IH-I/64-1/2023.

20/2023. (VI.14) IH elnöki utasítás

az Integritás Hatóság adatvédelmi és adatbiztonsági szabályzatáról

Az európai uniós költségvetési források felhasználásának ellenőrzéséről szóló 2022. évi XXVII. törvény 33. § (1) bekezdés a) pontjában meghatározott hatáskörömben eljárva –figyelemmel a jogalkotásról szóló 2010. évi CXXX. 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 a következő utasítást adom ki:

2.§ Az Integritás Hatóság adatvédelmi és adatbiztonsági szabályzatát (a továbbiakban: Szabályzat) az 1. mellékletben foglaltak szerint állapítom meg és rendelem alkalmazni.

3.§ Ez a határozat az aláírását követő napon lép hatályba.

Budapest, 2023. június 14.

P.H.

Biró Ferenc Pál
elnök
sk.

1. melléklet a 20/2023 (VI.14.) IH elnöki utasításhoz

Az Integritás Hatóság adatvédelmi és adatbiztonsági szabályzata

I. Fejezet

A szabályzat célja és hatálya

1. A szabályzat célja

1.§ A Szabályzat célja az Integritás Hatóság (a továbbiakban: Hatóság) működése és feladatellátása során kezelt személyes adatok védelmének és kezelése rendjének meghatározása, továbbá annak biztosítása, hogy a Hatóság, 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 (továbbiakban: Infotv.) foglaltaknak.

2.§ A Szabályzatot a Hatóság működésére és feladatellátására vonatkozó jogszabályok rendelkezéseivel összhangban, a GDPR és az Infotv. szabályait nem lerontva szükséges értelmezni.

3.§ A Szabályzat alkalmazása során a GDPR 4. cikkében foglalt fogalom-meghatározások az irányadóak.

2. A szabályzat hatálya

4.§ A Szabályzat személyi hatálya kiterjed a Hatóságnál foglalkoztatott valamennyi köztisztviselőre, munkavállalóra, valamint a munkavégzésre irányuló egyéb jogviszony keretében foglalkoztatottra (a továbbiakban együtt: foglalkoztatott), továbbá a Hatósággal, mint megrendelővel szerződéses jogviszonyban álló magánszemélyekre, jogi személyek kapcsolattartóira, továbbá azon szervezetekre, akik az európai uniós költségvetési források felhasználásának ellenőrzéséről szóló 2022. évi XXVII. törvény (a továbbiakban: Eufetv.) 8. §-a alapján megkötött megállapodások keretében személyes adatokat ismernek meg.

5.§ A szabályzat tárgyi hatálya kiterjed a Hatóság kezelésében lévő, működése, feladatellátása során a Hatóság rendelkezésére bocsátott vagy működése, feladatellátása során keletkezett – az adatok megjelenési formájától függetlenül – személyes adatokra.

6.§ A Hatóság adatkezelési tevékenysége során a személyes adatok védelméhez való jog Hatóságon belüli érvényesülését biztosító, más normatív utasításokban foglalt szabályokat a jelen utasításban meghatározott részletszabályokkal együtt kell alkalmazni.

II. Fejezet

A személyes adatok kezelésével kapcsolatos feladatok és felelősségi körök

7.§ A személyes adatok védelméért, az adatkezelés jogszerűségéért a Hatóság elnöke felel. Ennek keretében a Hatóság Elnöke:

a) gondoskodik az adatkezelés személyi és tárgyi feltételeinek biztosításáról, az adatvédelmi és adatbiztonsági rendszer működtetéséről;
b) adatvédelemmel kapcsolatos vizsgálatot rendelhet el;
c) kijelöli a Hatóság adatvédelmi tisztviselőjét, közvetlenül irányítja az adatvédelmi tisztviselő tevékenységét;
d) biztosítja az adatvédelmi tisztviselő számára a hozzáférést a feladatai végrehajtásához szükséges elektronikus rendszerekhez, iratokhoz, egyéb adathordozókhoz, valamint a szakmai ismeretei naprakészen tartásához szükséges feltételeket, jogosultságokat és erőforrásokat a rendelkezésére bocsátja.

8.§ A Hatóság elnöke az elszámoltathatóság alapelvének biztosítása érdekében a Hatóság adatkezeléssel kapcsolatos döntéseinek előkészítéséről, a szabályzatban foglaltak végrehajtásáról, az adatvédelemmel kapcsolatos szabályok foglalkoztatottak általi megismeréséről és betartásáról az Infotv. 25/L. § (1) bekezdése alapján kinevezett adatvédelmi tisztviselő útján gondoskodik.

9.§ A Hatóság adatvédelmi tisztviselője:

a) feladatait más, a munkaköri leírásában meghatározott kötelezettségei mellett, attól függetlenül köteles ellátni;
b) az adatvédelmi tisztviselői tisztségével összefüggő kötelezettségei és feladatai ellátása során nem utasítható, és e tisztségének ellátásával kapcsolatban – a Hatóság Szervezeti és Működési Szabályzatában rögzítettek szerint – közvetlenül a Hatóság elnökének felel;

c) feladatainak ellátása érdekében - a feladatellátásához szükséges mértékben - a Hatóság nyilvántartási rendszereibe betekinthet, szükség esetén minősített adatot is megismerhet.
d) elősegíti a GDPR adatok kezelésére vonatkozó elvekre, az érintett jogaira, a beépített és alapértelmezett adatvédelemre, az adatkezelési tevékenységek nyilvántartására, az adatkezelés biztonságára, valamint az adatvédelmi incidens bejelentésére és arról való tájékoztatásra vonatkozó rendelkezéseinek Hatóságon belüli végrehajtását;
a) tanácsot ad a Hatóság foglalkoztatottjainak a Hatóság adatkezelési folyamatainak jogszerű, az érintettek számára átlátható kialakítása érdekében;
b) a személyes adatok kezelésére vonatkozó jogi előírásokról naprakész tájékoztatást nyújt és azok érvényesítésének módjaival kapcsolatban tanácsot ad;
c) figyelemmel kíséri és ellenőrzi a személyes adatok kezelésére vonatkozó jogi előírások és belső adatvédelmi és adatbiztonsági szabályzatok érvényesülését;
d) elősegíti az érintetteket megillető jogok gyakorlását, elkészíti a Hatóság adatkezeléseire vonatkozó adatkezelési tájékoztatóit;
e) megvizsgálja a Hatóságnál folyamatban lévő, a Hatóság által tervezett vagy módosuló adatkezelések érintettekre gyakorolt kockázatát, szükség esetén javaslatot tesz adatvédelmi hatásvizsgálat lefolytatására, nyomon követi a hatásvizsgálat GDPR 35. cikke szerinti elvégzését;
f) közreműködik az adatvédelmi és adatbiztonsági szabályzat megalkotásában;
g) vezeti a Hatóság adatvédelmi nyilvántartásait;
h) adatvédelmi ellenőrzési tervet készít, amelyet a Hatóság elnöke hagy jóvá;
i) közreműködik az adatvédelmi incidens kezelésében, kivizsgálásában, és a vizsgálat eredménye alapján az adatvédelmi incidenst a GDPR 33. cikke szerint bejelenti a Hatóság részére;
j) adatvédelmi szempontból véleményezi az adatfeldolgozóval, közös adatkezelővel vagy más önálló adatkezelővel kötendő megállapodásokat;
k) ellátja a Hatóság munkatársainak adatvédelmi tudatosító képzését;
l) részt vesz a Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: NAIH) elnöke által összehívott adatvédelmi tisztviselők éves konferenciáján, továbbá – az Elnök kijelölése alapján – képviseli a Hatóságot a Hatóság adatvédelmi és adatkezelési feladatait érintő szakmai rendezvényeken.

10.§ Az adatvédelmi tisztviselő feladatait az adatkezelési műveletekhez fűződő kockázat megfelelő figyelembevételével, az adatkezelés jellegére, hatókörére, körülményére és céljára is tekintettel végzi.

11.§ Az adatkezelés jogszerű fenntartása, kialakítása, illetve az elszámoltathatóság elvének történő megfelelés érdekében a Hatóság szervezeti egységei kötelesek együttműködni az adatvédelmi tisztviselővel.

12.§ A Hatóság foglalkoztatottjai a személyes adataik kezeléséhez és jogaik gyakorlásához kapcsolódó bármely kérdésben – a hivatali út betartása nélkül - közvetlenül fordulhatnak az adatvédelmi tisztviselőhöz.

III. Fejezet

A személyes adatok kezelésének elvei, jogalapja

13.§ A Hatóság

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) a Hatóság felelős azért, hogy adatkezelési tevékenységei megfeleljenek az alapelveknek, továbbá képesnek kell lennie e megfelelés igazolására is (elszámoltathatóság).

14.§ A Hatóság a Hatóságon belüli adatkezelési folyamatait a GDPR alapelvei alapján úgy alakítja és működteti, hogy a Hatóság adatkezelésével elérendő célok és az adatvédelmi követelmények közötti összhang biztosított legyen, a kialakított szabályrendszer ne vezessen a személyes adatok védelmére vonatkozó követelmények sérelméhez, az adatvédelem pedig ne legyen akadálya a jogszerű célok elérésének. A Hatóság 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.

15.§ A Hatóság a működése és feladatellátása során ügyviteli, illetve nyilvántartási célú adatkezelést végez.

16.§ A Hatóság 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.

17.§ A Hatóság 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.

18.§ A Hatósági 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 a Hatóságra 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 a Hatóságra ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges;
f) az adatkezelés a Hatóság 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.

19.§ A Hatóság adatkezelési tevékenységei kapcsán az általánosan használt jogalap a GDPR 6. cikk (1) bekezdés e) pontja (az adatkezelés közérdekű vagy a Hatóságra ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges).

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

20.§ (1) A Hatóság adatkezelésének jogalapja kizárólag abban az esetben lehet az érintett hozzájárulása, ha a Hatóság és az érintett között nincs egyértelműen egyenlőtlen viszony.

(2) Ha az adatkezelés hozzájáruláson alapul a Hatóságnak 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.

(3) Az érvényes hozzájárulás feltételit az adatkezelés megkezdése előtt minden esetben vizsgálni szükséges.

21.§ (1) Amennyiben a személyes adat kezelése a GDPR 6. cikk (1) f) pontján (az adatkezelés a Hatóság vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges) alapul, a Hatóság 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) A jogalap alkalmazhatósága korlátozott, a Hatóság feladatellátása során végzett adatkezelések vonatkozásában e jogalap nem alkalmazható.

22.§ Különleges személyes adatok kizárólag a GDPR 9. cikke alapján kezelhetőek. A különleges személyes adatok kezelése akkor és annyiban jogszerű, ha teljesül legalább egy, a GDPR 6. cikke szerinti, a jogszerűséget megalapozó feltétel, továbbá teljesül legalább egy, a GDPR 9. cikk (2) bekezdésében meghatározott feltétel is.

Adattovábbítás szabályai

23.§ A Hatóság a személyes adatok továbbítására irányuló megkeresés teljesítése során figyelemmel van a GDPR célhoz kötöttségre és adattakarékosságra vonatkozó alapelveinek betartására.

24.§ Adatvédelmi szempontból akkor tekinthető az adattovábbítás jogszerűnek, ha

a) a Hatóság jogosult a személyes adat továbbítására,
b) az adattovábbítás címzettje rendelkezik a személyes adat kezeléséhez szükséges jogalappal vagy az érintett hozzájárulásával,

és az adatkérés célja a fentiekkel összhangban van.

25.§ (1) 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 a Hatóság az adatok kezelőjének minősül-e.

(2) 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 adatok.

26.§ Az Európai Gazdasági Térségbe (a továbbiakban: EGT) irányuló adattovábbítást úgy kell tekinteni, mintha Magyarország területén belüli adattovábbításra kerülne sor. Harmadik országba (nem EGT tagállamba) történő személyes adat a GDPR 44-50. cikkében szabályozott garanciális feltételek fennállta esetén továbbítható.

27.§ Az adattovábbítás jogszerűségének ellenőrzése, valamint az érintettek tájékoztatása céljából az adatot továbbító szervezeti egységek a 2. melléklet szerinti adattartalommal adattovábbítási nyilvántartást kötelesek vezetni.

28.§ A Hatóság szervezeti egységei a szervezeten kívülre történő adattovábbítás jogszerűsége céljából kikérhetik az adatvédelmi tisztviselő véleményét.

IV. Fejezet

Az érintett jogai érvényesülésének biztosításával kapcsolatos feladatok

29.§ A Hatóság 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 - az adatvédelmi

tisztviselő elkészíti az adatkezelési tájékoztatókat melyek tartalmi megfelelőségét, naprakészségét és elérhetőségét köteles figyelemmel kísérni.

30.§ A Hatóság foglalkoztatottjait érintő adatkezelési tájékoztatókat a Hatóság székhelyén elérhető módon kell a foglalkoztatottak számára biztosítani. A Hatóságnál foglalkoztatotti jogviszonyt létesítő személyek számára a belépéshez szükséges dokumentációval együtt, elektronikus úton szükséges megküldeni az őket érintő adatkezelési tájékoztatókat.

31.§ Az adatvédelmi tisztviselő:

a) a Hatósághoz 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 egy hónapon belül tájékoztatja az érintettet – az általa megjelölt formában és módon - a jogai gyakorlására irányuló kérelme nyomán hozott intézkedésekről.

32.§ A Hatóság 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 szerint megvalósuló beadványokat, a teljes bizonyító erejű magánokiratokban foglalt postai úton előterjesztett és az érintett azonosításához szükséges adatokat tartalmazó kérelmeket.

V. Fejezet

Adatvédelmi hatásvizsgálat

33.§ A Hatóság 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.

34.§ Az adatvédelmi hatásvizsgálat lefolytatását a Hatóság adatkezelésért felelős szervezeti egysége írásban kezdeményezi a Hatóság elnökénél.

A 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 stb.,)
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.

35.§ A Hatóság elnöke kikéri az adatvédelmi tisztviselő álláspontját az adatvédelmi hatásvizsgálat szükségessége kapcsán, majd elrendeli az adatvédelmi hatásvizsgálat lefolytatását vagy írásban rögzíti a mellőzésének okait.

36.§ Amennyiben a Hatóság elnöke 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 a Hatóság elnöke részére.

37.§ A tervezett adatkezelés akkor kezdhető meg, amikor a Hatóság elnöke elfogadja a munkacsoport jelentését.

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

VI. Fejezet

Adatbiztonsági intézkedések

39.§ A GDPR 25. cikkével összhangban a Hatóság elnöke olyan technikai és szervezési intézkedéseket hoz, amelyek célja az adatvédelmi elvek érvényesítése, az érintettek jogainak és

szabadságainak védelméhez szükséges garanciák beépítése az adatkezelés teljes folyamatába, a jogszerű és az érintettek számára átlátható adatvédelmi folyamatok kialakítása és működtetése.

40.§ A Hatóság 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;
a) fizikai;
b) szervezeti (adminisztratív) védelmi intézkedéseket alkalmaz.

41.§ A Hatóság alkalmazásában logikai védelmi intézkedések:

a) a személyes adatokat tartalmazó iratok/adathordozók zárható páncélszekrényben történő tárolása;
b) a Hatóság 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 meghozása, mely a d) pontban leírt képességeket és védelmet rendszeresen tesztelik.
f) álnevesítő rendszer kialakítása, amely a személyes adatok anonimizálásával vagy pszeudonimizálásával olyan adatbázist, adatokat állít elő, ami lehetővé teszi a személyes adatokat kezelő rendszerek fejlesztéseinek tesztelését vagy az adatok elemzését olyan szereplők számára, akik ezen adatok megismerésére nem jogosultak.

42.§ A Hatóság 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 software-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 a Hatóságnak 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.

43.§ A Hatóság alkalmazásában szervezeti védelmi intézkedések:

h) a „privacy-by-design” adatvédelem beépítése a folyamatokba;
i) a szervezeten belüli adatvédelmi ismereteket bővítő és adatvédelmi tudatosságot növelő képzések;
j) a Hatóság 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;
k) a papíralapú nyilvántartások védelme.

VII. Fejezet

Adatvédelmi incidensek kezelése

44.§ (1) Amennyiben a Hatóság foglalkoztatottja adatvédelmi incidens bekövetkezésének gyanúját észleli, haladéktalanul köteles az önálló szervezeti egységének vezetőjén keresztül legalább a 3. számú melléklet szerinti tartalommal 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 a Hatóság illetékes szervezeti egységeit.

(3) Amennyiben az adatvédelmi incidens a Hatóság által igénybe vett adatfeldolgozó tevékenységével összefüggésben következett be, az adatvédelmi incidens körülményeinek és a lehetséges kockázatok és hatások kivizsgálásába az adatfeldolgozó képviselőjét is be kell vonni.

45.§ (1) 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.

(2) 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.

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

47.§ (1) Az adatvédelmi incidenst a Hatóság 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 igazolására szolgáló indokokat is.

(2) Amennyiben a Hatóság elnöke 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.

48.§ 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 – ésszerű módon nincs lehetőség, úgy az adatvédelmi tisztviselő az adatvédelmi incidens főbb jellemzőire vonatkozó értesítés soron kívüli közzétételét kezdeményezi a Hatóság honlapján.

49.§ 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.

2. számú melléklet a 20/2023. (VI.14.) IH elnöki utasításhoz

Adattovábbítási nyilvántartás

Adatot továbbító szervezeti egység megnevezése	Az adattovábbítás időpontja	Adattovábbítás jogalapja	A továbbított személyes adtok fajtája

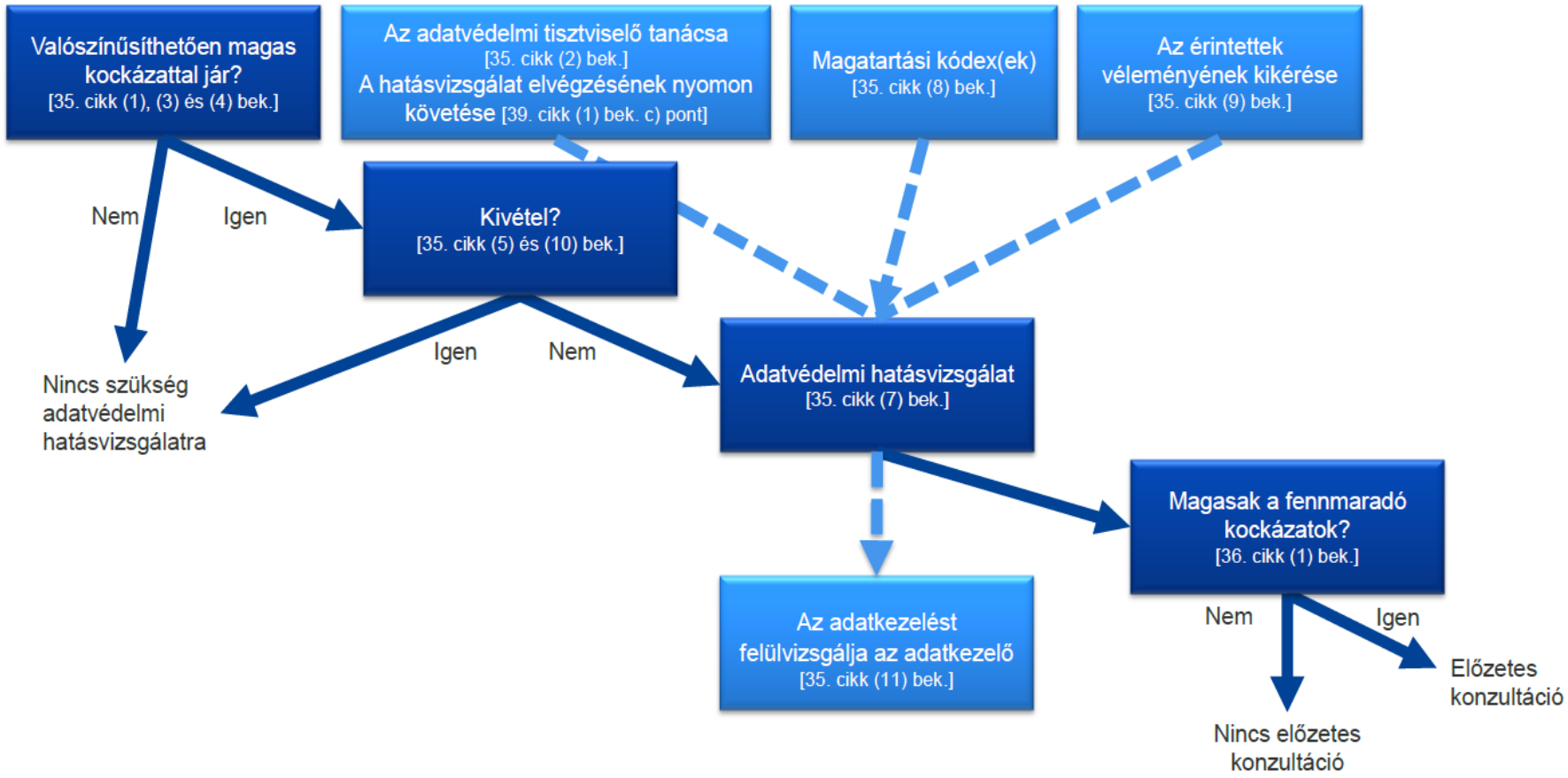
3. számú melléklet a 20/2023. (VI.14.) IH elnöki utasításhoz

Adatvédelmi incidens bejelentése

Az incidenssel érintett szervezeti egység	
Adatvédelmi incidens valószínűsíthető időpontja	
Az incidensről való tudomásszerzés időpontja	
Az adatvédelmi incidens továbbra is fennáll	
Az incidens észlelésének módja	
Egyéb megjegyzések az incidens időpontját érintően	
A személyes adatok	
Bizalmas jellege	Sérült/Nem sérült
Integritása	Sérült/Nem sérült
Rendelkezésre állása	Sérült/Nem sérült
Adatvédelmi incidens jellege (több válasz is elfogadható)	adathalászat
	eszköz elvesztése vagy ellopása
	informatikai rendszer feltörése
	levél elvesztése vagy jogosulatlan felnyitása
	papír alapú dokumentum elvesztése, ellopása, vagy olyan helyen hagyása, amely nem minősül biztonságosnak

	papír alapú dokumentum nem megfelelő módon történő megsemmisítése
	rosszindulatú számítógépes programok pl. Zsarolóprogram
	személyes adatok jogosulatlan megismerése
	személyes adatok jogosulatlan szóbeli közlése
	személyes adatok nagy nyilvánosság előtti jogellenes közzététele
	személyes adatok téves címzett részére történő elküldése
	egyéb
Adatvédelmi incidens okai	külső, rosszhiszemű cselekmény
	külső, rosszhiszeműnek nem minősülő cselekmény
	szervezeten belüli, rosszhiszemű cselekmény
	szervezeten belüli, rosszhiszeműnek nem minősülő cselekmény
	egyéb
Az adatvédelmi incidenssel érintett személyes adatok	
Az adatvédelmi incidenssel érintett személyes adatok becsült száma	
Az adatvédelmi incidenssel érintettek becsült száma	
A valószínűsíthető következmények súlyossága	elhanyagolható
	korlátozott
	jelentős

Hatásvizsgálat szakaszai[1]



[1] Forrás: WP29, 2017