MAGYAR NEMZETI BANK Közzététel: Budapest, 2021. március 5.

**2021-104. elnöki utasítás**

 **a Magyar Nemzeti Bank adatvédelmi szabályzatáról**

**Hatálybalépés:** 2021. március 6.

**Kibocsátó:** Dr. Matolcsy György, elnök

**Készítő szervezeti egység:** Jogi igazgatóság

**Előadó(k):** Dr. Bércesi Tamás, vezető jogász, Jogi igazgatóság

 Dr. Marton Tivadar János, adatvédelmi tisztviselő, Jogi igazgatóság

**Közreműködők:** Humánerőforrás-menedzsment igazgatóság

 Informatikai igazgatóság

 Informatikai biztonsági főosztály

 Felügyeleti koordinációs igazgatóság

 Fenntartható pénzügyi és felügyeleti támogató igazgatóság

 Compliance főosztály

Belső ellenőrzési főosztály[[1]](#footnote-2)

Az utasítás módosításainak hatálybalépései:

Kibocsátó: …………………………………………..

Dr. Matolcsy György s. k.,

elnök

Annak érdekében, hogy a Magyar Nemzeti Bank (a továbbiakban: MNB) 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 (a továbbiakban: GDPR), továbbá az információs önrendelkezési jogról és információszabadságról szóló 2011. évi CXII. törvény (továbbiakba: Infotv.) figyelembevételével teljesítse a Magyar Nemzeti Bankról szóló 2013. évi CXXXIX. törvényben (MNBtv.), valamint az MNBtv. 39. § (1) bekezdésben meghatározott, felügyelt intézményekre vonatkozó ágazati jogszabályokban és az Európai Unió kötelező jogi aktusaiban foglalt feladatait, az MNB belső adatvédelmi szabályait, valamint az adatvédelmi tisztviselő tevékenységével kapcsolatos szabályokat az alábbiak szerint állapítom meg:

**Az utasítás hatálya**

**1. §**

1. Jelen utasítás személyi hatálya kiterjed
* az MNB valamennyi szervezeti egységére és munkavállalójára – ideértve a próbaidejüket, valamint a felmondási idejüket töltő, illetve a munkaviszony megszűnése vagy megszüntetése miatt a munkavégzési kötelezettség alól mentesített munkavállalókat, továbbá a szakmai gyakorlat megszerzésére irányuló, valamint ösztöndíj program keretében foglalkoztatottakat;
* az MNB-vel egyéb foglalkoztatási jogviszonyban vagy a Polgári Törvénykönyvről szóló 2013. évi V. törvény (a továbbiakban Ptk.) rendelkezésein alapuló szerződéses jogviszonyban álló valamennyi személyre.

(2) Jelen utasítás tárgyi hatálya kiterjed az MNB-ben folytatott minden papír alapú és elektronikus adatkezelésre és adatfeldolgozásra a személyes adatok tekintetében. Az utasítás tárgyi hatálya nem terjed ki a közérdekű adatkezelésre és a minősített adatok kezelésére.

**Fogalommeghatározások**

**2. §**

(1) Jelen utasítás alkalmazásában:

1. „személyes adat”: azonosított vagy azonosítható természetes személyre („érintett”) vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például: név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható;
2. „adatkezelés”: a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés;
3. „új adatkezelés”: az új célból és jogalappal kezelt teljesen új adat, valamint az adatkezelés jogalapjának, céljának változása, ideértve az eddigiektől eltérő jogalap, cél szükségessége következtében felmerülő adatkezelés;[[2]](#footnote-3)
4. „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;
5. „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; ha az adatkezelés céljait és eszközeit az uniós vagy a tagállami jog határozza meg, az adatkezelőt vagy az adatkezelő kijelölésére vonatkozó különös szempontokat az uniós vagy a tagállami jog is meghatározhatja;
6. „adatfeldolgozó”: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel;
7. „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 adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére felhatalmazást kaptak;
8. „az érintett hozzájárulása”: az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez;
9. „felsővezető”: az elnök, alelnökök, főigazgató, ügyvezető igazgatók;
10. „megfelelőségi határozat”: az Európai Bizottság határozata a megfelelő védelmi szint biztosításáról;
11. „harmadik ország”: az EGT tagállamain kívüli ország;
12. „szervezeti egység”: az igazgatóságok, az Elnöki kabinet, valamint az igazgatósági szervezethez nem tartozó főosztályok és az igazgatósági szervezethez nem tartozó önálló osztályok, továbbá a Pénzügyi Békéltető Testület, valamint az MNB Felügyelőbizottság titkársága.
13. „szervezeti alegység”: a Bank szervezeti egységein belül szervezeti alegységként főosztály vagy önálló osztály, igazgatósághoz nem tartozó főosztályok esetében osztály vagy csoport hozható létre. A főosztályokon belül osztály, illetve csoport, önálló osztályokon - ideértve az igazgatósági szervezethez nem tartozó önálló osztályokat is - és osztályokon belül pedig csoport hozható létre.
14. „szervezeti egység vezető”: az igazgatóságok, az Elnöki kabinet, az igazgatósági szervezethez nem tartozó főosztályok, valamint az igazgatósági szervezethez nem tartozó önálló osztályok vezetője, a Pénzügyi Békéltető Testület elnöke, az MNB Felügyelőbizottság titkárságának vezetője, továbbá szervezeti egység vezetőnek minősül a szervezeti egységhez nem tartozó munkavállaló esetében a munkavállaló munkavégzését SZMSZ szerint közvetlenül irányító, legalább igazgató besorolású vezető;
15. „adatvédelmi felügyeleti hatóság” a GDPR rendeletben a felügyeleti hatóság részére megállapított feladat- és hatásköröket a Magyarország joghatósága alá tartozó jogalanyok tekintetében a GDPR rendeletben és az Info tv-ben meghatározottak szerint a Nemzeti Adatvédelmi és Információszabadság Hatóság gyakorolja.
16. A jelen utasításban nem meghatározott fogalmakat a [GDPR 4. cikkében](http://www.privacy-regulation.eu/hu/4.htm) meghatározottak szerint kell érteni.

**Alapelvek**

**3. §**

1. Az MNB által, illetve az MNB szervezetében, rendszereiben személyes adat kizárólag jogszerűen, tisztességes eljárás keretei között és átlátható módon kezelhető. Az adatkezelés kizárólag akkor és annyiban jogszerű, ha legalább a [GDPR 6. cikk (1) bekezdésében](http://www.privacy-regulation.eu/hu/6.htm) foglaltak (jogalapok) egyike teljesül. Tisztességes és átlátható az eljárás, amennyiben az érintett könnyen hozzáférhető, közérthető módon megfelelő tájékoztatást kap arról, hogy adatait hogyan gyűjtik, használják fel, azokba hogyan és kik tekintenek be vagy milyen egyéb módon kezelik, valamint azzal összefüggésben, hogy a személyes adatokat milyen mértékben kezelik vagy fogják kezelni.
2. Személyes adatok egyértelműen meghatározott jogszerű célból kezelhetők. A személyes adatok nem kezelhetők ezekkel a célokkal össze nem egyeztethető módon.
3. Az adatkezelés a célra figyelemmel indokolt kell legyen és a legszükségesebb mértékre kell korlátozódjon.
4. Az adatkezelésnek pontosnak és szükség esetén naprakésznek kell lenni, a cél szerinti pontatlan adatkezelés haladéktalanul helyesbítendő, azaz minden észszerű intézkedést meg kell tenni annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat töröljék vagy helyesbítsék.
5. Az adatokat olyan módon kell tárolni, amely az érintettek azonosítását csak a cél eléréséhez szükséges mértékben teszi lehetővé.
6. Az adatok kezelése során a megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítani kell a személyes adatok megfelelő biztonságát, ideértve az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is.
7. Az adatkezelés során folyamatosan képesnek kell lenni az (1)-(6) bekezdésekben foglaltaknak való megfelelés igazolására.

**Harmadik országba vagy nemzetközi szervezet részére történő adattovábbítás általános szabályai**

**4. §**

1. Személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására megfelelőségi határozat, vagy megfelelő garanciák megléte esetén, illetve adatvédelmi felügyeleti hatóság engedélyével kerülhet sor.
2. Megfelelőségi határozat alapján akkor történhet adattovábbítás, ha az Európai Bizottság dokumentáltan megállapította, hogy a harmadik ország, a harmadik ország valamely területe vagy egy vagy több meghatározott ágazata, vagy a szóban forgó nemzetközi szervezet megfelelő védelmi szintet biztosít. Az ilyen adattovábbításhoz nem szükséges külön engedély.
3. Figyelemmel a GDPR 49. cikk (1) bekezdés b) pontjára, amennyiben az adattovábbítás célja az MNB hatósági feladataihoz kapcsolódó valamely eljárás lefolytatása – így különösen a jó hírnév megállapítása – érdekében harmadik országbeli társhatóság, illetve pénzügyi intézmény eseti megkeresése, az adattovábbítás megfelelőségi határozat, illetve a megfelelő garanciák meglétének vizsgálata nélkül elvégezhető.
4. Harmadik országba vagy nemzetközi szervezet részére történő adattovábbítás megkezdése előtt – a (3) bekezdésben meghatározott adattovábbítások kivételével –az adattovábbítással megbízott munkavállaló az intraneten elérhető tájékoztató alapján köteles meggyőződni arról, hogy az adattovábbítás címzettje szerinti ország rendelkezik-e megfelelőségi határozattal.
5. Amennyiben az adattovábbítás címzettje szerinti ország nem szerepel az intraneten elérhető tájékoztatóban, az adattovábbítással megbízott munkavállaló kikéri az adatvédelmi tisztviselő állásfoglalását, hogy a címzett esetében megállapítható-e a [GDPR 46. cikk (2) bekezdésében](http://www.privacy-regulation.eu/hu/46.htm) rögzített megfelelő garanciák megléte, vagy az adattovábbítás egyéb jogalapja meghatározható-e.

**Felelősségek, feladatok, hatáskörök**

**5. §**

1. Az MNB elnöke felügyeli az MNB adatvédelmi tevékenységét, felelős az adatvédelmi szabályok betartásáért. Az elnök jelöli ki az adatvédelmi tisztviselőt, akit az elvégzett feladatokról és ellenőrzésekről évente beszámoltat, gondoskodik a jogszerűséget veszélyeztető körülmények megszüntetéséről.
2. Az adatvédelmi tisztviselő helyettesítését az elnök által kijelölt személy látja el. Az adatvédelmi tisztviselő helyettesítésére megfelelő szaktudással rendelkező személy jelölhető ki.
3. Az adatvédelmi tisztviselő
4. közreműködik, illetve segítséget nyújt az adatkezeléssel összefüggő döntések meghozatalában, az MNB felsővezetőinek vagy szervezeti egységeinek megkeresésére 7 napon[[3]](#footnote-4) belül tájékoztatást és szakmai tanácsot ad az adatkezelést végzők részére a GDPR, valamint az egyéb uniós vagy tagállami, és hazai adatvédelmi rendelkezések szerinti kötelezettségekkel kapcsolatban;
5. ellenőrzi a GDPR, valamint az egyéb uniós vagy tagállami, és hazai adatvédelmi rendelkezéseknek, a személyes adatok védelmével kapcsolatos belső szabályoknak való megfelelést, ideértve a feladatkörök kijelölését, a jelen utasítás személyi hatálya alá tartozó személyek, kiemelten az adatkezelési műveletekben résztvevők tudatosság-növelését és képzését, valamint a kapcsolódó auditokat is;
6. együttműködik az adatvédelmi felügyeleti hatósággal az adatkezeléssel összefüggő ügyekben – ideértve az előzetes konzultációt is – kapcsolattartó pontként szolgál az adatvédelmi felügyeleti hatóság felé, valamint adott esetben bármely egyéb kérdésben konzultációt folytat vele;
7. kérésre szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, a tapasztalatok alapján intézkedési tervet készít, valamint nyomon követi a hatásvizsgálat elvégzését;
8. közreműködik, illetve segítséget nyújt az érintettek jogainak biztosításában;
9. kivizsgálja a hozzá érkezett bejelentéseket, jogosulatlan adatkezelés észlelése esetén annak megszüntetésére hívja fel az adatkezelőt vagy az adatfeldolgozót, tájékoztatja az Informatikai biztonsági főosztályt; a tudomására jutott adatvédelmi incidensekkel kapcsolatban szükség esetén 72 órán belül gondoskodik az incidens adatvédelmi felügyeleti hatósághoz történő bejelentéséről;
10. a működési kockázatkezelés koordinálását és felügyeletét ellátó szervezeti egységet – kérésére – tájékoztatja az MNB adatvédelmi kockázatairól és a tudomására jutott adatvédelmi incidensekről;
11. elkészíti és felülvizsgálja a belső adatvédelmi szabályzatot és a Jogi igazgatóság közreműködésével gondoskodik annak a Szabályozástárban történő közzétételéről;
12. elkészíti az MNB adatkezelésére vonatkozó általános tájékoztatót és gondoskodik annak az MNB honlapján való közzétételéről;
13. vezeti az MNB adatkezelési, adattovábbítási és adatvédelmi incidens nyilvántartásait;
14. a [11. §-ban](#tíz) foglaltaknak megfelelően gondoskodik az adatvédelmi ismeretek oktatásáról, valamint rendszeresen közzéteszi az intraneten az oktatási és a GDPR, valamint az egyéb uniós vagy tagállami, és hazai adatvédelmi rendelkezéseknek, a személyes adatok védelmével kapcsolatos belső szabályoknak való megfelelést támogató tájékoztató anyagokat, útmutatókat, továbbá az adatvédelmi incidensekkel kapcsolatos általános megállapításokat összefoglaló tájékoztatót;
15. annak érdekében, hogy mindenki számára elérhető legyen – az intraneten rendszeresen közzéteszi a több szervezeti egységnél is felmerülő, kérdésekre adott válaszait, a több szervezeti egységnél is felmerülő, hasonló jellegű adatkezelések kapcsán meghatározható jó gyakorlatokat;
16. a személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbításához kapcsolódóan a megfelelőségi határozattal rendelkező országokat tartalmazó tájékoztatót közzéteszi az intraneten és gondoskodik annak szükség esetén történő aktualizálásáról, illetve válaszol a munkavállalók e tárgyban hozzá intézett állásfoglalás-kéréseire;
17. képviseli az MNB-t az adatvédelmi tisztviselők konferenciáján;
18. a [12. § (2) és (3) bekezdéseiben](#tizenegykettőhárom) foglaltaknak megfelelően éves ellenőrzési tervet készít, amely alapján adatvédelmi ellenőrzést végez (belső adatvédelmi ellenőrzési eljárás), melynek eredményéről a következő év március 31-éig írásban tájékoztatja az elnököt, illetve igény esetén a szakterületi vonatkozások tekintetében az illetékes felsővezetőt;
19. szükség esetén – a szervezeti egység vezetőjének közreműködéssel – érdekmérlegelési tesztet készít.

(4) A szervezeti egység vezető vagy felsővezető által erre kijelölt személy

a) gondoskodik arról, hogy a szervezeti egységnél folytatott adatkezelés esetén érvényesüljenek a [3. §](#négy) szerinti alapelvek;

1. az adatkezelést végző, az utasítás személyi hatálya alá tartozó személyek utasítás hatálya alóli kikerülése (pl. munkaviszony megszűnése) esetén gondoskodik az ezen személy által kezelt adatok további jogszerű kezelésének biztosításáról;
2. együttműködik az adatvédelmi tisztviselővel a személyes adatok kezelésének jogalapja, mennyisége, kezelésük mértéke, időtartama, hozzáférhetősége figyelemmel kísérésében;
3. kizárólag a szervezeti egységet érintő új adatkezelés megkezdése előtt, valamint a [10. §-ban](#kilenc) felsorolt nyilvántartásokban szereplő adatkezelések esetében beálló változásokról, lehetőség szerint az új adatkezelés megkezdését vagy a változást megelőző 15 nappal írásban értesíti az adatvédelmi tisztviselőt;
4. új adatkezelésre vonatkozó igény felmerülésekor kikéri az adatvédelmi tisztviselő véleményét az adatkezelés jogszerűsége tekintetében. Jogszabály által elrendelt új adatkezelés esetén a kihirdetést követő 5 napon belül írásban értesíti az adatvédelmi tisztviselőt.
5. jelzi az adatvédelmi tisztviselő felé a külső vállalkozó, külső megbízott személy adatvédelmi oktatására vonatkozó igényt;

g) ellenőrzi az irányítása alá tartozó szervezeti egységnél folytatott tevékenységgel összefüggő adatvédelmi előírások teljesülését;

h) gondoskodik az adatvédelmi vonatkozású folyamatba épített és a vezetői ellenőrzés rendszeres megvalósulásáról;

i) gondoskodik a belső adatvédelmi ellenőrzési eljárást követően készített Intézkedési tervben előírt feladatok elvégzéséről;

j) az adatvédelmi tisztviselő megkeresése alapján részt vesz a szervezeti egységnél folytatott adatkezelés esetén felmerülő kockázatok mennyiségi és minőségi felmérésében, elemzésében, értékelésében, dokumentálásában, és adatokkal, információkkal segíti ezek elvégzését;

(5) A Humánerőforrás-menedzsment igazgatóság a [11. § (2) bekezdésben](#tízkettő) foglaltaknak megfelelően belépéskor dokumentáltan tájékoztatja az új munkavállalót a személyes adatok kezeléséről.

(6) Az Informatikai biztonsági főosztály együttműködik az adatvédelmi tisztviselővel. Az együttműködés keretében:

a) haladéktalanul tájékoztatja az adatvédelmi tisztviselőt minden olyan IT biztonsági incidensről, melynek adatkezeléssel járó kockázata van;

b) informatikai eszközöket is érintő adatvédelmi incidens esetén közreműködik a hatásvizsgálat lefolytatásában és az intézkedési terv összeállításában.

(7) A jelen utasítás személyi hatálya alá tartozó személy felelősséggel tartozik a jelen utasításban foglaltak betartásáért. Az MNB adatkezelést végző munkatársa fegyelmi, kártérítési, büntetőjogi és szabálysértési felelősséggel tartozik a feladat- és hatáskörének gyakorlása során tudomására jutott személyes adatok jogszerű kezeléséért, az MNB nyilvántartásaihoz rendelkezésére álló hozzáférési jogosultságok jogszerű gyakorlásáért, továbbá a tudomására jutott adatvédelmi incidens [6. § (1) bekezdés](#hétegy) szerinti indokolatlan késedelem nélküli bejelentéséért.

**Az adatvédelmi incidens kezelésének szabályai**

**6. §**

1. A jelen utasítás személyi hatálya alá tartozó személy adatvédelmi incidens tudomására jutása esetén köteles az incidensről az adatvédelmi tisztviselőt személyesen, e-mailen vagy telefonon indokolatlan késedelem nélkül értesíteni, a közvetlen felettes vezető és a szervezeti egység vezetőjének egyidejű tájékoztatása mellett.
2. Az adatvédelmi tisztviselő (1) bekezdés szerinti tájékoztatása a jelen utasítás [1. mellékletében](#_melléklet) található, kitöltött adatvédelmi incidens-bejelentő lap (intranetes elérhetősége: [Unipoll (mnb.hu)](https://mnbpoll.mnb.hu/Survey.aspx?surveyid=79653010&lng=hu-HU)) elektronikus megküldésével vagy a tartalmi elemeinek megfelelő információk átadásával teljesíthető, részletesen ismertetve

a) az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit (pl. munkavállaló, gyakornok, ügyfél, külső vállalkozó stb.) és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát;

b) az adatvédelmi incidensből eredő, valószínűsíthető következményeket;

c) az adatvédelmi incidens orvoslására tett vagy megtehető intézkedéseket.

A tájékoztatásnak elsősorban a releváns információkat kell tartalmaznia.

1. Az adatvédelmi tisztviselő a tájékoztatást követően, a beérkezett incidens-bejelentésben szereplő információk alapján rögzíti az incidens adatait az adatvédelmi incidens nyilvántartásba, illetve szükség esetén az érintett szervezeti egység vezetőjével egyeztetve mérlegeli az incidens kockázati szintjét. Amennyiben az incidens valószínűsíthetően magas kockázattal jár, a szervezeti egység vezetőjével konzultálva gondoskodik a szükséges intézkedések megtételéről. Az adatvédelmi incidensek esetében az adatvédelmi tisztviselő mérlegeli, hogy a megtett intézkedésekre és a [GDPR 34. cikk (3) bekezdésére](http://www.privacy-regulation.eu/hu/34.htm) figyelemmel, szükséges-e az érintettek értesítése az adatvédelmi incidensről. Amennyiben az értesítés szükséges, arról az adatvédelmi tisztviselő haladéktalanul gondoskodik.
2. Valószínűsíthetően magas kockázattal járó incidens esetén a szervezeti egység vezetője tájékoztatja az adott szervezeti egység irányításáért felelős felsővezetőt az incidensről, valamint a kapcsolódó intézkedésekről, szükséges nyomonkövetésről.

(5) Az adatvédelmi incidenst az adatvédelmi tisztviselő indokolatlan késedelem nélkül, de legkésőbb a tudomásra jutástól számított 72 órán belül bejelenti az adatvédelmi felügyeleti hatóságnak, kivéve, ha az incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. A bejelentés tényéről, valamint annak tartalmáról az adatvédelmi tisztviselő tájékoztatja az érintett szervezeti egység vezetőjét.

(6) Az adatvédelmi incidens kezelése érdekében, az adatvédelmi tisztviselő a szervezet egység vezetőjével egyeztetve intézkedési tervet fogalmazhat meg a hasonló incidensek elkerülése érdekében. A megfogalmazott intézkedések teljesülését az adatvédelmi tisztviselő folyamatosan követi, illetve támogatást nyújt a szervezeti egység vezetőjének az intézkedések megtételéhez.

1. A bejelentett adatvédelmi incidensek dokumentációjáért az adatvédelmi tisztviselő felel.
2. Az adatvédelmi hatóság felé bejelentett súlyos adatvédelmi incidenssel érintett szervezeti egységet a következő évi adatvédelmi ellenőrzési tervben szerepeltetni kell.

**Adatvédelmi hatásvizsgálat és előzetes konzultáció**

**7. §**

1. Az adatkezelést megelőzően hatásvizsgálatot kell elvégezni, ha az adatkezelés valamely – különösen új technológiákat alkalmazó – típusa, figyelemmel annak jellegére, hatókörére, körülményére és céljaira, valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve.
2. Az adatvédelmi hatásvizsgálat a tervezett adatkezelési műveletnek vagy műveleteknek az adatkezelés érintettekre gyakorolt hatására, kockázatainak felmérésére, a kockázatok kezelésének módjára vonatkozik.
3. Nem kell adatvédelmi hatásvizsgálatot végezni
4. ha az adatkezelés valószínűsíthetően nem jár magas kockázattal;
5. egymáshoz hasonló típusú adatkezelési műveletek esetében, amelyek egymáshoz hasonló magas kockázatokat jelentenek, és az egyik esetben a hatásvizsgálat már lezárult;
6. a [GDPR 35. cikk (10) bekezdésében](http://www.privacy-regulation.eu/hu/35.htm) meghatározott esetben;
7. ha az adatkezelés az adatvédelmi felügyeleti hatóság azon listáján szerepel, amely szerint az adott adatkezelés tekintetében nem kötelező hatásvizsgálatot végezni.

 (4) Az (1) bekezdésben foglaltaknak megfelelően a szervezeti egység vezetője, akinek a feladatkörében az adatkezelés szükségessége felmerül, kikéri az adatvédelmi tisztviselő írásos véleményét.

 (5) Ha az adatvédelmi tisztviselő véleménye szerint az adatkezelés valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatkezelésért felelős szervezeti egység, több felelős szervezeti egység esetén az összefogóként kijelölt szervezeti egység vezetője az adatvédelmi tisztviselővel együttműködve a lehető leghamarabb adatvédelmi hatásvizsgálatot végez.

 (6) Az adatvédelmi hatásvizsgálat során fel kell tárni a kockázatok forrását, jellegét, egyediségét és súlyosságát. A kockázatok azonosítása, súlyozás, prioritások felállítása, a személyes adatok kezelésében részt vevő infrastruktúra elemek felmérése és főbb jellemzőinek összegyűjtése érdekében az érintett szervezeti egység vezető együttműködik az adatvédelmi tisztviselővel.

 (7) Az adatvédelmi tisztviselő az összegyűjtött információk alapján súlyozza az azonosított kockázatokat, majd a tapasztalatok alapján javaslatot tesz a kockázatok csökkentésére, vagy teljes kizárására. A szervezeti egység vezetője, illetve több felelős szervezeti egység esetén az összefogóként kijelölt szervezeti egység vezetője a hatásvizsgálat jóváhagyásával zárja le a vizsgálatot.

 (8) A szervezeti egység vezetője – az adatvédelmi tisztviselő javaslatának figyelembevételével –, az adatvédelmi tisztviselő támogatásával gondoskodik az azonosított kockázatok kezeléséről.

 (9) A hatásvizsgálat megállapításait figyelembe kell venni annak meghatározásakor, hogy mely intézkedések a megfelelőek annak bizonyítására, hogy a személyes adatok kezelése megfelel a GDPR követelményeinek.

(10) Az adatvédelmi hatásvizsgálat eredményét minden esetben dokumentálni kell, és egy esetleges ellenőrzés során az adatvédelmi felügyeleti hatóság kérésére be kell mutatni. A dokumentáció elkészítéséért és kezeléséért az adatvédelmi tisztviselő felel.

(11) Az adatvédelmi hatásvizsgálattal érintett szervezeti egységet a hatásvizsgálat lezártát követő következő évi adatvédelmi ellenőrzési tervben szerepeltetni kell. A lezárt hatásvizsgálatokat időszakosan - lehetőség szerint évente - felülvizsgálni szükséges.

(12) Ha az adatvédelmi hatásvizsgálat szerint az adatkezelési műveletek olyan magas kockázattal járnak, amelyet nem lehet a rendelkezésre álló technológia és a végrehajtási költségek szempontjából is megfelelő intézkedésekkel mérsékelni, az adatkezelést megelőzően az adatvédelmi tisztviselő előzetes konzultációt kezdeményez az adatvédelmi felügyeleti hatósággal.

(13) Az adatkezelés nem kezdhető meg a hatásvizsgálat lezárásáig, illetve az esetleges előzetes konzultáció során tett megállapítások alapján szükséges intézkedések bevezetéséig.

(14) A konzultáció lezárása után az adatvédelmi tisztviselő az érintett szervezeti egység vezetőjének tájékoztatása mellett gondoskodik arról, hogy az adatvédelmi felügyeleti hatóság írásbeli tanácsában foglaltak, illetve az esetlegesen a [GDPR 58. cikkében](http://www.privacy-regulation.eu/hu/58.htm) meghatározott hatáskörökből fakadó intézkedések az adatkezelési gyakorlatba átültetésre kerüljenek.

Adatfeldolgozó kiválasztásának folyamata

8. §

(1) Amennyiben a tervezett adatkezelés adatfeldolgozó megbízását igényli, akkor a leendő adatfeldolgozóval kötendő szerződés felelőse, a szerződés megkötése előtt az adatvédelmi felelőssel egyeztetve – szükség esetén az érintett szervezeti egység bevonásával – köteles megbizonyosodni arról, hogy a leendő adatfeldolgozó képes megfelelő garanciákat nyújtani az adatkezelés GDPR követelményeinek való megfeleléséről és az érintettek jogainak védelmét biztosító, megfelelő technikai és szervezési intézkedések végrehajtásáról.

(2) Amennyiben az adatfeldolgozó igénybevételét jogszabály nem rendeli el, az adatfeldolgozóval adatkezelési megállapodást kell kötni, vagy a megállapodás tartalmát a szerződésbe rögzíteni kell, mely megállapodás vagy szerződési feltétel köti az adatfeldolgozót az adatkezelővel szemben, és amely meghatározza az adatkezelés tárgyát, időtartamát, jellegét és célját, a személyes adatok típusát, az érintettek kategóriáit, valamint az adatkezelő, illetve az adatfeldolgozó kötelezettségeit és jogait a GDPR 28. cikkében foglaltaknak megfelelően.

(3) Az adatfeldolgozói megállapodást, vagy szerződési feltételt lehetőség szerint a szerződés aláírása előtt legalább 5 nappal az adatvédelmi tisztviselő számára véleményezésre meg kell küldeni. Az adatvédelmi tisztviselő a kézhezvételt követő legfeljebb 2 napon belül a megállapodást, illetve szerződési feltételt véleményezi.

(4) A megállapodás, vagy szerződési feltétel véleményezését követően az adatfeldolgozót az adatvédelmi tisztviselő nyilvántartásba veszi.

Az adatkezelési tájékoztatók elkészítésével kapcsolatos feladatok

9. §

(1) A tervezett – az MNB hatósági feladataihoz nem kötődő – adatkezelés megkezdése előtt az adatkezelésért felelős szervezeti egység – szükség esetén az adatvédelmi tisztviselő közreműködését kérve – köteles elkészíteni a [GDPR 13.- 14. cikk](https://www.privacy-regulation.eu/hu/14.htm) szerinti egyedi, az adott adatkezelésre vonatkozó tájékoztatót.

(2) A tájékoztatót, annak publikálása előtt, illetve az adatkezelés megkezdése előtt legalább 5 nappal az érintett szervezeti egység jóváhagyásra megküldi az adatvédelmi tisztviselő részére.

(3) A megküldött tájékoztatót az adatvédelmi tisztviselő legkésőbb a kézhezvételtől számított 2 napon belül véleményezi, illetve jóváhagyja, a tájékoztatót nyilvántartásba veszi.

**Adatkezelési, adattovábbítási és adatvédelmi incidens nyilvántartása**

**10. §**

1. Az adatvédelmi tisztviselő a szervezeti egység vezetőktől összegyűjtött és általuk átadott információk alapján – a [GDPR 30. cikkében](http://www.privacy-regulation.eu/hu/30.htm) foglaltaknak megfelelően – az alábbi nyilvántartásokat vezeti:
	1. adatkezelési nyilvántartás;
	2. adattovábbítási nyilvántartás;
	3. adatvédelmi incidens nyilvántartás.

(2) Az (1) bekezdés a) pontja szerinti nyilvántartás a [GDPR 30. cikkében](http://www.privacy-regulation.eu/hu/30.htm) foglaltakon felül tartalmazza az adatfeldolgozók nyilvántartását is..

(3) Az érintett szervezeti egység vezetője a nyilvántartásban szereplő adatok változása, valamint új adatkezelés megkezdésekor az [5. § (4) bekezdés d) pontjának](#hatötdé) megfelelően tájékoztatja az adatvédelmi tisztviselőt az (1) bekezdésben felsorolt nyilvántartások módosításának szükségességéről. A harmadik személyhez történő adattovábbítást a nyilvántartásban szereplő adatváltozásnak kell tekinteni.

**Adatvédelmi ismeretek oktatása**

**11. §**

(1) Az adatvédelmi ismeretek oktatása keretében az adatvédelmi tisztviselő

a) új adatkezelés, illetve áthelyezés vagy munkakör változásához kapcsolódó adatkezelés megkezdése előtt – az érintett szervezeti egység vezetőjének felkérésére – az adatkezelés tekintetében kiemelten kezelt speciális szabályokat összefoglaló;

b) a munkavállalók részére évente legalább egy alkalommal az adatkezelési és adatvédelmi kérdések aktualitásaira vonatkozó, elsősorban a gyakorlatban hasznosítható ismeretek átadását célzó;

c) külső vállalkozóknak, külső megbízott személyeknek a [5. § (4) bekezdés e) pontja](#hatöte) szerint beérkező igény alapján az a) pontban rögzített általános ismeretekre vonatkozó;

d) egyéb, a szervezeti egység vezetők részére, valamint a szakterületi igények esetén felmerülő általános vagy speciális adatvédelmi ismeretekről szóló;

e) a Humánerőforrás-menedzsment igazgatóság felkérésére az új belépők számára szervezett orientációs képzéseken adatvédelmi alapismereti

oktatást tart.

(2) Minden munkavállaló részére felvételekor a Humánerőforrás-menedzsment igazgatóság illetékes munkatársa az MNB által elfogadott adatkezelési alapelveket, általános szabályokat, valamint az MNB egyes szakterületei által az adatkezelés tekintetében kiemelten kezelt speciális szabályokat összefoglaló „adatkezelési tájékoztatót” köteles – az [5. § (5) bekezdésnek](#öthatbé) megfelelően dokumentált módon – átadni, ami általános adatkezelési oktatási anyagnak tekintendő.

(3) Az (1) bekezdésben foglalt oktatások ismeretanyagainak, valamint a (2) bekezdésben foglalt általános adatkezelési tájékoztatónak az elkészítése és biztosítása – ideértve annak közzétételét az intraneten – az adatvédelmi tisztviselő feladata.

1. Az (1) bekezdésben felsorolt oktatások megszervezéséről – az (1) bekezdés e) pont kivételével - és megtartásáról az adatvédelmi tisztviselő gondoskodik.

**Belső adatvédelmi ellenőrzési eljárás**

**12. §**

1. A belső adatvédelmi ellenőrzési eljárás célja, hogy az adatvédelmi tisztviselő meggyőződjön arról, hogy az egyes szervezeti egységek az adatvédelemmel kapcsolatos jogszabályoknak és belső szabályoknak megfelelően kezelik az adatokat.
2. Az adatvédelmi tisztviselő éves ellenőrzési tervet készít az adott naptári évben ellenőrzés alá kerülő szervezeti egységekről. Az éves ellenőrzési tervnek az ellenőrzés alá vont szervezeti egység, szervezeti alegység nevét és az ellenőrzés főbb szempontjait és várható időpontját kell tartalmaznia.
3. Az éves ellenőrzési tervet  legkésőbb adott év március 31. napjáig kell elkészíteni és az elnök részére jóváhagyásra beterjeszteni az előző évről szóló, a [5. § (3) bekezdés o) pontjában](#ötkettőká) meghatározott tájékoztatóval együtt. A jóváhagyott ellenőrzési tervről az érintett szervezeti egység vezetőket a DPO tájékoztatja.
4. Adatvédelmi szempontból indokolt esetben az adatvédelmi tisztviselő önállóan, vagy az elnök elrendelése alapján, illetve a hatásvizsgálat vagy egyéb információk – különösen adatvédelmi incidensek – alapján beazonosított kockázatok esetén rendkívüli ellenőrzést is lefolytathat. Rendkívüli ellenőrzésnek minősül az éves ellenőrzési tervben nem szereplő ellenőrzés. A rendkívüli ellenőrzést az éves ellenőrzési tervben szereplő ellenőrzésekre vonatkozó, az (5)-(7) bekezdésekben foglalt eljárási szabályok szerint kell lefolytatni.
5. Helyszíni ellenőrzés esetén az adatvédelmi tisztviselő az ellenőrzés lefolytatásáról az érintett szervezeti egység vezetőjét e-mailben tájékoztatja legkésőbb az ellenőrzés előtt 15 nappal. A tájékoztató e-mail tartalmazza az ellenőrzés tárgyát és az eljárás kezdő időpontjára vonatkozó javaslatot is. A szervezeti egység vezetője köteles gondoskodni arról, hogy az adatvédelmi tisztviselő a javasolt időpontban megkezdhesse ellenőrzését, illetve szükség esetén új időpontra tesz javaslatot.
6. Az ellenőrzés során az adatvédelmi tisztviselő a szervezeti egység irodahelyiségeibe beléphet, a szervezeti egység irataiba betekinthet, a szervezeti egység munkatársaitól tájékoztatást kérhet adott üggyel kapcsolatos adatkezelésről.
7. Az adatvédelmi tisztviselő az ellenőrzés eredményéről írásban tájékoztatja az ellenőrzés alá vont szervezeti egység vezetőjét. Amennyiben az érintett szervezeti egység munkatársai az ellenőrzési jelentés tartalmával nem értenek egyet, észrevételeiket a szervezeti egység vezetőjének továbbítják, aki jóváhagyása esetén lehetőség szerint az ellenőrzés eredményéről szóló tájékoztatás kézbesítésétől számított 15 napon belül, írásban jelzi az adatvédelmi tisztviselőnek, aki a beérkezett észrevétel áttekintését követően egyetértése esetén módosítja a jelentést, vagy megjeleníti az észrevételeket a (10) bekezdésben szereplő elnöki összefoglaló jelentésben.
8. Ha az adatvédelmi tisztviselő megállapítja, hogy az adatkezelés az ellenőrzés alá vont szervezeti egységnél nem a belső szabályoknak és a jogszabályoknak megfelelően történik, javaslatot tesz a szabályszerű adatkezelés – meghatározott határidőn belüli – helyreállítására. A javaslatot megküldi az érintett szervezeti egység vezetőjének. A javaslat alapján megtett intézkedésekről az azok bevezetésére közösen megállapított határidő után a szervezeti egység vezetője írásban tájékoztatja az adatvédelmi tisztviselőt, aki a megtett intézkedéseket, illetve a javaslatban foglaltak betartását bármikor jogosult ellenőrizni.
9. Az adatvédelmi tisztviselő jogsértés megállapítása hiányában is jogosult az általa legjobb gyakorlatnak ítélt szervezeten belüli és kívüli eljárásokról az éves vagy rendkívüli ellenőrzési jelentésében az adatkezelő szervezeti egységek vezetőinek tájékoztatást adni, továbbá javasolni adott eljárás vagy eljárások alkalmazását a jövőre nézve. A adatvédelmi tisztviselő ezen javaslatok követésére felkérheti a szervezeti egység vezetőjét, továbbá amennyiben szükségesnek ítéli, külön vizsgálat tárgyává is teheti a javaslatok követését.
10. A adatvédelmi tisztviselő évente egy alkalommal, legkésőbb az adott év március 31. napjáig összefoglaló jelentést készít lefolytatott ellenőrzésekről az elnök részére, igény esetén a szakterületi vonatkozások tekintetében az illetékes felsővezető részére. Emellett az elnök bármely ellenőrzéssel kapcsolatban soron kívüli tájékoztatást kérhet a adatvédelmi tisztviselőtől.
11. A (10) bekezdésben hivatkozott jelentés tartalmazza a lefolytatott ellenőrzésre vonatkozó összefoglaló jelentést, a tárgyévi ellenőrzési tervet, valamint az érintetti jogok gyakorlására vonatkozó tájékoztatót.

**Az érintett jogainak érvényesítésével kapcsolatos eljárás**

**13. §**

1. Amennyiben bármely, az érintettől származó személyes adat kezelésére vonatkozó kérelem érkezik az MNB-hez, az érintett szervezeti egység vezetője 5 napon belül kikéri az adatvédelmi tisztviselő véleményét annak eldöntése érdekében, hogy a kérelem teljesíthető-e.
2. Ha az adatvédelmi tisztviselő – figyelemmel a szakterületi szabályzatokra is – a kérelmet teljesíthetőnek minősíti – az e) pontban foglaltak kivételével – a kérelem benyújtásától számított 25 napon belül, a szervezeti egység vezetőjének közreműködése mellett,
	1. ha az adatokat az érintettől gyűjtötték, gondoskodik arról, hogy az érintett a kezelt adatokról a [GDPR 13. cikk (1) bekezdése](http://www.privacy-regulation.eu/hu/13.htm) szerinti tájékoztatást megkapja;
	2. abban az esetben, ha az adatokat nem az érintettől gyűjtötték, az adatvédelmi tisztviselő az adatkezelést megelőzően dönt arról, hogy az adatkezelésről – a [GDPR 14. cikkére](http://www.privacy-regulation.eu/hu/14.htm) figyelemmel – kell-e, és ha igen, milyen módon kell tájékoztatni az érintettet;
	3. hozzáférésre irányuló igény esetén az Informatikai igazgatóság bevonásával tájékozódik az érintett szervezeten belüli adatkezeléséről, illetve gondoskodik arról, hogy az érintett a [GDPR 15. cikk](http://www.privacy-regulation.eu/hu/15.htm) szerinti tájékoztatásokat megkapja;
	4. helyesbítésre vonatkozó igény esetén az érintett szervezeti egység vezetőjének tájékoztatása mellett, az Informatikai igazgatóság közreműködésével gondoskodik a helyesbítés adatkezelésben történő átvezetéséről, illetve az adattovábbítási nyilvántartásra figyelemmel az esetleges címzettek tájékoztatásáról; amennyiben a helyesbítési igény az iratkezelő rendszerben rögzített adatokra vonatkozik, tájékoztatja az érintettet, az iratkezelési szabályok megtartása mellett megtehető intézkedésekről;
	5. törlésre irányuló kérelem esetén mérlegeli a törlési kérelem végrehajthatóságát. Amennyiben a kérelem végrehajtható, az adatkezelésért felelős szervezeti egység és az Informatikai igazgatóság közreműködésével gondoskodik arról, hogy az érintettről kezelt személyes adatok az MNB minden alrendszerére kiterjedő módon visszaállíthatatlanul törlésre kerüljenek, továbbá az adattovábbítási nyilvántartás adataira figyelemmel, szükség esetén értesíti a törlési kérelemről az esetleges adattovábbítások címzettjeit. Amennyiben a törlési igény az iratkezelő rendszerben rögzített adatokra vonatkozik, tájékoztatja az érintettet, az iratkezelési szabályok megtartása mellett megtehető intézkedésekről;
	6. az adatkezelés korlátozásához való jog gyakorlása iránti kérelem esetén, amennyiben a [GDPR 18. cikk (1) bekezdés a)-d) pontjai](http://www.privacy-regulation.eu/hu/18.htm) közül valamelyik teljesül, haladéktalanul gondoskodik arról, hogy az adatkezelő szervezeti egységek tájékoztatást kapjanak a korlátozás alá eső adatok kezelésének módjáról;
	7. adathordozhatósághoz való jog gyakorlása iránti kérelem esetén mérlegeli annak végrehajthatóságát. Amennyiben a kérelem végrehajtható, az Informatikai igazgatóság közreműködésével gondoskodik arról, hogy az érintett a rá vonatkozó adatokat széles körben használt géppel olvasható formátumban megkapja, illetve erre vonatkozó igény esetén azok az érintett által meghatározott adatkezelőnek továbbításra kerüljenek;
	8. tiltakozáshoz való jogra hivatkozó kérelem esetén mérlegeli, hogy az adatkezelést olyan kényszerítő erejű jogos okok indokolják-e, amelyek elsőbbséget élveznek az érintett érdekeivel, jogaival és szabadságaival szemben, vagy amelyek jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódnak. Ilyen jogos okok hiányában gondoskodik a kezelt adatok törléséről.
3. Az adatvédelmi tisztviselő a kérelem teljesítésének elutasításáról dönt ha,
	1. az érintett megfelelő azonosítására nincs lehetőség, kivéve, ha az érintett az azonosítását lehetővé tévő kiegészítő információkat nyújt;
	2. az érintett kérelme olyan adat helyesbítésére, törlésére irányul, amely adat kezelését jogszabály írja elő;
	3. az érintett kérelme ellenében bizonyítható az adatkezelés jogszerűsége.
4. Az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény 54. § szerinti - adattovábbítási nyilvántartással kapcsolatos - elektronikus úton érkezett kérelem esetében
	1. a kérelmet tartalma alapján a központi iktató, iktatás után a Magyar Nemzeti Bank Iratkezelési szabályzatáról szóló főigazgatói utasításban rögzített módon a Jogi igazgatóság részére, az adatvédelmi tisztviselőnek továbbítja,
	2. az adatvédelmi tisztviselő a 10. § (1) bekezdése szerinti nyilvántartások alapján, illetve szükség esetén az ezen nyilvántartások szerinti felelős szervezeti egység bevonásával, a kérelem beérkezésétől számított 3 napon belül a választ elektronikus úton megküldi a kérelmező részére.
5. A kérelem elutasítása esetén - a (4) bekezdés szerinti kérelem kivételével - annak benyújtását követő 25 napon belül az adatvédelmi tisztviselő tájékoztatja az érintettet az intézkedés elmaradásának okairól, valamint arról, hogy az érintett panaszt nyújthat be az adatvédelmi felügyeleti hatóságnál, és élhet bírósági jogorvoslati jogával.

**Záró rendelkezések**

**14. §**

Jelen utasítás a közzétételét követő napon lép hatályba. Ezzel egyidejűleg hatályát veszti a Magyar Nemzeti Bank belső adatvédelmi és adatbiztonsági szabályzatáról szóló 2018-108. elnöki utasítás.

# melléklet

a 2021-104. elnöki utasításhoz

**Adatvédelmi incidens bejelentő lap**

Az adatvédelmi incidenssel érintett szervezeti egység megnevezése:

Az adatvédelmi incidenssel érintett szervezeti alegység megnevezése (Főosztály, osztály):

Szervezeti egység vezető neve:

Az incidens bekövetkezésének pontos ideje (nap, óra perc):

Az incidens észlelésének pontos ideje (nap, óra, perc):

Az incidens jellegének ismertetése:

1. Az incidens körülményeinek leírása (Annak ismertetése, hogy történt az incidens: pl. elveszett laptop, telefon, hibás címre küldött e-mail):
2. Az érintettek kategóriáinak, és valószínűsíthető számának ismertetése (Azok meghatározása akiknek jogait, szabadságait az incidens befolyásolhatta: pl. ügyfelek, kapcsolattartók, valameny adatbázisban szereplők):
3. Az adatok kategóriáinak, és valószínűsíthető számának ismertetése (Az adatok körét és mennyiségét kell meghatározni pl. név, anyja neve, lakcím):

Az adatvédelmi incidensből eredő valószínű következmények (Ha lehetséges, annak leírása, hogy az érintettek, milyen kárt szenvedhettek az incidens következtében: pl. egy elveszett laptopon tárolt adatbázis, mely akár személyes adatokat tartalmaz, a reputációs kockázat mellett ronthatja az érintettek megítélését és sértheti személyiségi jogaikat):

Az adatvédelmi incidens orvoslására megtett, vagy megtehető intézkedések (Ha van ilyen annak leírása, melyet már megtett az adatkezelő, illetve amit még tehet pl. a rossz helyre küldött e-mailt megkísérelte visszavonni, tájékoztatta a címzettet a tévedésről, feljelentést tett, továbbá javasolja az érintettek tájékoztatását):

1. A Magyar Nemzeti Bank Szervezeti és Működési Szabályzatának I.6.1. pontjában foglaltak szerint. [↑](#footnote-ref-2)
2. Nem tekinthető új adatkezelésnek az új hatósági eljárás, új hatósági ellenőrzés, vizsgálat megindítása és lefolytatása, vagy az az eset, amikor az adatok köre, érintettek köre változik tekintettel arra, hogy a jogalap, illetve az adatkezelés célja nem módosul. [↑](#footnote-ref-3)
3. az utasításban szereplő határidők naptári napban értendők [↑](#footnote-ref-4)