kiválogatni, amikor az érintett hivatali feladatot ellátó személy tartósan nem éri el azt, írásban kijelölhet olyan személyt (hivatali munkatárs esetében másik hivatali munkatársat), aki helyette a postafiókba belépve ezt megteheti. Ennek hiányában az ellenőrzést végző személy jelölhet ki két hivatali munkatársat, akik együttes jelenlétük mellett csak a meghatározott, hivatalos tárgyú leveleket menthetik le a postafiókból, a nem hivatalos tárgyú levelek tekintetében azonban titoktartási kötelezettségük áll fenn, azok tartalmát nem adhatják át, illetve azokról információt nem közölhetnek az ellenőrzést végző vagy más személlyel.

(9) Amennyiben a hivatali feladatot ellátó személyt felmentik a feladatellátás alól, a felmentés időtartamára, illetve a jogviszonya megszűnése esetén – a (11) bekezdésben írtak kivételével – az e-mail postafiók címet inaktívvá kell tenni, vagyis olyan informatikai beállítást kell életbe léptetni, amely megakadályozza, hogy a postafiók további levelet fogadhasson.

(10) A postafiók inaktívvá tétele mellett tilos olyan beállítás alkalmazása, mely a postafiókba érkező leveleket más e-mail címre továbbítaná.

(11) A hivatali feladatot ellátó személy számára a feladatellátása utolsó napján biztosítani kell, hogy a postafiókjában lévő esetleges magánjellegű leveleit a postafiókjából

lementhesse. E mentést egy erre kijelölt munkatárs kontrollálja, akit titoktartási kötelezettség terhel a tudomására jutott magánjellegű adatok tekintetében.

(12) Ha a postafiók olyan jellegű hivatalos levelezést tartalmaz, amely a későbbi adatkezelői feladatok ellátása tekintetében szükséges lehet, és a dokumentumok lementése az Adatkezelő részére aránytalan nehézséget okoz, akkor a magánjellegű adatok lementését és végleges eltávolítását követően a postafiók tovább működtethető, melyről a hivatali feladatot ellátó személyt is tájékoztatni kell. A postafiókban a továbbiakban csak hivatalos tárgyú levelek kezelhetők.

(13) Az e-mail rendszer használatának ellenőrzéséről jegyzőkönyvet kell felvenni.

IX.4.4. A munkatársak rendelkezésére bocsátott internethasználatnak és ellenőrzésének adatvédelmi szabályai

(1) A hivatali feladatot ellátó személyek részére rendelkezésre bocsátott internetkapcsolat célja a hatékony munkavégzés elősegítése.

(2) Az Adatkezelő informatikai rendszereinek biztonságos működéséért felelős információbiztonsági vezető jogosult az internethasználatot átfogó módon, a feladatot ellátó szoftverek paraméterezésével szabályozni, ennek során meghatározni azokat a kulcsszavakat vagy kategóriákat, amelyeket vagy amelyekbe tartalmazó weboldalak megnyitását az informatikai rendszer automatikusan elutasítja.

(3) Amennyiben megalapozottan vélelmezhető, hogy a hivatali feladatot ellátó személy az internetkapcsolatot a fenti szabályok megsértésével használja, az ellenőrzést végző személy a szabályszegés körülményeit főszabály szerint személyes elbeszélgetés útján köteles tisztázni.

(4) Amennyiben a (3) bekezdésben foglalt eljárás nem vezetett vagy vezetne eredményre, az ellenőrzést végző személy kérheti az informatikai és az információbiztonsági terület bevonását azzal, hogy a hivatali feladatot ellátó személy számítógépe segítségével megnyitott weboldalak listáját, illetve az internethasználat során keletkezett logok elemzését az ellenőrzést végző személy részére adják át. Ebben az esetben az adatkezelés jogalapja a GDPR 6. cikk (1) bekezdésének e) pontja, tekintettel arra, hogy az adatkezelés célja az Adatkezelő közfeladatának ellátását szolgálja. Az ellenőrzést az Adatkezelő által készített érdekmérlegelési teszt eredménye alapozza meg, amely tartalmazza a szükségesség-arányosság elvének érvényesülését. Az ellenőrzést végző személy köteles a hivatali feladatot ellátó személyt dokumentált módon, a tényleges ellenőrzés megkezdése előtt tájékoztatni, hogy mely, pontosan meghatározott érdek miatt kerül sor az ellenőrzésre, illetve annak körülményeiről.

(5) A megnyitott weboldalak listáját és a logelemzést az ellenőrzést végző személy főszabály szerint a hivatali feladatot ellátó személy jelenlétében jogosult ellenőrizni, és a nem hivatalos jellegű adatokat csak a szükséges mértékben és ideig kezelheti azzal, hogy azokat részleteiben nem ismerheti meg, de az esetleges munkajogi vagy polgári jogi, illetve más következmények megállapításához szükséges mértékben jogosult az adatokat

észrevételezni.

(6) Az internethasználat ellenőrzéséről jegyzőkönyvet kell felvenni.

IX.4.5. A hivatali feladatot ellátó személy fizikai környezetének ellenőrzése

(1) Azt a fizikai területet, ahol a hivatali feladatot ellátó személy munkáját végzi – így például az íróasztalának fiókját – munkaügyi célból nem lehet ellenőrizni. Amennyiben egyéb célból az ellenőrzés szükségessége felmerül, úgy azt csak abban az esetben lehet megtenni, ha a vonatkozó jogszabályi rendelkezések azt lehetővé teszik, azt az előzetesen elvégzett érdekmérlegelési teszt eredménye alátámasztotta, és ezt az adatvédelmi tisztviselő előzőleg jóváhagyta. A munkatársat minden esetben teljeskörűen tájékoztatni kell előzetesen az ellenőrzéssel kapcsolatban megvalósuló adatkezelésről.

IX.4.6. Elektronikus megfigyelőrendszer (kamerarendszer) alkalmazása

(1) Amennyiben az Adatkezelő elektronikus megfigyelőrendszert kíván alkalmazni, az erre vonatkozó rendelkezéseket külön dokumentumban kell megfogalmaznia. Az ellenőrzéshez fűződő legitim érdek mérlegelése során tekintettel kell lenni az alábbi adatkezelési korlátokra:
   a) az ellenőrzés akkor tekinthető jogszerűnek, amennyiben a munkaviszony vagy kormányzati szolgálati jogviszony, illetve az adatfeldolgozói megállapodásból fakadó polgári jogi jogviszony rendeltetésével közvetlenül összefüggő okból feltétlenül szükséges,
   b) az ellenőrzés és az annak során alkalmazott eszközök, módszerek nem járhatnak az emberi méltóság megsértésével, illetőleg a hivatali feladatot ellátó személyek magánélete nem ellenőrizhető,
   c) a hivatali feladatot ellátó személyeket előzetesen tájékoztatni kell az adatkezelés lényeges körülményeiről,
   d) az Adatkezelő köteles a jogszerűség, a tisztességes eljárás és átláthatóság, valamint a célhoz kötöttség elveit az adatkezelés során betartani.

Az adatvédelmi és adatbiztonsági szabályzat mellékletei:

1. számú melléklet A vonatkozó jogszabályok jegyzéke
2. számú melléklet A hozzáféréssel kapcsolatos intézkedések nyilvántartása
3. számú melléklet Az adattovábbítások nyilvántartása
4. számú melléklet Az adatkezelési tevékenységekről vezetett nyilvántartás
5. számú melléklet Adatvédelmi hatásvizsgálat szükségességének értékelése
6. számú melléklet Adatvédelmi hatásvizsgálati jelentés
7. számú melléklet Előzetes konzultációra vonatkozó jelentés
8. számú melléklet Nyilatkozat az informatikai eszközök adattartalmáról az eszköz visszaszolgáltatásakor

Az adatvédelmi és adatbiztonsági szabályzat 1. számú melléklete

A vonatkozó jogszabályok jegyzéke

Jelen Szabályzat tartalmának meghatározása során az Adatkezelő figyelembe vette a vonatkozó hatályos jogszabályokat, illetve a fontosabb nemzetközi ajánlásokat, különös tekintettel az alábbiakra:

- a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről szóló, 2016. április 27-i 2016/679/EU európai parlamenti és tanácsi rendelet (GDPR);

- az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Infotv.);

- a kormányzati igazgatásról szóló 2018. évi CXXV. törvény;

- a Munka Törvénykönyvéről szóló 2012. évi I. törvény;

- a Polgári Törvénykönyvről szóló 2013. évi V. törvény;

- a polgári perrendtartásról szóló 2016. évi CXXX. törvény.

Az adatvédelmi és adatbiztonsági szabályzat 2. számú melléklete

A hozzáféréssel kapcsolatos intézkedések nyilvántartása

Az Adatkezelő számára kiemelten fontos az adatkezelés átláthatóságának és ellenőrizhetőségének lehetővé tétele az érintettek számára. Ennek érdekében a GDPR 15. cikke szerinti hozzáféréshez való jog gyakorlásával kapcsolatos intézkedésekről az alábbi nyilvántartást vezeti. E nyilvántartás teszi lehetővé, hogy a NAIH ellenőrizze a vonatkozó követelményeknek való megfelelést.

I. AZ ADATKEZELŐ MEGNEVEZÉSE ÉS ELÉRHETŐSÉGEI

Adatkezelő megnevezése: Szellemi Tulajdon Nemzeti Hivatala

Székhely: 1081 Budapest, II. János Pál pápa tér 7.

Telefonszám.: +36 (1) 312 4400

Fax: +36 (1) 474 5534

E-mail: sztnh@hipo.gov.hu

Adatvédelmi tisztviselő neve: dr. Hegedüs Krisztina

Adatvédelmi tisztviselő elérhetősége: adatvedelem@hipo.gov.hu

II. A HOZZÁFÉRÉSSEL KAPCSOLATOS INTÉZKEDÉSEK NYILVÁNTARTÁSA

#	A hozzáférési jogát érvényesíteni kívánó érintett neve, elérhetősége	Az érintett érvényesíteni kívánt hozzáférési jogának jellege (kérelem tartalma)	A jogérvényesítési kérelem benyújtásának dátuma	A hozzáférési jogát érvényesíteni kívánó érintett esetében történő adatkezelés jogalapja	A jogérvényesítési kérelem teljesítése érdekében tett intézkedés	A jogérvényesítési kérelem teljesítésének dátuma	A hozzáférési jogot korlátozó vagy megtagadó intézkedések jogi és ténybeli indokai	Bejegyzés dátuma, bejegyző aláírása
1.								
2.								

Az adatvédelmi és adatbiztonsági szabályzat 3. számú melléklete

Az adattovábbítások nyilvántartása

Az Adatkezelő számára kiemelten fontos az adatkezelés átláthatóságának és ellenőrizhetőségének lehetővé tétele. Ennek érdekében a személyes adatok harmadik személyek számára történő hozzáférhetővé tételéről, vagyis a személyes adatok továbbításáról az alábbi nyilvántartást vezeti. E nyilvántartás teszi lehetővé, hogy a NAIH ellenőrizze a vonatkozó követelményeknek való megfelelést.

I. AZ ADATKEZELŐ MEGNEVEZÉSE ÉS ELÉRHETŐSÉGEI

Adatkezelő megnevezése: Szellemi Tulajdon Nemzeti Hivatala

Székhely: 1081 Budapest, II. János Pál pápa tér 7.

Telefonszám.: +36 (1) 312 4400

Fax: +36 (1) 474 5534

E-mail: sztnh@hipo.gov.hu

Adatvédelmi tisztviselő neve: dr. Hegedüs Krisztina

Adatvédelmi tisztviselő elérhetősége: adatvedelem@hipo.gov.hu

II. AZ ADATTOVÁBBÍTÁSOK NYILVÁNTARTÁSA

#	A személyes adatok továbbításának időpontja	Az adatszolgáltatást teljesítő szervezeti egység megnevezése	Az adattovábbítás jogalapja és célja	A továbbított személyes adatok körének meghatározása	Az adattovábbítás címzettje	Harmadik országba történt adattovábbítás	Az adatkezelést előíró jogszabályban meghatározott egyéb adatok, további megjegyzés	Bejegyzés dátuma, bejegyző neve, aláírása
1.								
2.								

Az adatvédelmi és adatbiztonsági szabályzat 4. számú melléklete

Az adatkezelési tevékenységekről vezetett nyilvántartás

Az Adatkezelő a GDPR 30. cikkében foglaltak szerint az alábbi nyilvántartás vezeti az adatkezelési tevékenységeiről. A nyilvántartást az Adatkezelő köteles a NAIH megkeresésére rendelkezésre bocsátani erre irányuló megkeresés esetén.

Az adatkezelő neve: Szellemi Tulajdon Nemzeti Hivatala								
Az adatkezelő elérhetősége: székhely: 1081 Budapest, II. János Pál pápa tér 7., levélcím: 1438 Budapest, pf. 415., központi telefonszám: (1) 312-4400, faxszám: 474-5534, e-mail cím: sztnh@hipo.gov.hu								
Az adatvédelmi tisztviselő neve: Dr. Hegedüs Krisztina								
Az adatvédelmi tisztviselő elérhetősége: személyesen: 1081 Budapest, II. János Pál pápa tér 7., levélben: 1438 Budapest, pf. 415., telefonon: (1) 474-5941 vagy (1) 312-4400, faxon: (1) 474-5534, e-mailen: krisztina.hegedus@hipo.gov.hu vagy adatvedelem@hipo.gov.hu								
sorszám	az adatkezelés célja	az adatkezelés jogalapja	az érintettek kategóriái	a személyes adatok kategóriái	a címzettek kategóriái	harmadik országba vagy nemzetközi szervezetnek továbbítás információi	törlésre előirányzott idő	az adatbiztonságra vonatkozó technikai és szervezési intézkedések általános leírása
1.								
2.								

Az adatvédelmi és adatbiztonsági szabályzat 5. számú melléklete

ADATVÉDELMI HATÁSVIZSGÁLAT SZÜKSÉGESSÉGÉNEK ÉRTÉKELÉSE

Azonosító:

Az adatkezelési módszer leírása, beleértve az adatkezelés jellegének, hatókörének, körülményeinek és céljainak, a kezelt személyes adatok, illetve az adatkezeléshez használt eszközök ismertetését is.

A. A NAIH GDPR 35. cikk (4) bekezdése alapján kibocsátott lista szerinti vizsgálat

Az adatkezelés szerepel a NAIH GDPR 35. cikk (4) bekezdése alapján kibocsátott listáján: □ igen □ nem

Amennyiben az adatkezelés szerepel a NAIH GDPR 35. cikk (4) bekezdése alapján kibocsátott listáján, kérjük, jelölje be, hogy melyik feltétel(ek) teljesülése alapján szükséges az adatvédelmi hatásvizsgálatot elvégezni.

Feltétel	Teljesülés
Biometrikus adat kezelése módszeres megfigyelés céljából	
Kiszolgáltatott helyzetben lévő érintettek biometrikus adatának kezelése	
Pontozás	
Harmadik személytől begyűjtött személyes adatok felhasználása az érintettre vonatkozó döntés meghozatalánál	
Profilozás	
Joghatással bíró vagy az érintettet hasonlóképpen jelentős mértékben érintő döntéshozatal	
Módszeres megfigyelés	
Helymeghatározási adatok kezelése módszeres megfigyelés vagy profilalkotás céljából	
Munkatársak munkájának megfigyelése	
Különleges adatok nagy számban való kezelése	
Kiszolgáltatott helyzetben lévő érintettekkel kapcsolatos, nagy számban kezelt adatok eredeti céltól eltérő felhasználása	
Gyermekek személyes adatainak kezelése profilozás, automatikus döntéshozatal, vagy marketing, vagy közvetlenül részükre kínált, információs társadalommal összefüggő szolgáltatások ajánlása céljából	
Új technológiai megoldások használata	

Feltétel	Teljesülés
Egészségügyi adatok nagy számban történő felhasználása	
Több adatkezelő egy egész ágazat által közösen használt alkalmazást, rendszert, eszközt, illetve platformot tervez létrehozni, amelyben különleges adatokat is kezelnek	
Különböző forrásokból származó adatok összevonása, egymással való megfeleltetése vagy összehasonlítása	

Egyéb megjegyzések:

B. Az adatkezelés kockázatai szerinti vizsgálat

Az adatkezelés esetén teljesül az alábbi feltételek körül legalább kettő: □ igen □ nem

Amennyiben az adatkezelés esetén teljesül az alábbi feltételek körül legalább kettő, kérjük, jelölje be, hogy melyik feltételek teljesülése alapján szükséges az adatvédelmi hatásvizsgálatot elvégezni.

Feltétel	Teljesülés
Értékelés, pontozás vagy profilalkotást	
Joghatással vagy hasonló jelentős hatással járó automatizált döntéshozatal	
Módszeres megfigyelés	
Különleges adatok vagy fokozottan személyes jellegű adatok kezelése	
Nagy számban kezelt adatok	
Adatkészletek egymással való megfeleltetése vagy összevonása	
Kiszolgáltatott helyzetben lévő érintettekkel kapcsolatos adatok kezelése	
Új technológiai vagy szervezési megoldások innovatív használata vagy alkalmazása	
Az adatkezelés megakadályozza, hogy az érintettek a jogaikat gyakorolják, szolgáltatásokat vegyenek igénybe vagy szerződést érvényesítsenek	

Egyéb megjegyzések:

C. Adatvédelmi hatásvizsgálat a Hivatal döntése alapján

Az adatvédelmi hatásvizsgálatot kell végezni a Hivatal döntése alapján az adatkezelés vonatkozásában: □ igen □ nem

A Hivatal azon döntésének ismertetése, amelynek értelmében az adatkezeléssel kapcsolatban adatvédelmi hatásvizsgálatot kell végezni, beleértve annak a B. pont szerinti feltételnek a bemutatását is, amely a döntés alapjául szolgál.

D. Adatvédelmi hatásvizsgálat alóli mentesülés

Nem kell adatvédelmi hatásvizsgálatot végezni, amennyiben az alábbi feltételek valamelyike teljesül az adatkezelés vonatkozásában: □ igen □ nem

Feltétel	Teljesülés
Az adatkezelés valószínűsíthetően nem jár magas kockázattal	
Az adatkezelés hasonlít olyan adatkezelésre, amelyről már készült adatvédelmi hatásvizsgálat	
Az adatkezelést valamely uniós tagállam adatvédelmi felügyeleti hatósága korábban ellenőrizte	
Az adatkezelés a Hivatalra vonatkozó jogi kötelezettség teljesítéséhez szükséges, a jog szabályozza az adott adatkezelési műveletet, és az említett jogalap megállapítása során már készült adatvédelmi hatásvizsgálat	
Az adatkezelés szerepel a NAIH GDPR 35. cikk (5) bekezdése alapján összeállított jegyzékében	

Dátum:

Készítette:

_____

név, munkakör, szervezeti egység, aláírás

Közreműködött:

_____

név, munkakör, szervezeti egység, aláírás

Adatvédelmi tisztviselő:

_____

név, aláírás

Az adatvédelmi és adatbiztonsági szabályzat 6. számú melléklete

ADATVÉDELMI HATÁSVIZSGÁLATI JELENTÉS

Azonosító:

A. Az adatkezelési módszer leírása

Ismertesse az adatkezelés céljait, jogalapját, a kezelendő személyes adatokat, a személyes adatok forrását, az érintettek kategóriáit, a személyes adatok tárolásának időtartamát, valamint az adatkezelés egyéb jellemzőit!

Ismertesse az adatkezeléssel kapcsolatos felelősségi viszonyokat, különös tekintettel az adatkezelő(k)re, az adatfeldolgozó(k)ra, illetve a címzettekre!

Ismertesse az adatkezelésre vonatkozó esetleges belső és külső szabványokat!

B. A szükségesség és arányosság értékelése

1. Ismertesse az adatkezelés arányosságát és szükségességét előmozdító intézkedéseket!

Az adatkezelés célja vagy céljai meghatározottak, egyértelműek és jogszerűek?

Miként érvényesül az adattakarékosság elve?

Miként érvényesül a pontosság elve?

Miként érvényesül a korlátozott tárolhatóság követelménye?

2. Ismertesse az érintettek jogait támogató intézkedéseket!

Az adatkezelésre az érintett hozzájárulása esetén kerül sor? □ igen □ nem
Amennyiben igen, ismertesse a hozzájárulás visszavonásához való jog érvényesülését!

Ismertesse az érintettek részére nyújtott tájékoztatást és annak módját!

Ismertesse a hozzáféréshez való jog érvényesülésének módját!

Ismertesse a helyesbítéshez való jog érvényesülésének módját!

Ismertesse a törléshez (elfeledtetéshez) való jog érvényesülésének módját!

Ismertesse az adatkezelés korlátozásához való jog érvényesülésének módját!

Az adatkezelés esetén teljesülnek a GDPR 20. cikk (1) bekezdésében foglalt feltételek? □ igen □ nem
Amennyiben igen, ismertesse az adathordozhatósághoz való jog érvényesülésének módját!

Az adatkezelés esetén teljesülnek a GDPR 21. cikk (1)-(2) vagy (6) bekezdésében foglalt feltételek? □ igen □ nem
Amennyiben igen, ismertesse az adathordozhatósághoz való jog érvényesülésének módját!

Az adatkezelés esetén teljesülnek a GDPR 22. cikk (1) bekezdésében foglalt feltételek? □ igen □ nem
Amennyiben igen, ismertesse az érintett egyedi ügyekben hozott automatizált döntéshozatallal kapcsolatos jogai érvényesülésének módját!

2. Ismertesse garanciális jelentőségű kiegészítő intézkedéseket!

Sor kerül adatfeldolgozó igénybevételére az adatkezelés során? □ igen □ nem
Amennyiben igen, az adatfeldolgozók kötelezettségeit egyértelműen rögzíti-e az adatfeldolgozási szerződés?

Sor kerül Európai Unión kívüli adattovábbításra az adatkezelés során? □ igen □ nem
Amennyiben igen, megfelelő védelemben részesülnek a személyes adatok?

C. Kockázatelemzés és a kockázatok kezeléséhez szükséges intézkedések

1. A kockázatok felmérése és a szükséges intézkedések

Milyen főbb következményekkel járna az érintettekre a személyes adatokhoz való jogosulatlan hozzáférés?

Milyen forrásai lehetnek a személyes adatokhoz való jogosulatlan hozzáférésnek?

Milyen jelenlegi intézkedések védik a személyes adatokat a jogosulatlan hozzáférés ellen?

Milyen jelenlegi intézkedések védik az érintetteket a jogosulatlan hozzáférés következményei ellen?

Milyen további intézkedések biztosíthatnak hatékonyabb védelmet a személyes adatokat a jogosulatlan hozzáférés ellen?

Milyen további intézkedések biztosíthatnak hatékonyabb védelmet az érintettek részére a jogosulatlan hozzáférés következményei ellen?

Egyéb információk:

Milyen főbb következményekkel járna az érintettekre a személyes adatok véletlen vagy jogellenes megváltoztatása?

Milyen forrásai lehetnek a személyes adatok véletlen vagy jogellenes megváltoztatásának?

Milyen jelenlegi intézkedések védik a személyes adatokat a véletlen vagy jogellenes megváltoztatás ellen?

Milyen jelenlegi intézkedések védik az érintetteket a személyes adatok a véletlen vagy jogellenes megváltoztatásának következményei ellen?

Milyen további intézkedések biztosíthatnak hatékonyabb védelmet a személyes adatokat véletlen vagy jogellenes megváltoztatása ellen?

Milyen további intézkedések biztosíthatnak hatékonyabb védelmet az érintettek részére a személyes adatok véletlen vagy jogellenes megváltoztatásának következményei ellen?

Egyéb információk:

Milyen főbb következményekkel járna az érintettekre a személyes adatok elvesztése?

Milyen forrásai lehetnek a személyes adatok elvesztésének?

Milyen jelenlegi intézkedések védik a személyes adatokat az adatvesztés ellen?

Milyen jelenlegi intézkedések védik az érintetteket az adatvesztés következményei ellen?

Milyen további intézkedések biztosíthatnak hatékonyabb védelmet az adatvesztés ellen?

Milyen további intézkedések biztosíthatnak hatékonyabb védelmet az érintettek részére az adatvesztés következményei ellen?

Egyéb információk:

2. Intézkedése terv

D. Az érdekeltek bevonása

Az adatvédelmi tisztviselő véleménye

Sor került-e az érintettek bevonására? □ igen □ nem
Amennyiben igen, ismertesse az érintettek véleményét, valamint a Hivatal intézkedéseit!
Amennyiben nem, ismertesse az érintettek bevonása elmaradásának okait!

Dátum:

Készítette:

_____
név, munkakör, szervezeti egység, aláírás

Közreműködött:

_____
név, munkakör, szervezeti egység, aláírás

Adatvédelmi tisztviselő:

_____
név, aláírás

Mellékletek:

Az adatvédelmi és adatbiztonsági szabályzat 7. számú melléklete

ELŐZETES KONZULTÁCIÓRA VONATKOZÓ JELENTÉS

Az adatvédelmi hatásvizsgálat azonosítója:

A. Az előzetes konzultáció szükségességének értékelése

Ismertesse, hogy milyen okból szükséges előzetes konzultáció a NAIH-hal?

Előzetes konzultáció oka(i)	Státusz
A fennmaradó kockázatok továbbra is magasak az érintett jogaira és szabadságaira nézve	
Jogszabályi kötelezettség	

Ismertesse részletesen az előzetes konzultáció okát!

B. Az előzetes konzultáció keretében a NAIH rendelkezésére bocsátott információk

Ismertesse a NAIH részére továbbított információkat és azok rendelkezésére bocsátásának idejét!

C. A NAIH-hal folytatott egyeztetések

Foglalja össze a NAIH-hal folytatott kommunikáció lényegét és tüntesse fel a kapcsolattartás idejét!

D. Az előzetes konzultáció keretében a NAIH által megfogalmazott javaslatok és/vagy intézkedések

Foglalja össze az előzetes konzultáció keretében a NAIH által megfogalmazott javaslatokat és / vagy intézkedéseket!

E. A NAIH által megfogalmazott javaslatokkal kapcsolatos intézkedések

Foglalja össze az előzetes konzultáció keretében a NAIH által megfogalmazott javaslatokkal kapcsolatban foganatosított intézkedéseket!

Dátum:

Készítette:

_____

név, munkakör, szervezeti egység, aláírás

Közreműködött:

_____

név, munkakör, szervezeti egység, aláírás

Adatvédelmi tisztviselő:

_____

név, aláírás

Az adatvédelmi és adatbiztonsági szabályzat 8. számú melléklete

Nyilatkozat az informatikai eszközök adattartalmáról az eszköz visszaszolgáltatásakor

Név: ……., a …….. Főosztály/Osztály munkatársa kijelentem, hogy a Szellemi Tulajdon Nemzeti Hivatala által a feladataim elvégzése céljából biztosított alábbi infokommunikációs eszközökön

eszközök megnevezése: SAP azonosító:

.....

.....

.....

kizárólag a hivatali feladatokkal összefüggő adatok találhatók, azokról az esetlegesen ott tárolt magánjellegű adatokat eltávolítottam.

Kelt: ……..……

…….

aláírás

A nyilatkozat egy példányát a Szellemi Tulajdon Nemzeti Hivatala nevében átvettem:

Kelt: ……..……

…… ……

név aláírás