

1/2025. (I.31.) NKFH elnöki utasítás
A NEMZETI KERESKEDELMI ÉS
FOGYASZTÓVÉDELMI HATÓSÁG
ADATBIZTONSÁGI ÉS ADATKEZELÉSI
SZABÁLYZATÁRÓL

1/2025. (I.31.) NKFH elnöki utasítás
a Nemzeti Kereskedelmi és Fogyasztóvédelmi Hatóság
Adatbiztonsági és Adatkezelési Szabályzatáról

A Nemzeti Kereskedelmi és Fogyasztóvédelmi Hatóság Szervezeti és Működési Szabályzatáról szóló 31/2024. (XII.30.) NGM utasítás 29. § (4) bekezdés b) pontjában meghatározott hatáskörömben eljárva – figyelemmel a jogalkotásról szóló 2010. évi CXIII. törvény 23. § (4) bekezdés c) pontjára – a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről szóló, 2016. április 27-i (EU) 2016/679 európai parlamenti és tanácsi rendelet 24. cikk (2) bekezdésében foglaltak alapján, továbbá az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény 25/A. § (3) bekezdésében foglaltak szerint a Nemzeti Kereskedelmi és Fogyasztóvédelmi Hatóság Adatbiztonsági és Adatkezelési Szabályzatát az alábbiak szerint állapítom meg:

I. FEJEZET

ÁLTALÁNOS RENDELKEZÉSEK

1. Az Adatbiztonsági és Adatkezelési Szabályzat célja

1. § Az Adatbiztonsági és Adatkezelési Szabályzat (a továbbiakban: **Szabályzat**) célja a Nemzeti Kereskedelmi és Fogyasztóvédelmi Hatóság (a továbbiakban: **NKFH**) működése, hatáskörének gyakorlása és feladatellátása során kezelt személyes adatok védelmének és kezelése rendjének meghatározása, továbbá annak biztosítása, hogy az NKFH, mint Adatkezelő megfeleljen a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről szóló, az Európai Parlament és a Tanács 2016/679 Rendeletében (a továbbiakban: **GDPR**), valamint az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvényben (a továbbiakban: **Infotv.**) foglaltaknak.

2. A Szabályzat értelmezése

2.§ (1) A Szabályzatot az elnök (a továbbiakban: **Elnök**) elnöki utasítás formájában adja ki, annak visszavonása tárgyában az Elnök intézkedik.

(2) A jelen Szabályzat általános, lényeges és folyamatos, tartós jellegű előírásokat tartalmazó normatív aktus.

(3) A Szabályzatot a GDPR, valamint az Infotv. rendelkezéseivel, továbbá az NKFH működésére, hatáskörének gyakorlására, valamint feladatainak ellátására irányadó hatályos jogszabályi rendelkezésekkel, továbbá az NKFH belső szabályzataiban foglaltakkal összhangban kell értelmezni.

(4) A Szabályzat alkalmazása során a definíciók vonatkozásában a GDPR 4. cikkében foglalt „Fogalommeghatározások”, valamint az Infotv. 3. § szerinti „Értelmező rendelkezések”-ben foglaltak az irányadóak.

3. A Szabályzat hatálya

3. § (1) A Szabályzat személyi hatálya kiterjed az NKFH-nál foglalkoztatott valamennyi kormánytisztviselőre, munkavállalóra, valamint munkavégzésre irányuló egyéb jogviszony keretében foglalkoztatottra (a továbbiakban, együttesen: **Foglalkoztatott**), továbbá az NKFH-val a Polgári Törvénykönyvről szóló 2013. évi V. törvény szerinti szerződéses jogviszonyban álló természetes személyekre, jogi személyekre, valamint jogi személyiség nélküli jogalanyokra, továbbá mindazokra, akik az NKFH-val való kapcsolatfelvétel, kapcsolattartás során, vagy egyéb módon személyes adatokat ismernek meg.

(2) A Szabályzat tárgyi hatálya az NFKH működése, hatáskör-gyakorlása, valamint feladatellátása során felmerülő személyes adatok kezelésére terjed ki, ideértve az érintett vagy más személy által rendelkezésre bocsátott, valamint a működés során megismert személyes adatok körét.

(3) Az NKFH a jogszabályban foglalt közhatalmi jogkör részét képező jogalkalmazói feladatellátásából és hatáskör-gyakorlásából fakadóan mindennapi operatív működése során a személyes adatok - GPDR 9. cikk szerinti - különleges kategóriáinak nagy számban történő, szisztematikus kezelését is ellátja.

(4) Az NKFH tárgyi hatálya alá tartozóan kiemelt figyelmet fordít az egészségügyi adatok, valamint a gyermekek – 16. életévét be nem töltött kiskorúak - személyes adatainak kezelésére, amelyre vonatkozóan iránymutatást az egyéb, adott szervezeti egységre irányadó belső szabályozók tartalmazzák.

(5) A Szabályzat az Elnök által történő visszavonásig hatályos.

II. FEJEZET

A SZEMÉLYES ADATOK KEZELÉSÉVEL KAPCSOLATOS ELNÖKI FELELŐSSÉG, AZ ADATVÉDELMI TISZTVISELŐ

4. Az Elnök felelőssége

4. § (1) Az NKFH szervezetén belül a személyes adatok kezelése jogszerűségének biztosításáért, az adatvédelmi- és adatbiztonsági intézkedések megtartásáért az Elnök felel.

(2) Az Elnök felelősségi körén belül:

- a) gondoskodik az adatkezelés személyi és tárgyi feltételeinek biztosításáról, az adatvédelmi és adatbiztonsági rendszer működtetéséről;
- b) adatvédelemmel kapcsolatos vizsgálatot rendelhet el;
- c) kijelöli az NKFH adatvédelmi tisztviselőjét;
- d) biztosítja az adatvédelmi tisztviselő számára a hozzáférést a feladatai végrehajtásához szükséges elektronikus rendszerekhez, iratokhoz - a jelen Szabályzatban foglalt iratok kivételével -, az egyéb adathordozókhoz, valamint
- e) a feladatai naprakész ellátásához szükséges feltételeket, jogosultságokat és erőforrásokat a rendelkezésére bocsátja.

5. Az adatvédelmi tisztviselő jogállása és a feladatellátáshoz kapcsolódó követelmények

5. § (1) Az NKFH jogszerű működése biztosításának érdekében adatvédelmi tisztviselő kijelölése a GDPR 37. cikk (1) bekezdés a) pontjában, valamint az Infotv. 25/L. § (1) bekezdés a) pontjában foglaltaknak megfelelően kötelező.

(2) Az NKFH adatkezeléssel és adatbiztonsággal kapcsolatos döntéseinek előkészítéséről, a GDPR-ban, az Infotv.-ben, valamint az adatvédelmet érintő belső szabályozókban foglaltak végrehajtásáról, a jogszerű adatkezelés, valamint az adatvédelmi rendelkezések megtartásának biztosításáról továbbá a szervezeten belüli adatvédelmi tudatosság erősítéséről az Elnök az adatvédelmi tisztviselő útján gondoskodik.

(3) Az adatvédelmi tisztviselőt szakmai rátermettség és különösen az adatvédelmi jog és gyakorlat szakértői szintű ismerete, valamint a tisztség betöltésével felmerülő feladatok ellátására való alkalmasság alapján kell kijelölni.

(4) Az adatvédelmi tisztviselő nevét, elektronikus levélcímét, postai levelezési címét az NKFH honlapján a közérdekű adatok között külön menüpontban közzé kell tenni.

6. § (1) Az adatvédelmi tisztviselő

a) az NKFH-n belüli, jogszabályból eredő kötelezettségeit és feladatait más, a munkaköri leírásában meghatározott kötelezettségei mellett, attól függetlenül köteles ellátni;

b) tisztségével összefüggő kötelezettségei és feladatai ellátása során nem utasítható, és e tisztségének ellátásával kapcsolatban – az NKFH Szervezeti és Működési Szabályzatában (a továbbiakban: SzMSz) rögzítettek szerint – közvetlenül az Elnöknek felel;

c) feladatainak ellátásához szükséges feltételek biztosítása, az ezzel összefüggő titkársági, egyéb adminisztratív feladatok ellátása a Jogi Főosztály feladata.

(2) Az adatvédelmi tisztviselővel az adatkezelés jogszerű fenntartása, kialakítása, illetve az elszámoltathatóság elvének történő megfelelés érdekében az NKFH szervezeti egységei kötelesek együttműködni.

(3) Az adatvédelmi tisztviselő a szervezet mindennapi működése során független tanácsadói, megfigyelői, illetve ellenőrző funkciót tölt be, amelyre tekintettel:

a) az NKFH Foglalkoztatottjai a hivatali út betartása nélkül közvetlenül fordulhatnak hozzá a személyes adataik kezeléséhez és jogaik gyakorlásához kapcsolódó bármely kérdésben;

b) hivatalos elérhetőségein keresztül az NKFH Foglalkoztatottjai számára folyamatosan köteles rendelkezésre állni azzal, hogy adatvédelmi tárgyú megkeresés esetén – a soron kívüli eseteket kivéve – a megkeresés napját követő munkanap végéig válaszolni köteles.

(4) Az adatvédelmi tisztviselő egyéb feladatokat is elláthat, azonban a szervezetnek biztosítania kell, hogy e feladatokból ne fakadjon összeférhetetlenség. Az adatvédelmi tisztviselő az NKFH-n belül vezető pozíciót nem tölthet be.

(5) A szervezeten kívüli, szolgáltatási szerződés alapján – megbízási jogviszonyban - foglalkoztatott adatvédelmi tisztviselő garanciát nyújt a feladatellátás külső befolyástól mentes elvégzésére, ennek okán szükséges:

- a) nyilatkozatba foglalni, hogy a kijelölt adatvédelmi tisztviselővel szemben nem áll fenn összeférhetetlenségi ok;
- b) biztosítani, hogy a szervezeten kívüli megbízott esetén a megbízási szerződés kellő pontossággal és részletességgel tartalmazza az összeférhetetlenség elkerüléséhez szükséges kontroll mechanizmusokat.

6. Az adatvédelmi tisztviselő feladatai

7. § (1) Az adatvédelmi tisztviselő feladatait az adatkezelési műveletekhez fűződő kockázatok megfelelő figyelembevételével, az adatkezelés jellegére, hatókörére, körülményére és céljára is tekintettel végzi, így különösen:

- a) közreműködik az adatvédelmi és adatbiztonsági belső szabályzatok megalkotásában;
- b) a tisztségéből fakadó feladatai ellátása érdekében - a feladatellátásához szükséges mértékben – az NKFH nyilvántartási rendszereibe betekinthez;
- c) elősegíti a GDPR adatok kezelésére vonatkozó elvekre, az érintett jogaira, az adatkezelési tevékenységek nyilvántartására, az adatkezelés biztonságára, valamint az adatvédelmi incidens bejelentésére és arról való tájékoztatásra vonatkozó rendelkezéseinek az NKFH-n belüli végrehajtását;
- d) szakmai tanácsot ad az NKFH Foglalkoztatottjainak az adatkezelési folyamatok jogszerű és - az érintettek számára - transzparens kialakítása érdekében;
- e) a személyes adatok kezelésére vonatkozó jogi előírásokról naprakész tájékoztatást nyújt és tanácsot ad azok érvényesítésének módjaival kapcsolatban;
- f) figyelemmel kíséri és ellenőrzi a személyes adatok kezelésére vonatkozó jogszabályi előírások, valamint a belső adatvédelmi és adatbiztonsági szabályzatok érvényesülését;
- g) elősegíti az érintetteket megillető jogok gyakorlását, elkészíti az NKFH adatkezeléseire vonatkozó adatkezelési tájékoztatóit;
- h) megvizsgálja a folyamatban lévő, az NKFH által tervezett vagy módosuló adatkezelések érintettekre gyakorolt kockázatát, szükség esetén javaslatot tesz adatvédelmi hatásvizsgálat lefolytatására, nyomon követi a hatásvizsgálat GDPR 35. cikke szerinti elvégzését;
- i) a jelen Szabályzatban foglalt kivételekkel vezeti az NKFH adatvédelmi nyilvántartásait;
- j) közreműködik az adatvédelmi incidensek dokumentálásában, valamint körülményeinek tisztázásában;
- k) az adatvédelmi incidensek körülményeinek feltárása eredményként az adatvédelmi incidenst a GDPR 33. cikke szerint bejelenti a Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: **NAIH**) részére;
- l) elvégzi az adatvédelmi auditokhoz kapcsolódó teendőket;
- m) szükség esetén elkészíti, valamint dokumentálja az érdekmérlegelési tesztet;
- n) közreműködik és koordinálja a közérdekű adatok nyilvánosságával kapcsolatos feladatok ellátását;
- o) ellátja az NKFH munkatársainak adatvédelmi tudatosság képzését;
- p) kapcsolatot tart a NAIH-val;
- q) részt vesz a NAIH elnöke által megrendezésre kerülő adatvédelmi tisztviselők éves konferenciáján,
- r) képviseli az NKFH-t a feladatellátásával kapcsolatban felmerülő adatvédelmi és adatbiztonsági tárgyú szakmai rendezvényeken.

8. § (1) Az adatvédelmi tisztviselő személyügyi dokumentációban foglalt személyes adatokat az érintett hozzájárulása esetén a feladatainak ellátásához szükséges mértékben ismerhet meg.

(2) A Humánpolitikai Főosztály, valamint a Számviteli és Bérszámfejtési Osztály által az NKFH Foglalkoztatottjait érintő, személyes adatokat tartalmazó nyilvántartásainak jogszerű – a mindenkori

adatbiztonsági és adatvédelmi szabályoknak megfelelő - kezeléséért az adott szervezeti egység vezetője felelős.

III. FEJEZET

A SZEMÉLYES ADATOK KEZELÉSÉNEK ELVEI ÉS JOGALAPJA, ADATTOVÁBBÍTÁS

7. A személyes adatok kezelésének elvei

9. § (1) Az NKFH a személyes adatok kezelését az adatvédelmi szabályok elveinek megfelelően végzi, az alábbiak szerint:

- a) a személyes adatok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon végzi (jogszerűség, tisztességes eljárás és átláthatóság);
- b) személyes adatot csak meghatározott, egyértelmű és jogszerű célból gyűjt, rögzít, vesz át, és azt az eredeti céllal összeegyeztethető módon kezel (célhoz kötöttség);
- c) kizárólag az adatkezelés céljai szempontjából szükséges és releváns adatokat kezel (adattakarékosság);
- d) az adatkezelés célja szempontjából pontatlan személyes adatok haladéktalan törlése, vagy helyesbítése iránt intézkedik (pontosság);
- e) biztosítja, hogy az érintett azonosítására alkalmas személyes adatai csak az adatkezelés céljának eléréséhez szükséges ideig kerüljenek megőrzésre (korlátozott tárolhatóság);
- f) biztosítja a személyes adatok teljes körű és kockázatokkal arányos védelmét az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve (integritás és bizalmas jelleg);
- g) az NKFH felelős azért, hogy adatkezelési tevékenységei megfeleljenek az alapelveknek, továbbá képesnek kell lennie e megfelelés igazolására is (elszámoltathatóság).

(2) Az NKFH a szervezeten belüli adatkezelési folyamatait a GDPR alapelvei alapján úgy alakítja és működteti, hogy az NKFH adatkezelésével elérendő célok és az adatvédelmi követelmények közötti összhang biztosított legyen, a kialakított szabályrendszer ne vezessen a személyes adatok védelmére és biztonságára vonatkozó követelmények sérelméhez, az adatvédelem pedig ne legyen akadálya a jogszerű célok elérésének. Az NKFH a személyes adatok védelmét – ideértve az informatikai és fizikai biztonsági intézkedéseket is - a személyes adatok teljes életciklusa során biztosítja, érvényesítve a személyes adatok felvételétől azok kezelésén át a végleges és visszaállíthatatlan törlésükig.

(3) Az NKFH a működése és feladatellátása során

- a) ügyviteli, illetve
- b) nyilvántartási célú adatkezelést végez.

(4) Az NKFH ügyvitelhez kapcsolódó adatkezelése kizárólag az ügy elintézéséhez kapcsolódik, alapvető célja az adott ügyhöz kapcsolódó eljárás lefolytatásához, az eljárás szereplőinek azonosításához és az ügy befejezéséhez szükséges adatok biztosítása. Az ügyviteli célú adatkezelés során a személyes adatok kizárólag az adott ügy irataiban és az ügyviteli segédletekben szerepelhetnek, kezelésükre e célból csak az alapul szolgáló irat selejtezéséig van lehetőség.

(5) Az NKFH nyilvántartási célú adatkezelése az előre meghatározott szempontok alapján gyűjtött személyes adatfajtákból strukturált adatállományt hoz létre, az adatkezelés időtartama alatt biztosítva az adatok különböző jellemzők alapján történő visszakereshetőségét, automatizált nyilvántartások esetében a lekérdezhetőségét.

8. A személyes adatok kezelésének jogalapjai

10. § (1) Az NKFH általi személyes adatkezeléseknek az alábbi jogalapjai lehetnek:

- a) az érintett hozzájárulását adta 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 NKFH-ra 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 NKFH-ra ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges;
- f) az adatkezelés az NKFH 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) Az NKFH adatkezelési tevékenységei kapcsán az általánosan használt jogalap a GDPR 6. cikk (1) bekezdés e) pontja (az adatkezelés közérdekű vagy az NKFH-ra ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges).

(3) E jogalap helyett akkor alkalmazható más, a GDPR 6. cikke szerinti jogalap, ha az adatkezelés az NKFH közfeladatának ellátásához vagy közhatalmi tevékenysége gyakorlásához nem szükséges.

11. § (1) Amennyiben az adatkezelés az érintett hozzájárulásán alapul az NKFH-nak képesnek kell lennie annak igazolására, hogy az érintett hozzájárulása

- a) önkéntes,
- b) konkrét,
- c) megfelelő tájékoztatáson alapuló és
- d) egyértelmű kinyilvánítása, amellyel az érintett beleegyezését adja az őt érintő személyes adatok kezeléséhez, mely bármikor visszavonható.

(2) Az érvényes hozzájárulás feltételeit az adatkezelés megkezdése előtt minden esetben vizsgálni szükséges.

12. § (1) Amennyiben a személyes adat kezelése a GDPR 6. cikk (1) bekezdés f) pontján (az adatkezelés az NKFH vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges) alapul, az NKFH az adatkezelés jogszerűségének vizsgálatához érdekmérlegelési tesztet folytat le, mely során az adatkezelés céljának szükségességét és az érintettek jogainak és szabadságainak arányos mértékű korlátozását vizsgálja. Az érdekmérlegelési tesztet az érintettek rendelkezésére kell bocsátani.

(2) Az NKFH mindennapi operatív működése során a személyes adatok - GDPR 9. cikk szerinti - különleges kategóriáinak nagy számban történő, szisztematikus kezelését is ellátja. Főszabály szerint a

„különleges adatok” kezelése tilos, érintetti hozzájárulás, valamint a megfelelő garanciák biztosítása mentén azonban jogszerű.

9. Az adattovábbítás szabályai

13. § (1) Az NKFH a személyes adatok továbbítására irányuló megkeresés teljesítése során figyelemmel van a GDPR célhoz kötöttségre és adattakarékosságra vonatkozó alapelveinek betartására.

(2) Adatvédelmi szempontból akkor tekinthető az adattovábbítás jogszerűnek, ha

- a) az NKFH jogosult a személyes adat továbbítására,
- b) az adattovábbítás címzettje rendelkezik a személyes adat kezeléséhez szükséges jogalappal vagy az érintett hozzájárulásával, és
- c) az adatkérés célja a fentiekkel összhangban van.

(3) Az adattovábbítás feltételeinek megléte és a célhoz kötöttség a jogszerűség együttes követelménye. Az adatot továbbító szervezeti egység az adattovábbítás feltételeinek meglétét minden egyes személyes adattal összefüggésben köteles ellenőrizni, így különösen azt, hogy az igényelt adatokra vonatkozóan az NKFH az adatok kezelőjének minősül-e.

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

- a) az adatkérés célját, jogalapját;
- b) a kért adatok körének pontos meghatározását;
- c) az adatkérő személyét, az adatkérő azonosítását lehetővé tevő adatokat.

14. § (1) Az NKFH egyes szervezeti egységei az Európai Gazdasági Térségbe (a továbbiakban: **EGT**) jogszabály alapján továbbítanak személyes adatokat. Harmadik országba (nem EGT tagállamba) vagy nemzetközi szervezet részére történő személyes adat a GDPR 44-50. cikkében szabályozott garanciális feltételek fennállta esetén továbbítható.

(2) Az adattovábbítás jogszerűségének ellenőrzése, valamint az érintettek tájékoztatása céljából az adatot továbbító szervezeti egységek adattovábbítási nyilvántartást kötelesek vezetni.

(3) Az NKFH szervezeti egységei a szervezeten kívüli történő adattovábbítás jogszerűsége céljából kikérhetik az adatvédelmi tisztviselő véleményét.

IV. FEJEZET

AZ ÉRINTETT JOGAI ÉRVÉNYESÜLÉSÉNEK BIZTOSÍTÁSÁVAL KAPCSOLATOS FELADATOK

10. Az érintett jogai érvényesülésének biztosításával kapcsolatos feladatok

15. § (1) Az adatvédelmi tisztviselő az NKFH adatkezelési tevékenységeire vonatkozó, az adatkezelés érintettjei számára világos, könnyen értelmezhető és átlátható módon, adatkezelési célonként a GDPR 13-14. cikke szerinti tartalommal – a GDPR 5. cikke szerinti alapelvek sérelme nélkül - elkészíti az adatkezelési

tájékoztatásokat, melyek tartalmi megfelelőségét, naprakészségét és elérhetőségét köteles figyelemmel kíséreni.

(2) Az NKFH Foglalkoztatottjait érintő adatkezelési tájékoztatásokat az NKFH székhelyén elérhető módon kell a Foglalkoztatottak számára biztosítani.

(3) Az NKFH-nál foglalkoztatotti jogviszonyt létesítő személyek számára a belépéshez szükséges dokumentációval együtt, elektronikus úton az őket érintő adatkezelési tájékoztatásokat szükséges megküldeni, azok megismertetését hitelt érdemlően – aláírással ellátva – igazolni.

(4) Az adatvédelmi tisztviselő:

- a) az NKFH-hoz érkezett érintetti joggyakorlásra irányuló kérelmet a kérelmet benyújtó személyazonosságának megállapítása érdekében megvizsgálja;
- b) amennyiben a kérelmet benyújtó személyazonossága kétséget kizáróan nem állapítható meg, az azonosítás érdekében további intézkedéseket tesz;
- c) a kérelmet benyújtó személyazonosságának megállapítása után a kérelmet a GDPR 15-23. cikkei alapján érdemben elbírálja;
- d) indokolatlan késedelem nélkül és a lehető legrövidebb időn belül, de legkésőbb az azonosítható érintettől származó kérelem beérkezésétől számított 15 napon belül tájékoztatja az érintettet – az általa megjelölt formában és módon - a jogai gyakorlására irányuló kérelme nyomán hozott intézkedésekről.

16. § Az NKFH az ellenkező bizonyításáig a kérelmet előterjesztő személy megfelelő azonosításának ismeri el az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény 18. §-a és a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól szóló 2023. évi CIII. törvény 34. §-a szerint megvalósuló beadványokat, a teljes bizonyító erejű magánokiratokban foglalt postai úton előterjesztett és az érintett azonosításához szükséges adatokat tartalmazó kérelmeket.

11. Adatvédelmi hatásvizsgálat

17. § (1) Az NKFH adatvédelmi hatásvizsgálatot folytat le akkor, ha a tervezett adatkezelése valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, valamint, ha a tervezett adatkezelés a NAIH által összeállított jegyzékben szerepel.

(2) Az adatvédelmi hatásvizsgálat lefolytatását az NKFH adatkezelésért felelős szervezeti egysége írásban kezdeményezi az Elnöknél.

(3) Az adatvédelmi hatásvizsgálat lefolytatására vonatkozó kezdeményezésnek tartalmaznia kell:

- a) a tervezett adatkezelés jellegét, hatókörét, körülményeit és céljait;
- b) a személyes adatok körét, a címzetteket, valamint a személyes adatok tárolásának időtartamát;
- c) a személyes adatok kezeléséhez használt eszközök bemutatását (hardverek, szoftverek)
- d) az adatkezelés jogszerűségének indokait;
- e) az érintettek jogait támogató intézkedések leírását;
- f) a kockázatok forrását, jellegét, egyediségét és súlyosságát;
- g) a kockázatok orvoslására irányuló intézkedések meghatározását.

18. § (1) Az Elnök kikéri az adatvédelmi tisztviselő álláspontját az adatvédelmi hatásvizsgálat szükségessége kapcsán, majd elrendeli az adatvédelmi hatásvizsgálat lefolytatását vagy írásban rögzíti a mellőzésének okait.

(2) Amennyiben az Elnök a hatásvizsgálat szükségességéről dönt, a hatásvizsgálat lefolytatására eseti munkacsoportot hoz létre. Az Európai Adatvédelmi Testület által elfogadott, az adatvédelmi hatásvizsgálatra vonatkozó hatályos iránymutatásban foglalt szempontokat és eljárásrendet a munkacsoport köteles figyelembe venni. A munkacsoport munkáját az adatvédelmi tisztviselő segíti. A munkacsoport az adatvédelmi hatásvizsgálat lefolytatását követően megállapításairól és javaslatairól, a hatásvizsgálat esetleges mellőzéséről összefoglaló írásbeli jelentést készít az Elnök részére.

(3) A tervezett adatkezelés akkor kezdhető meg, amikor az Elnök elfogadja a munkacsoport jelentését.

(4) Ha az adatvédelmi hatásvizsgálat eredményeként a tervezett adatkezelés vonatkozásában a kockázatok nem mérsékelhetők az NKFH rendelkezésére álló technológiák és a végrehajtási költségek szempontjából ésszerű módon, akkor az adatkezelési tevékenység megkezdése előtt a GDPR 36. cikke alapján az NKFH – az adatvédelmi tisztviselője útján – köteles konzultálni a NAIH-val. A konzultáció során a GDPR 36. cikk (3) bekezdése szerinti információkat a NAIH rendelkezésére kell bocsátani.

V. FEJEZET

ADATBIZTONSÁGI INTÉZKEDÉSEK, AZ ADATVÉDELMI INCIDENSEK KEZELÉSE

12. Adatbiztonsági intézkedések

19. § (1) A GDPR 25. cikkével összhangban az Elnök olyan technikai és szervezési intézkedéseket hoz, amelyek célja az adatvédelmi elvek érvényesítése, az érintettek jogainak és szabadságainak védelméhez szükséges garanciák az adatkezelés teljes folyamatába történő beépítése, a jogszerű és az érintettek számára átlátható adatvédelmi folyamatok kialakítása és működtetése.

(2) Az NKFH a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítéséből, elvesztéséből, megváltoztatásából, jogosulatlan nyilvánosságra hozatalából vagy az azokhoz való jogosulatlan hozzáféréséből (bizalmasság, sértetlenség és rendelkezésre állás) eredő kockázatok mérséklése céljából

- a) logikai;
- b) fizikai;
- c) szervezeti (adminisztratív) védelmi intézkedéseket alkalmaz.

20. § (1) Az NKFH alkalmazásában logikai védelmi intézkedések:

- a) a személyes adatokat tartalmazó iratok/adathordozók zárható páncélszekrényben történő tárolása;
- b) az NKFH Foglalkoztatottjai részére egyéni felhasználói profilok biztosítása a feladatok és felelősségi körök elválasztásával azért, hogy csak az illetékes felhasználók – a szükséges ismeret és legkisebb jogosultság elveinek betartásával – férhessenek hozzá a személyes adatokhoz;
- c) naplózó rendszer kialakítása (például a rendszerbe történő bejelentkezésekkel, a benne eszközölt változtatásokkal kapcsolatban stb.), amely lehetővé teszi az adatvédelmi incidensek korai észlelését;

- d) olyan rendszerkörnyezetek, védelmi eszközök és felügyeleti képességek kialakítása, melyek a személyes adatokat kezelő rendszerek integritását, az adatokhoz való hozzáférés folyamatos bizalmas jellegét, ellenálló képességét és rendelkezésre állását kockázatarányos védelemmel biztosítják;
- e) olyan szervezési intézkedések meghozatala, mely a d) pontban leírt képességeket és védelmet rendszeresen tesztelik.

21. § (1) Az NKFH alkalmazásában fizikai védelmi intézkedések:

- a) a jogosulatlan hozzáférés elleni védelmet biztosító intézkedések alkalmazása (hozzáférés védelem, hálózati védelem);
- b) a munkaállomásokra és a szerverekre telepített rosszindulatú szoftverek (malware-ek) kiszűrésére alkalmas programok használata;
- c) a felhasználói eszközökre (munkaállomások, okostelefonok stb.) vonatkozó biztonsági házirendek (adattitkosítás, jelszókezelés, több faktoros hitelesítés) meghozása és ellenőrzése;
- d) az adatközponti eszközökre és az adatközpontra vonatkozó elvárások meghatározása és betartásuk ellenőrzése;
- e) az adatátviteli kapcsolatok megfelelő titkosítása és a kapcsolódást biztosító eszközök fizikai védelme;
- f) a biztonsági mentés [a GDPR 32. cikk (1) bekezdés c) pontja alapján, annak érdekében, hogy az NKFH-nak fizikai vagy műszaki incidens esetén képes legyen arra, hogy a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását kellő időben vissza tudja állítani];
- g) az épületbiztonsággal kapcsolatos fizikai biztonsági intézkedések alkalmazása.

22. § (1) Az NKFH alkalmazásában szervezeti védelmi intézkedések:

- a) a „privacy-by-design” adatvédelem beépítése a folyamatokba;
- b) a szervezeten belüli adatvédelmi ismereteket bővítő és adatvédelmi tudatosságot növelő képzések;
- c) az NKFH közös használatú helyiségeiben és közös használatú eszközei kapcsán – így különösen nyomtatók, másológépek, irattárolók esetében – a személyes adatok célhoz kötött felhasználását, valamint integritását és bizalmas jellegét garantáló intézkedések alkalmazása;
- d) a papíralapú nyilvántartások védelme.

13. Adatvédelmi incidensek kezelése

23. § (1) Amennyiben az NKFH Foglalkoztatottja adatvédelmi incidens bekövetkezésének gyanúját észleli, haladéktalanul köteles az önálló szervezeti egységének vezetőjén keresztül az adatvédelmi tisztviselőt értesíteni.

(2) Az adatvédelmi tisztviselő megvizsgálja az értesítésben foglaltakat, és az adatvédelmi incidens lehetséges hatásainak felmérése és megállapítása érdekében szükség szerint bevonja az NKFH illetékes szervezeti egységeit.

(3) Az adatvédelmi tisztviselő a vizsgálata során figyelembe veszi

- a) az adatvédelmi incidens jellegét;
- b) az érintettek körét, hozzávetőleges számukat;
- c) az incidenssel érintett adatok kategóriáit, az érintett különleges adatokat és azok hozzávetőleges számát, illetve nagyságrendjét;
- d) az adatvédelmi incidensből eredő, valószínűsíthető következményeket;

- e) minden, az adatvédelmi incidens megoldására tett vagy tervezett intézkedést, ideértve az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket;
- f) az elektronikus információbiztonságot is érintő incidensek esetén az Elnöki Kabinet által azonosított további kockázatot;
- g) az adatvédelmi incidensek kezelése és a kapcsolódó kockázatok mérlegelése tárgyában az Európai Adatvédelmi Testület által elfogadott iránymutatást.

24. § (1) Az adatvédelmi incidensek

- a) bizalmassági incidens (pl. személyes adat jogellenes nyilvánosságra hozatala)
- b) sérthetlenségi incidens (pl. személyes adat jogellenes módosítása)
- c) elérhetőségi incidens (pl. jogosulatlan hozzáférés személyes adathoz, illetve jogellenes megsemmisítés) lehetnek.

25. § (1) Ha a rendelkezésre álló adatok alapján egyértelműen megállapítható, hogy adatvédelmi incidens következett be, soron kívül meg kell kezdeni az incidens érintettekre nézve megjelenő hatásainak csökkentését.

(2) Az adatvédelmi tisztviselő a GDPR 33. cikk (1) bekezdésében meghatározott bejelentési kötelezettség határidőben történő teljesítésének sérelme nélkül, írásban - sürgős esetben, szóban - tájékoztatja az Elnököt az adatvédelmi incidens kapcsán tett megállapításairól és az érintettekre vonatkozatható kockázatokról, valamint javaslatot állít össze az adatvédelmi incidens kapcsán teendő intézkedésekről.

(3) Az adatvédelmi incidenst az NKFH köteles indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, bejelenteni a NAIH részére kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Ha a bejelentés nem történik meg 72 órán belül, mellékelni kell hozzá a késedelem igazolását megalapozó indokokat is.

(4) Amennyiben az Elnök a kapott tájékoztatás alapján úgy ítéli meg, hogy az adatvédelmi incidens valószínűsíthetően kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatvédelmi tisztviselő az adatvédelmi incidenst - a GDPR 33. cikk (3) bekezdése szerinti tartalommal - bejelenti a NAIH részére. Amennyiben a rendelkezésre álló információk a teljes körű bejelentést nem teszik lehetővé, szakaszos bejelentést kell tenni.

(5) Amennyiben az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve – a GDPR 34. cikk (3) bekezdésében felsorolt esetek kivételével – az adatvédelmi tisztviselő intézkedik az érintettek tájékoztatása iránt. Amennyiben az adatvédelmi incidenssel érintett természetes személyek tájékoztatására – különösen az érintettek köre vagy a kapcsolattartási adatok biztonságának sérülése miatt – észszerű módon nincs lehetőség, úgy az adatvédelmi tisztviselő az adatvédelmi incidens főbb jellemzőire vonatkozó értesítés soron kívüli közzétételét kezdeményezi az NKFH honlapján.

(6) Az adatvédelmi tisztviselő a bekövetkezett adatvédelmi incidensekről a GDPR 33. cikk (5) bekezdése szerint nyilvántartást vezet, amely tartalmazza:

- a) az adatvédelmi incidensről készült feljegyzés iktatószámát;
- b) az adatvédelmi incidenssel érintett irat vagy nyilvántartás, elektronikus információs rendszer megjelölését vagy azonosítóját;

- c) az incidens észlelésének időpontját és a bekövetkezésének megállapított vagy valószínűsített időpontját;
- d) az érintett személyes adatok körét;
- e) az incidens hatásait, következményeit, valamint az orvoslásukra tett intézkedéseket;
- f) a NAIH részére történő bejelentés időpontját, vagy annak rövid indokolását, ami miatt az adatvédelmi incidens nem került bejelentésre.

VI. FEJEZET

ÉRINTETTI JOGOK, JOGORVOSLAT

14. Érintetti jogok

26. § (1) Az NKFH megfelelő intézkedéseket hoz annak érdekében, hogy a személyes adatok kezelésére vonatkozó, a GDPR 13. cikkben említett valamennyi információt és a 15–22. és 34. cikkek szerinti minden egyes tájékoztatást tömör, átlátható, érthető és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva nyújtsa az érintett részére.

(2) Az érintett jogainak védelme, valamint az adatbiztonsági követelmények teljesülése érdekében az NKFH köteles meggyőződni az érintetti jogait gyakorolni kívánó személy személyazonosságának egyezésétől. Az érintetti joggyakorlás teljesítése érdekében a tájékoztatásnyújtás, az adatokba történő betekintés, illetve az azokról történő másolat kiadása szintén az érintett személyének azonosításához kötött.

(3) Az NKFH az érintett jogai gyakorlására irányuló kérelmét az annak beérkezésétől számított legfeljebb 15 napon belül teljesíti. A kérelem beérkezésének napja a határidőbe nem számít bele.

27. § (1) Az érintett – hozzáféréshez való jogának gyakorlása keretein belül - jogosult arra, hogy az adatvédelmi tisztviselőn keresztül tájékoztatást kérjen arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e, és ha ilyen adatkezelés folyamatban van, jogosult arra, hogy megismerje azt, hogy az NKFH:

- a) milyen személyes adatait;
- b) milyen jogalapon;
- c) milyen adatkezelési célra hivatkozással;
- d) mennyi ideig kezeli;

továbbá, hogy

- e) kinek, mikor, milyen jogszabályi hivatkozás alapján, mely személyes adataihoz biztosított hozzáférést vagy kinek továbbította a személyes adatait;
- f) milyen forrásból származnak a személyes adatai (amennyiben nem az érintett bocsátotta azokat az NKFH rendelkezésére);
- g) az NKFH alkalmaz-e automatizált döntéshozatalt, valamint annak logikáját - ideértve a profilalkotást is.

28. § (1) Az érintett – a helyesbítéshez való jogának gyakorlása keretein belül - az adatvédelmi tisztviselőn keresztül kérheti, hogy az NKFH módosítsa valamely személyes adatát. Amennyiben az érintett hitelt

érdemlően igazolni tudja a helyesbített adat pontosságát, az NKFH a kérést legfeljebb 30 napon belül teljesíti, és erről az érintettet az általa megadott elérhetőségen késedelem nélkül értesíti.

29. § (1) Az érintett – zároláshoz, vagy az adatkezelés korlátozásához való jogának gyakorlása keretein belül - az adatvédelmi tisztviselőn keresztül kérheti, hogy a személyes adatai kezelését az NFKH korlátozza (az adatkezelés korlátozott jellegének egyértelmű jelölésével és az egyéb adatoktól elkülönített kezelés biztosításával) amennyiben:

- a) vitatja a személyes adatai pontosságát (ebben az esetben az NKFH arra az időtartamra korlátozza az adatkezelést, amíg ellenőrzi 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 tiltakozott 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).

30. § Az érintett - tiltakozáshoz való jogának gyakorlása keretein belül - az adatvédelmi tisztviselőn keresztül tiltakozhat az adatkezelés ellen, ha álláspontja szerint az NFKH a személyes adatát a jelen Szabályzatban megjelölt célokkal összefüggésben nem megfelelően kezelné. Ebben az esetben az NKFH köteles igazolni, hogy a személyes adat kezelését 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.

31. § Az érintett - a törléshez, vagy elfeledtetéshez való jogának gyakorlása keretein belül - jelen Szabályzatban ismertetett adatkezelések kapcsán csak akkor élhet a törléshez való jogával, ha az NKFH-ra ruházott közhatalmi jogosítványok gyakorlása keretében végzett feladat végrehajtásához az érintett vonatkozásában kezelt adat nem szükséges.

15. Az érintett jogorvoslathoz való joga

32. § (1) Ha az érintett úgy ítéli meg, hogy az NKFH a személyes adatainak kezelése során megsértette a hatályos adatvédelmi szabályokat, bejelentéssel élhet a NAIH-nál az alábbi elérhetőségek valamelyikén:

- a) székhely: 1055 Budapest, Falk Miksa utca 9-11.,
- b) postacím: 1363 Budapest, Pf. 9.,
- c) e-mail: ugyfelszolgalat@naih.hu, honlap: www.naih.hu.

(2) Az érintettnek lehetősége van adatainak védelme érdekében bírósághoz fordulni, amely ügyben a bíróság soron kívül jár el. Ebben az esetben szabadon eldöntheti, hogy a lakóhelye (állandó lakcím) vagy a tartózkodási helye (ideiglenes lakcím), illetve az NKFH székhelye szerint illetékes törvényszéknél nyújtja-e be keresetét. A lakóhelye vagy tartózkodási helye szerinti törvényszéket megkeresheti a <https://birosag.hu/birosag-kereso> oldalon. Az NKFH székhelye szerint a perre a Fővárosi Törvényszék rendelkezik illetékességgel.

VII. FEJEZET

ZÁRÓ RENDELKEZÉSEK

16. Hatályba lépés

33. § Ez az utasítás a közzétételt követő napon lép hatályba.



