A Magyar Nemzeti Bank 12/2020. (XI.6.) számú ajánlása
a távmunka és távoli hozzáférés informatikai biztonsági követelményeiről

I. Az ajánlás célja és hatálya

Az informatikai és telekommunikációs technológiák rohamos fejlődése mind nagyobb teret enged a távmunka elterjedésének. A növekvő igényeket a kényelmen túl más gazdasági és társadalmi szempontok is kikényszerítették, a pandémiás helyzet okozta kijárási korlátozások miatt olyan intézményeknél is megjelent a távmunka tömeges igénye, ahol korábban nem, vagy csak korlátozott keretek közt éltek a munkavégzés ilyen formájával.

Ennek okán egyre nagyobb teret nyertek a csoportmunka és videókonferencia megoldások, amelyek gyakran felhőszolgáltatásokon alapulnak, és olyan infrastruktúrákon keresztül valósulnak meg, amelyek felett az intézmény nem rendelkezik teljes kontrollal.

A pénzügyi közvetítőrendszer felügyeletével kapcsolatos feladatkörében eljáró Magyar Nemzeti Bank (a továbbiakban: MNB) a vonatkozó jogszabályi előírások rendelkezéseivel összhangban biztosítani kívánja, hogy a pénzügyi közvetítőrendszer intézményei a munkavállalók és egyéb szerződéses jogviszony keretében az intézmény belső hálózatához, illetve az intézmény érzékeny adataihoz vagy rendszereihez hozzáféréssel rendelkező személyek (együtt: távoli felhasználók) számára biztosított távoli, irodán kívüli munkavégzés lehetőségét (továbbiakban: távoli hozzáférés) a megfelelő tárgyi és technikai feltételek mellett, a vonatkozó jogszabályok betartásával és a biztonsági követelmények figyelembevételével legyenek képesek megteremteni.

Az ajánlás célja a távmunka és távoli hozzáférés informatikai biztonsági követelményeivel kapcsolatban az MNB elvárásainak rögzítése, és ezzel a jogalkalmazás kiszámíthatóságának növelése, a vonatkozó jogszabályok egységes alkalmazásának elősegítése és az innovációk támogatása.

Az ajánlás címzettjei a Magyar Nemzeti Bankról szóló 2013. évi CXXXIX. törvény 39. §-ában meghatározott jogszabályok hatálya alá tartozó szervezetek és személyek (a továbbiakban együtt: intézmény).

Jelen ajánlás a jogszabályi rendelkezésekre teljeskörűen nem utal vissza az elvek és elvárások megfogalmazásakor, az ajánlás címzettjei a kapcsolódó jogszabályi előírásoknak való megfelelésre azonban természetesen továbbra is kötelesek.

Jelen ajánlás adatkezelési, adatvédelmi kérdésekben iránymutatást nem fogalmaz meg, a személyes adatok kezelése vonatkozásában semmilyen elvárást nem tartalmaz, és az abban foglalt követelmények semmilyen módon nem értelmezhetők személyes adatok kezelésére vonatkozó

felhatalmazásnak. Az ajánlásban rögzített felügyeleti elvárások teljesítésével összefüggésben történő adatkezelés kizárólag a mindenkor hatályos adatvédelmi jogszabályi rendelkezések betartásával végezhető.

II. Általános elvárások, fogalmak

1. A jelen ajánlás alkalmazásában *távmunka* az intézmény telephelyétől elkülönült helyen munkaviszonyból vagy egyéb szerződéses jogviszonyból származó feladat rendszeres vagy eseti jellegű ellátását jelenti, amelyet számítástechnikai eszközzel végeznek és eredményét elektronikusan továbbítják. A *távoli hozzáférés* tágabb, technikai fogalom, mely az intézmény belső hálózatához, informatikai erőforrásaihoz való külső hozzáférést jelent (függetlenül a felhasználó jogviszonyától).

2. Elvárt, hogy az intézmény fokozottan ügyeljen a távmunkával kapcsolatos informatikai biztonsági kockázatokra, valamint az intézmény és ügyfelei adatainak teljeskörű védelmére, különös tekintettel azok távmunka során történő kezelésének és feldolgozásának kockázataira.

3. Az ajánlásban foglaltak az informatikai rendszer védelméről szóló 8/2020 (VI. 22.) MNB ajánlással [a továbbiakban: 8/2020. (VI. 22.) MNB ajánlás], valamint a közösségi és publikus felhőszolgáltatás igénybevételéről szóló 4/2019. (IV. 1.) MNB ajánlással [a továbbiakban: 4/2019. (IV. 1.) MNB ajánlás]) együtt alkalmazandók.

III. A távmunka szabályozása

4. Az MNB elvárja, hogy az intézmény rendelkezzen a távmunkát és a távmunkához szükséges hozzáféréseket szabályozó dokumentummal, amely szerves részét képezi az intézmény informatikai biztonsági szabályozási rendszerének. Elvárt, hogy a szabályozó dokumentum legalább az alábbiakat tartalmazza:
   a) a távmunka fogalmának, valamint feltételeinek egyértelmű meghatározása;
   b) a távmunkában elvégezhető folyamatok, részfolyamatok és tevékenységek köre;
   c) a távmunkában elérhető rendszerek, adatkörök listája;
   d) a távmunkára jogosult szerepkörök vagy munkakörök listája;
   e) a kiemelt, nagyobb rendszerterhelés esetén a távoli hozzáférés igénybevételénél prioritást élvező felhasználók vagy munkakörök listája,
   f) a távmunka elrendelésének és visszavonásának eljárásrendje (igénylés, jóváhagyás, visszavonás, időtartam);
   g) a kiosztott távmunka-engedélyek nyilvántartásának helye;
   h) a távmunka során alkalmazott azonosítási és hitelesítési szabályrend[1];

[1] Az intézmény informatikai biztonsági szabályozási rendszerében foglaltak szerint.

i) a távmunka során betartandó speciális adatkezelési és adatfeldolgozási szabályok (hozzáférés, tárolás, továbbítás, törlés stb.);
j) a távmunka során a kiemelt felhasználói (pl. adminisztrátori és rendszergazdai) hozzáférés külön szabályozása[1];
k) az általános naplózási követelményeken felül a távmunka során felmerülő naplógyűjtési követelmények, a naplóbejegyzésekről készült riportok tartalma és az azokhoz való hozzáférés joga[1];
l) a távmunkához engedélyezett és elvárt eszközök típusainak listája;
m) a távmunkához használt eszközöket (notebook, PC, okostelefon, internet elérés, kommunikációs szoftver stb.) biztosító szervezeti egység, személy meghatározása, az eszközök igénylésének eljárásrendje;
n) a távmunkához kapcsolódó eszközök (pl. token, tanúsítvány) átvételi eljárásrendje, amely előírja legalább a távoli felhasználó távmunkára vonatkozó biztonsági szabályok megismerésére és elfogadására vonatkozó írásbeli nyilatkozat megtételét,
o) a távmunka igénybevételéhez szükséges otthoni informatikai és informatikai biztonsági feltételek meghatározása;
p) a távoli felhasználótól elvárt általános és egyes kiemelt biztonságot igénylő területek (pl. treasury) távmunkában történő ellátásához szükséges speciális biztonságtudatos viselkedés, valamint az erre vonatkozó szabályok felsorolása és az azok oktatására vonatkozó szabályok;
q) a távmunka befejezésének eljárásrendje és a telephelyre történő visszatérés szabályai;
r) a távmunkában használt felhasználói eszközök karbantartási, javítási folyamatának szabályai;
s) a távmunka során alkalmazandó adathordozó-megsemmisítési eljárásrend;
t) a papír alapú dokumentumok kezelésének tiltása, és a kiemelten indokolt esetekre vonatkozó külön szabályozása;
u) a kiemelt biztonságot igénylő területek (pl. treasury) távmunkában történő ellátására vonatkozó speciális technikai feltételek és biztonsági szabályok; valamint
v) a távmunka során használt eszközök elvesztése, eltulajdonítása, kompromittálódása esetén követendő eljárásrend.

IV. A távmunka informatikai biztonsági kockázatelemzése

5. Az MNB elvárja, hogy az intézmény az informatikai biztonsági kockázatelemzése keretében térjen ki a távmunka során felmerülő speciális informatikai biztonsági kockázatokra is, és gondoskodjon a kockázatcsökkentő intézkedési tervek[2] kidolgozásáról, az intézkedések végrehajtásához szükséges feltételek biztosításáról, az intézkedések végrehajtásáról és a megtett intézkedések ellenőrzéséről. A kockázatelemzés során az intézmény térjen ki legalább a távmunkában résztvevő személyekre, folyamatokra és rendszerekre (beleértve az

[2] Az intézkedési tervekkel kapcsolatos követelményeket a 8/2020. (VI. 22.) MNB ajánlás tartalmazza.

adatátviteli rendszereket is), valamint az ezekben a rendszerekben feldogozott adatokra, továbbá a távmunka helyszínéből fakadó kockázatokra.

6. Az MNB elvárja, hogy az intézmény a távmunkához kapcsolódó kockázatelemzését rendszeresen, legalább a jogszabályban foglalt gyakoriság szerint vizsgálja felül[3], és a feltárt kockázatokat, valamint azok kezelésének nyomon követesét dokumentálja.

V. A távmunka infrastruktúrájának kiépítése

7. Az intézmény a távmunkát biztosító informatikai infrastruktúrájának kiépítése során támaszkodhat a már meglévő eszközeire, rendszereire vagy szükség szerint bővítheti azokat, illetve újakat építhet ki.

8. Az eszközbeszerzés, üzembehelyezés és üzemeltetés során az MNB a következőket várja el:
   a) a távmunkában a távoli hozzáférés minden esetben titkosított csatornán keresztül történjen;
   b) az intézmény gondoskodjon a távmunka során használt összes rendszerhez a megfelelő számú távoli hozzáférés licensz beszerzéséről és gondoskodjon a licenszek nyilvántartásáról;
   c) a távmunkához szükséges infrastruktúra kiépítése során az intézmény határozza meg a rendszerek elvárt rendelkezésre állását és ennek kiszolgálásához szükséges kapacitást, valamint a riasztási és az architektúra-bővítési küszöbértékeket;
   d) az intézmény kockázatfelmérés alapján határozza meg a távmunkához használható eszközök típusát, menedzselhetőségét (intézményi, harmadik fél által menedzselt, távoli felhasználó saját eszköze);
   e) az intézmény határozza meg a távolról csatlakozó eszközök hozzáférésének módját a belső hálózaton található erőforrásokhoz (pl. terminál szerver, nyomtatók) – és a szükséges mértékben határozzon meg különböző biztonsági szinteket és kapcsolódási típusokat;
   f) az intézmény előzetesen határozza meg és rendszeresen vizsgálja felül a működés során elvárt paramétereket (adatkapcsolatok száma, adatkapcsolatok eloszlási ideje és helye, forgalmazott adatmennyiség stb.);
   g) a távmunka során az üzleti folyamatokat támogató felhő alapú szolgáltatások (csoportmunka felület, kommunikációs alkalmazás stb.) igénybevétele esetén is biztosítsa a 4/2019. (IV. 1.) MNB ajánlásnak való megfelelést;
   h) a távoli hozzáférést biztosító szolgáltatások beszerzésénél az intézmény lehetőleg olyan, referenciákkal, nemzetközi biztonsági tanúsítványokkal rendelkező szolgáltatót, illetve megoldást válasszon, aki vagy amely nem szerepel sem az intézményi, sem az interneten elérhető, általánosan elfogadott tiltólistákon; továbbá

[3] A 8/2020 (VI.22.) ajánlás 3.4.2. pontja.

i) a távoli felhasználó és eszköze hitelesítéséhez az intézmény használjon többfaktoros autentikációt, mely során az erős hitelesítést biztosító faktort – például tokent, dinamikus kódot vagy tanúsítványt – megbízható forrásból szerezze be.

VI. A távmunkában használt eszközök

9. A távmunka végzéséhez elsősorban az intézmény által biztosított és menedzselt eszközök ajánlottak (notebook, okostelefon, tablet stb.). Amennyiben az intézmény nem tud megfelelő számú és minőségű eszközt biztosítani a távmunka ellátásához, vagy az a hozzáférések típusának függvényében a biztonsági kockázatokkal arányosan nem indokolt, akkor a szükséges kockázatcsökkentő intézkedések megtétele mellett, a megfelelő kontrollintézkedések alkalmazásával az intézmény engedélyezheti a távoli felhasználók számára saját eszköz, valamint harmadik felek eszközeinek használatát.

10. Az MNB elvárja, hogy az intézmény a távoli hozzáférések során az tiltsa, illetve megfelelő technológiai megoldásokkal akadályozza a nyilvánosan elérhető számítógépek, valamint technológiai, illetve adminisztratív eszközökkel a nyilvánosan elérhető vezetékes és vezeték nélküli hálózatok (könyvtári, internetkávézós stb.) használatát.

VI.1. Az intézmény eszközeinek használata

VI.1.1. A notebookokra és munkaállomásokra vonatkozó biztonsági ajánlások

11. Elvárás, hogy az intézmény a tulajdonában álló, a távmunkához biztosított asztali és hordozható számítógépek esetében a kockázatokkal arányosan biztosítsa:
    a) az eszközök központi címtárszolgáltatásaiban (pl. LDAP, Active Directory) való kezelését és hitelesítését (pl. Kerberos, RADIUS), továbbá az informatikai biztonsági felügyeleti rendszerekbe való bekötését;
    b) a távoli felhasználók helyi rendszergazda (Local Admin) jogosultságának tiltását, indokolt esetben dokumentált korlátozott használatát és fokozott ellenőrzését;
    c) azt, hogy az eszközökre csak és kizárólag az intézmény által jóváhagyott szoftver legyen telepíthető;
    d) központi megoldásokkal az eszközök firmware-einek, driver-einek, operációs rendszerének, vírusvédelmének és vírusdefiníciós adatbázisának, valamint alkalmazásainak folyamatos biztonsági frissítéseit;
    e) azt, hogy az eszközök és a központi felügyelet alá tartozó szoftverek biztonsági konfigurációjának távoli felhasználó általi módosíthatósága kerüljön tiltásra technikai eszközökkel is;
    f) azt, hogy külső hálózat közvetlen elérése csak a távoli kapcsolat kialakításának idejére legyen megengedett (pl. autentikációt igénylő szállodai vagy otthoni WiFi hálózat elérése esetén), vagy indokolt esetben a távoli hozzáféréshez elvárt technikai feltételek

teljesítéséhez szükséges kapcsolatok biztosításáig (pl. kártékonykód elleni védelmi rendszer vírusdefiníciós állományok frissítéséhez, biztonsági javítócsomag letöltéséhez);

g) lokális tűzfal alkalmazását és azt, hogy az internetre csak távoli kapcsolat felépülését követően, az intézmény határvédelmi infrastruktúráján (tűzfal, proxy, tartalomszűrő) keresztül lehessen kapcsolódni;
h) ezen eszközök beépített adattárolóinak titkosítását és a kockázatokkal arányosan további végponti adatszivárgás elleni (DLP) megoldást;
i) a külső adathordozók (például USB meghajtó, külső merevlemez, CD/DVD stb.) alapértelmezés szerinti tiltását, azok használatát csak különösen indokolt esetben külön, dokumentált jóváhagyással engedélyezze; valamint, hogy csak az általa biztosított és menedzselt, szükség szerint titkosított külső adathordozók használatát engedélyezi;
j) a lokális nyomtatók használatának külön engedélyhez kötését; és
k) az eszközök óráinak központi forrás alapján történő szinkronizálását.

VI.1.2. Okostelefonokra és tabletekre vonatkozó biztonsági ajánlások

12. Elvárás, hogy a távmunkához használt, kiadott okostelefonok, tabletek (a továbbiakban együtt: okoseszközök) használata esetén az intézmény biztosítsa:
    a) az okoseszközök bevonását a használt informatikai, informatikai biztonsági felügyeleti rendszerekbe, feltéve, hogy az okoseszköz képességei ezt kockázatarányosan lehetővé teszik;
    b) azt, hogy az okoseszközök csakis az intézmény mobileszközeinek központi felügyeletére szolgáló (Mobile Device Management, a továbbiakban: MDM) megoldással, az informatikai szabályozási rendszerben meghatározott feltételekkel és beállításokkal kerüljenek kiadásra a távoli felhasználónak;
    c) az MDM megoldásokon felül további mobil menedzsment megoldások kockázatokkal arányos alkalmazását (pl. unified endpoint management (UEM), mobile application management (MAM), Enterprise Mobility Management (EMM) stb.);
    d) az MDM megoldásokon felül – a kockázatokkal arányosan – ezen okoseszközökön is a további védelmi megoldások alkalmazását (pl. mobil kártékonykód elleni védelmi megoldás, Mobile Threat Defense (MTD) megoldások stb.);
    e) az alkalmazott MDM megoldás lehetőségeinek függvényében a külön felhasználói profil, vagy tároló (konténer) használatát annak érdekében, hogy az intézmény által védendő érzékeny adatok, valamint a távoli felhasználó személyes adatai elkülöníthetők legyenek;
    f) az okoseszközökön tárolt adatok megfelelő titkosítással, azonosítási móddal, jelszavakkal történő védelmét;
    g) az ismeretlen forrásból származó alkalmazások telepíthetőségének korlátozását, továbbá az okoseszközök feltörésének észlelését és ilyen esetben az okoseszköz csatlakozásának a tiltását és a rajta lévő adatok távoli, biztonságos törlését;
    h) a távoli felhasználók és az intézmény által számukra átadott okoseszközeik egyértelmű összerendelését az intézmény távoli hozzáférést biztosító informatikai

infrastruktúrájában, valamint azt, hogy a távoli felhasználó – a notebook-okra és munkaállomásokra vonatkozó szabályok alapján használt eszközökön kívül – csak a számára átadott, regisztrált okoseszköz(ök)ről érhesse el az intézmény hálózatát, erőforrásait;

i) azt, hogy a beszerzett okoseszközök és azok operációs rendszerei az intézmény által elvárt titkosítási követelményekkel kompatibilisek legyenek;
j) a kockázatokkal arányosan az okoseszközök operációs rendszereinek és alkalmazásainak naprakészségét, és határozza meg a minimálisan elvárt operációs rendszer verziókat;
k) azt, hogy az intézmény által meghatározott és beállított biztonsági beállításokat a távoli felhasználók nem módosíthatják;
l) az intézmény által biztosított okoseszközökön keresztül elért belső hálózati szolgáltatások (pl. elektronikus levelezés, naptár, fájlszerver elérés) a távoli felhasználók számára csak a szükséges mértékben legyenek biztosítottak;
m) azt, hogy az intézmény által biztosított okoseszközök az intézmény belső hálózatára a távmunkavégzést és a távoli hozzáférést biztosító infrastruktúrán keresztül kapcsolódjanak; valamint
n) naprakész és teljeskörű nyilvántartás vezetését a hozzáférésekről, feltüntetve a távoli felhasználó személyét és az okoseszköz típusát.

VI.1.3. Külső adathordozókra vonatkozó biztonsági ajánlások

13. Elvárás, hogy a távmunkához használt, kiadott külső adathordozók (USB meghajtó vagy azzal azonos funkciót ellátó) használata esetén az intézmény biztosítsa, hogy:
    a) ismeretlen eredetű adathordozókat nem lehet használni, a távoli felhasználók csak az intézmény által biztosított, menedzselt és nyilvántartott adathordozókat használjanak a távmunkához a 11. i) alpontjában foglaltak szerint;
    b) az adathordozó eszközöket kizárólag névre szóló – és lehetőség szerint az adott adathordozó eszközhöz rendelt – jogosultsággal használhassák a távoli felhasználók;
    c) a nem nyilvános adatok tárolása az adathordozókon csak titkosított formában történhessen;
    d) a bizalmas információk csak a feltétlenül szükséges ideig legyenek tárolva az adathordozó eszközön, a felhasználást követően haladéktalanul törölje ezeket a távoli felhasználó az adathordozó eszközökről; továbbá
    e) a bizalmas információkat tartalmazó adathordozókat alapértelmezetten tilos legyen szállítani, amennyiben a szállítást valamilyen üzleti funkció fenntartása indokolja, elvárt, hogy az intézmény biztosítsa a biztonságos szállítás feltételeit, szabályait.

VI.2. Felhasználói saját eszközök használata

14. A távoli felhasználók saját eszközei használatának engedélyezését az MNB nem javasolja,

csak különösen indokolt esetben az intézményi saját eszközökkel biztosított elérésekhez képest lényegesen csökkentett hozzáférésekkel, illetve további kontrollintézkedések alkalmazásával.

15. Elvárt, hogy ilyen esetben az intézmény törekedjen legalább az intézmény eszközeire vonatkozó biztonsági követelmények érvényesítésére, így a VI.1. pontban felsorolt elvárásokat a kockázatokkal arányos mértékben adminisztratív és technikai intézkedésekkel kényszerítse ki.

16. Amennyiben a távoli felhasználók saját eszközeinek használata különösen indokolt, további elvárás, hogy:
    a) az intézmény részletesen határozza meg, hogy milyen típusú felhasználói saját eszközök (notebook, okostelefon, tablet), milyen rendszerekkel (minimum követelmények hardver és szoftver szinten, verziók, frissítések) történő használatát engedélyezi, azok milyen erőforrásokhoz, adatokhoz férhetnek hozzá, valamint az eszközökön milyen biztonsági beállításokat kell alkalmazni;
    b) az intézmény kösse külön, dokumentált engedélyezési eljáráshoz a távoli felhasználó tulajdonában lévő saját eszközök esetében azok intézményi hálózathoz való csatlakozását;
    c) a távoli felhasználó saját eszközeinek használatát megelőzően az intézmény írásban tájékoztassa a távoli felhasználót a rá és eszközére vonatkozó biztonsági elvárásokról, az eszköz távmunkához való használatára vonatkozó szükséges technikai feltételekről, követelményekről, a vonatkozó szabályzatról, és az abban foglaltakról, valamint az intézmény azon jogáról, hogy az adatai védelmében jogában áll a távoli felhasználó saját eszközeit ellenőrizni, úgy, hogy ezek megismeréséről és elfogadásáról a távoli felhasználót írásban nyilatkoztassa;
    d) a hozzáférés megadása előtt kerüljön írásban rögzítésre és a felhasználó által aláírásra, hogy a távoli felhasználó által használt saját eszköz változásakor vagy a munkaviszonyának, szerződésének vagy megbízásának megszűnése esetén köteles az eszközét az intézmény arra kijelölt szakterülete számára ellenőrzésre bemutatni, valamint lehetővé tenni a rajta tárolt intézményi adatok, alkalmazások haladéktalan törlését;
    e) a távoli felhasználó saját eszközeinek használhatóságát az intézmény kizárólag az intézmény mobileszközeinek központi felügyeletére szolgáló megoldásának alkalmazásával engedélyezze, ezen eszközök esetében az intézmény határozza meg és technológiailag kényszerítse ki a megfelelő egyedi, kockázatokkal arányos biztonsági beállításokat, gondoskodva arról, hogy az engedélyezett felhasználói saját eszközök biztonsági beállításait kizárólag az intézmény kijelölt szakterülete módosíthassa;
    f) az MDM megoldás és az adott okoseszköz lehetőségeinek függvényében az intézmény írja elő külön felhasználói profil vagy tároló (konténer) használatát annak érdekében, hogy az intézmény által védendő érzékeny adatok, valamint a távoli felhasználó személyes adatai elkülöníthetők legyenek;

g) az intézmény a távoli felhasználó saját eszközeinek esetében is biztosítsa az intézmény által védendő érzékeny adatok, illetve az eszközök távoli törlésének („remote wipe”) lehetőségét;
h) az intézmény vezessen naprakész és teljeskörű nyilvántartást arról, hogy kinek és milyen saját felhasználói eszközök számára biztosít távoli hozzáférést;
i) az intézmény informatikai rendszere legyen képes minden távoli hozzáférés munkamenetének egyértelmű azonosítására (felhasználó, távoli eszköz);
j) az intézmény technikai megoldásokkal is gondoskodjon arról, hogy a belső hálózathoz, illetve erőforrásokhoz hozzáférést biztosító kapcsolat csak az intézmény által jóváhagyott és regisztrált eszközről legyen felépíthető;
k) az intézmény lehetőség szerint kerülje, hogy egy felhasználó egyszerre több saját eszközről is elérhesse az intézmény hálózatát és érzékeny adatait;
l) az intézmény írja elő a távoli felhasználó számára, hogy köteles az érzékeny adatokat a saját felhasználói eszközéről a lehető legrövidebb időn belül az intézmény egy olyan, a távoli felhasználó számára előzetesen biztosított szerverére, illetve tárhelyére átmásolni, amelyen az adatok automatikus mentése megoldott, és a mentést követően a lehető legrövidebb időn belül biztonságos módon törölje a saját felhasználói eszközéről azokat az érzékeny és nem nyilvános adatokat, amelyek az aktuális feladatának elvégéséhez már nem szükségesek;
m) az intézmény tiltsa a feltört operációs rendszerrel üzemelő („jailbreak”-elt, „root”-olt) eszközök távmunka keretében történő használatát;
n) az intézmény korlátozza az elavult, sérülékenyebb operációs rendszerekkel üzemelő eszközök csatlakozását;
o) az intézmény biztosítsa, hogy a távoli felhasználó az intézmény rendszerével kiépített távoli kapcsolat ideje alatt, amennyiben annak technikai feltételei adottak, ne futtasson semmilyen parancsot helyi adminisztrátori jogosultsággal;
p) az intézmény írja elő, hogy a távoli felhasználó a saját eszközén telepítsen és a legfrissebb verzióval futtasson kártékonykód elleni védelmi szoftvert;
q) az intézmény biztosítsa, hogy az intézmény rendszerével kiépített távoli kapcsolat ideje alatt, amennyiben annak technikai feltételei adottak, az internetre csak az intézmény határvédelmi infrastruktúráján (tűzfal, proxy, tartalomszűrő) keresztül lehessen kapcsolódni;
r) az intézmény biztosítsa továbbá, hogy a távoli felhasználó a saját eszközén intézményi adatot csak titkosítva és a személyes adatoktól újbóli hitelesítés kikényszerítéssel elválasztott helyen tároljon; és
s) az intézmény szabályzatban vagy a távoli felhasználóval kötött megállapodásban rendezze az adatforgalommal és díjakkal kapcsolatos kérdéseket.

VI.3.Harmadik fél tulajdonában lévő eszközök használata

17. Az MNB elvárja, hogy az intézmény harmadik fél tulajdonában lévő eszközök használatát

lehetőség szerint kerülje, azokat csak korlátozottan, külön engedélyhez kötötten biztosítsa. Ezen eszközök használatát csak akkor engedélyezze az intézmény hálózatához való csatlakozásra, ha:

a) azok legalább az intézmény eszközeire vonatkozó követelményeket teljesítik és a harmadik féllel az intézmény az együttműködés részleteit megállapodásban rögzítette, valamint a harmadik fél titoktartási nyilatkozatot tesz;
b) a harmadik fél hozzáféréseinek kezelésére az intézmény intézményen belüli felelőst, kapcsolattartót jelöl ki;
c) a harmadik fél hozzáféréseit az intézmény csak meghatározott időtartamra adja ki, azokat érvényességük lejáratakor automatikusan visszavonja;
d) a harmadik fél eszközein az intézmény hálózatára történő csatlakoztatás előtt az intézmény ellenőrzi, hogy az eszközön az intézménynél használatban lévő védelmi megoldásokkal (mint például kártékonykód elleni védelmi kliens) legalább megegyező erősségű védelem van használatban;
e) a harmadik fél védelmi szoftverei teljesítik az intézmény biztonsági elvárásait; ennek hiányában elvárt, hogy az intézmény írja elő, hogy a harmadik fél tegye meg a szükséges intézkedéseket a pótlásra, vagy álljon el a csatlakozási szándékától; a szükséges szoftverek (pl. VPN kliens, titkosítást végző szoftver, szolgáltatás, kártékonykód elleni védelmi rendszer) telepítéséhez az intézmény nyújtson támogatást, vagy megállapodás függvényében biztosítsa azok telepítését; valamint
f) szerződésben vállalja a harmadik fél, hogy az abban foglalt munka elvégzésén kívül más tevékenységet akkor sem végez, ha rendelkezik technikailag tágabb lehetőséget biztosító jogosultságokkal.

VII. A távmunka infrastruktúrájának üzemeltetése, védelme

VII.1. A távmunka helyszínének biztonsága

18. Az MNB javasolja, hogy az otthoni munkavégzés helyének biztonságossá tételéhez az intézmény adjon iránymutatást a távoli felhasználónak legalább az otthoni környezet és hálózat biztonságos kialakítása, saját eszköz esetén az operációs rendszer és a távoli kapcsolat felépítéséhez szükséges program konfigurálása és biztonsági beállításai vonatkozásában. A távmunka során a távoli felhasználó nem a védett irodai környezetet használja, ezért telefonbeszélgetéseinek, munkaanyagainak bizalmassága fokozottabb védelmet igényel. Az MNB elvárja, hogy az intézmény határozza meg a távmunka helyszínétől elvárt minimális fizikai, logikai védelmi intézkedéseket (a helyszín elhelyezkedése, nagysága, infrastruktúrája, fizikai védelme stb.). Elvárt továbbá, hogy a távoli hozzáférés engedélyezési feltétele közé kerüljön be, hogy a távoli felhasználó hozzájárul a távmunka helyszínének szükség szerinti biztonsági ellenőrzéséhez. Az MNB elvárja, hogy a távmunka helyszínére vonatkozó biztonsági irányelveket és annak ellenőrzési feltételeit rögzítsék a harmadik féllel kötött szerződésben, melynek betartatását a harmadik fél garantálja.

19. Elvárt, hogy az intézmény mérje fel és a kockázatokkal arányosan biztosítsa az üzleti munkafolyamatok biztonságos és folyamatos elvégzéséhez szükséges eszközöket és szolgáltatásokat, úgy mint:
    a) számítástechnikai eszközök (notebook, PC, okostelefon stb.);
    b) számítástechnikai kiegészítő eszközök (mikrofonos fülhallgató, webkamera, SIM kártya, token, smartcard, kártyaolvasó stb.);
    c) fizikai eltulajdonítás elleni védelmi eszközök (pl. a Kensington-zár, elzárást biztosító páncélkazetta stb.);
    d) ha indokolt, a távmunkában keletkezett papíralapú dokumentumok feldolgozásához szükséges eszközök (szkenner, iratmegsemmisítő, biztonsági boríték stb.);
    e) szükség esetén betekintésvédelmi monitorszűrő vagy fólia; és
    f) szükség esetén adatkapcsolati előfizetés (pl. internet előfizetés, menedzselt mobil internet).

20. Az MNB elvárja, hogy az intézmény készítsen informatikai biztonsági oktatási anyagot a távmunka használatának feltételeiről, kockázatairól, melynek keretén belül az intézmény hívja fel a távoli felhasználó figyelmét legalább az alábbiakra:
    a) a távoli hozzáféréshez használt eszközöket a távoli felhasználó ne hagyja őrizetlenül, rövidebb távollét esetén is zárja le a képernyőt vagy kapcsolja be a jelszóval ellátott képernyővédőt;
    b) a távmunkában használt intézményi eszközöket csak az arra illetékesek használják (családtagok sem);
    c) a hitelesítéshez használt eszközeit (pl. token, smartcard) a távoli felhasználó tartsa biztonságos helyen, használaton kívül ne hagyja a géphez csatlakoztatva és ne ossza meg senkivel, ne adja át senkinek;
    d) a távmunka során a távoli felhasználó saját otthoni WiFi hálózatának biztonságosabbá tételére (WiFi router alapértelmezett adminisztrátori jelszavának megváltoztatása és a tűzfal biztonságos beállítása, WiFi hálózathoz való csatlakozás csak jelszóval történhessen megfelelő titkosítás mellett, WEP és WPS tiltás stb.);
    e) a távoli felhasználó gondoskodjon a távmunkához használt eszközök biztonságos tárolásáról a munkavégzés megszakítása vagy befejezése esetén, az eszközök ne maradjanak hosszabb ideig „alvó” vagy „hibernált” állapotban;
    f) az eszközöket ne hagyja őrizetlenül, különösen autóban, autó csomagtartójában, hotelszobában, gondoskodjon az eszközök elzárt tárolásáról;
    g) utazás esetén kézipoggyászként kerüljenek szállításra az eszközök és különös figyelmet fordítson a védelmükre;
    h) biztosítani kell az adatokat tartalmazó adathordozók – biztonsági osztálynak megfelelő – biztonságos tárolását (pl. páncélkazetta stb.), illetve az adatokhoz való illetéktelen hozzáférés megakadályozását, illetve észlelését (pl. bontás észlelésre alkalmas borítékban tárolás stb.);

i) az intézmény hálózatához és az alkalmazásaihoz szükséges jelszavakat a távoli felhasználó ne használja a magánügyek intézésénél;
j) az eszközök nyilvános helyen való használatát lehetőség szerint kerülje, ne engedje, hogy illetéktelen személy a képernyőjére betekintést nyerjen; valamint
k) bármilyen informatikai biztonsági incidenst, valamint a távmunkához használt eszköz kompromittálódását, elvesztését, ellopását haladéktalanul jelentse az intézménynek.

VII.2. Hálózatvédelem

21. Az MNB elvárja, hogy az intézmény a távmunka használatánál:
a) biztosítsa és ellenőrizze, hogy csak az informatikai biztonsági előírásoknak megfelelő, naprakész biztonsági frissítésekkel és védelmi eszközökkel (pl. kártékonykód elleni védelem) rendelkező, ellenőrzött és engedélyezett eszközök csatlakozhassanak az intézmény hálózatához;
b) biztosítsa és ellenőrizze, hogy az intézmény által menedzselt okoseszközök csak mobileszközeinek védelmére szolgáló megoldásában meghatározott biztonsági beállítások teljesülése esetén csatlakozhassanak az intézmény infrastruktúrájához;
c) a távoli hozzáférés során a csatlakozó eszköz hálózati forgalmát minden esetben ellenőrizze az intézmény határvédelmi megoldásai által (tűzfal, IDS/IPS, webgateway, adatszivárgás elleni védelmi rendszer stb.);
d) fordítson kiemelt figyelmet a távmunka alkalmazása során az adatszivárgás megelőzésére;
e) a távoli hozzáférés kialakítása során törekedjen az újabb és nagyobb biztonságot adó megoldások alkalmazására, a kockázatokkal arányos erős és biztonságos protokollokkal és algoritmusokkal;
f) a kevésbé biztonságosnak tartott távoli hozzáférést biztosító technológiákat, mint pl. a távoli asztal, fájlmegosztás (azok titkosított hitelesítése és adatátvitele ellenére is) kerülje, ezen kapcsolatokat csak különösen indokolt esetben, további hálózati titkosítással használja;
g) a távoli hozzáféréseket az intézmény belső, védett hálózataitól tűzfallal elválasztott szegmensén végződtesse, technikai megoldással gondoskodjon arról, hogy a távoli hozzáférést végződtető eszköz (pl. VPN koncentrátor) kompromittálódása esetén a támadó ne férhessen hozzá a belső, védett hálózatokhoz;
h) biztosítsa az adatszivárgás szempontjából kockázatos oldalak és szolgáltatások, mint például, de nem kizárólag a közösségi média, a publikus felhő alapú adattárolók, fájlmegosztók és webmail szolgáltatások elérésének tiltását, különösen indokolt esetben a kockázatokkal arányos korlátozását, illetve azok munkahelyi célokra való felhasználásának (intézményi adatok, képek, információk elhelyezésére, megosztására) külön engedélyhez kötését;
i) a bizalmas anyagok publikus e-mail szolgáltatáson való továbbítását tiltsa meg, indokolt esetben szigorúan szabályozza, korlátozza; továbbá

j) biztosítsa az adó-, üzleti, bank-, értékpapír-, pénztár-, fizetési, biztosítási vagy foglalkoztatói nyugdíjtitkot, illetve személyes adatot tartalmazó e-mailek bizalmasságát és sértetlenségét.

VII.3. A távmunka alatti informatikai szolgáltatások és napi üzemeltetések

22. Az MNB elvárja, hogy az intézmény távmunka során is tartsa fent azon szükséges és elégséges informatikai szolgáltatásokat, amik biztosítják az informatikai eszközök és rendszerek folyamatos működését. Ennek keretén belül MNB az intézménytől elvárja, hogy:
    a) alkalmazzon megfelelő számú és képzettségű szakembert a felhasználói támogatást ellátó (helpdesk) területen;
    b) biztosítsa a távoli felhasználók bejelentéseinek biztonságos eljutását a felhasználói támogatást ellátó területhez;
    c) a távmunka és rendkívüli események (pl. pandémiás helyzet) idején is biztosítsa a felhasználói támogatást ellátó terület elérhetőségét és megfelelő működését;
    d) mérje fel és határozza meg a telephelyhez kötött munkaköröket, munkafolyamatokat;
    e) biztosítson a telephelyhez kötött munkakörök és munkafolyamatok ellátásához megfelelő számú és képzettségű személyzetet, valamint biztonságos munkahelyi környezetet;
    f) mindenkor gondoskodjon a szükséges napi üzemeltetési tevékenységek elvégzéséről (mentések, napló- és monitorbejegyzések vizsgálata, riportolás stb.); és
    g) biztosítsa az informatikai biztonsági incidensek észlelését, kivizsgálását és a szükséges intézkedések végrehajtását.

VII.4. Fax, telefon-, konferencia-, videókonferencia-hívások és egyéb kommunikációs csatornák biztonsága

23. A távmunka során a telephelyen munkát végző és a távoli felhasználók egymással és harmadik féllel telefonon, illetve tele- és videókonferencia igénybevételével tarthatnak kapcsolatot. Ezeken és más (fax, online chat, egyéb) kommunikációs csatornákon bizalmas adatok és információk is közlekedhetnek, melyeknek bizalmasságát, sértetlenségét és hitelességét mindenkor biztosítani kell.

24. A kockázatok csökkentése és az adatok védelme érdekében az MNB elvárja, hogy az intézmény az adott kommunikációs megoldástól függően technikai és adminisztratív kontrollokkal biztosítsa:
    a) minden online konferencia/kollaborációs szolgáltatásnál (video, audio, chat, egyéb) az adatkapcsolatok titkosítását, a hitelesítő adatok titkosított továbbítását;
    b) a szabványos titkosítási algoritmusok és eljárások használatát;
    c) a titkosítás megszüntetés lehetőségének a kizárását (még az adminisztrátornak is);
    d) a nem publikus információk telefonon, faxon, videókonferencián, online chat és egyéb hasonló megoldáson való kezelésének technikai vagy adminisztratív kontrolokkal való korlátozását;

e) azt, hogy a meghívottak köre rendelkezik a hívások alatt elhangzó információk megismeréséhez szükséges jogosultsággal;
f) a bizalmas adatokat megosztó beszélgetések nyilvános helyen, illetéktelenek által is használt helyiségekben történő tiltását;
g) azt, hogy csak a megbeszélés szervezője által meghívott személyek tudjanak csatlakozni a hívásokhoz;
h) a bejelentkezésnél a hitelesítés kikényszerítését;
i) a bejelentkezésnél lehetőség szerint a „várószoba" használatát;
j) a licencet a szükséges számú résztvevőnek;
k) azt, hogy a hívás hang- és videóanyagairól felvétel csak indokolt és előre jóváhagyott esetben legyen készíthető, amiről minden résztvevő előzetes tájékoztatást kap; a beszélgetés vagy konferencia rögzítése kizárólag az erre a célra kijelölt vonalakon, erre a célra kijelölt eszközökkel történjen;
l) a hang- és videóanyagokról készült felvételek biztonságos és jogszabályok szerinti tárolását és használatát, valamint a cél megszűnésekor az azonnali törlését;
m) a megbeszélés szervezője általi felügyeletet a képernyőmegosztáshoz, a hívások közbeni fájlmegosztáshoz és fájltovábbításhoz;
n) a kockázatokkal arányos mértékben a konferencia-szolgáltatás feletti további titkosított csatorna kiépítését (ez hang- és adatátviteli vonalon nagyobb terhelést eredményezhet);
o) azt, hogy a bizalmas, védendő adatok faxon való küldése vagy fogadása alapértelmezetten tiltott legyen, különösen indokolt esetben a megfelelő kontrollok biztosítása mellett, csak a fogadó fél előzetes értesítése és jóváhagyása esetén történhessen;
p) azt, hogy az élőszóban és telekommunikációs eszközökön történő információközlés során a halló-, illetve látótávolságon belül tartózkodó illetéktelen személyeknek nem kerül birtokába bizalmas információ; valamint
q) a konferenciabeszélgetések bizalmasságának megőrzését a távoli felhasználók részére szükség szerint rendelkezésre bocsátott megfelelő mikrofonos fejhallgatóval.

VII.5. Rögzített vonalas hívások kezelése

25. A telefonhívások rögzítésével kapcsolatban az MNB az Európai Értékpapír-piaci Hatóság (ESMA) vonatkozó közleményével[4] összhangban elvárja az intézménytől, hogy:
    a) távmunka során az ügyfélmegbízásokat érintő telefonbeszélgetések vagy elektronikus (hang, levél, chat, videó) kommunikáció rögzítése és tárolása során is fordítson kiemelt figyelmet a vonatkozó jogszabályok betartására;
    b) amennyiben az elektronikus adatrögzítés bármilyen okból kifolyólag akadályba ütközik, gondoskodjon az adatrögzítés alternatív módon való megvalósításáról, melynek tényéről és módjáról az ügyfelet a telefonbeszélgetés megkezdése előtt tájékoztatni köteles[5];

[4] ESMA Statement on COVID-19 telephone recording (a továbbiakban: ESMA35-43-2348)
[5] ESMA35-43-2348 6. pontja

c) biztosítsa az alternatív adatrögzítési módon (papíralapú vagy elektronikus feljegyzés, diktafon, az ügyintéző mobiltelefonja, személyes telefonos hangrögzítő, egyéb) rögzített megbízások és ezen megbízások teljesítésének fokozott monitorozását és utólagos ellenőrzését[6];
d) kimenő hívás esetén ne hagyjon bizalmas adatokat tartalmazó üzenetet a hívott fél üzenetrögzítőjén; és
e) kövessen el minden tőle telhetőt, hogy az alternatív adatrögzítési módról a lehető leghamarabb térjen vissza az eredeti állapothoz[7].

VII.6. A távoli hozzáférés során használt felhasználói azonosítás és hitelesítés

26. Az MNB a távoli hozzáférés során az intézmény részéről elvárja:
    a) a távoli felhasználó hitelesítésére a többfaktoros hitelesítés használatát;
    b) a szabványos, erős kriptográfiai algoritmusok használatát a titkosításhoz és hitelesítéshez;
    c) a távoli felhasználók, eszközeik és a kapcsolatok egyedi azonosítását;
    d) az ugyanazon távoli felhasználó részére egyidejűleg engedélyezett távoli kapcsolatok maximális számának megállapítását;
    e) a végfelhasználói hozzáférés szabályozottságát és dokumentáltságát;
    f) azt, hogy a távmunkához használt jelszavak erőssége és összetettsége érje el vagy haladja meg az intézmény belső hálózatához való hozzáférésre vonatkozó követelményeket;
    g) azt, hogy úgy alakítsa ki a hitelesítéshez használt második faktor kiadásának, megújításának és visszavonásának biztonságos folyamatát, hogy az akár távolról biztosítható legyen;
    h) egy felépített kapcsolat intézmény általi azonnali megszakításának lehetőségét; továbbá
    i) a kockázatokkal arányos mértékben a megbízhatóbb hitelesítés érdekében a távoli eszközök hitelesítését is.

VII.7. Adatokhoz való hozzáférés

27. Az intézmény adataihoz való hozzáférésnél a távmunkában is a szükséges és elégséges feltételeket kell biztosítani a távmunkában dolgozóknak a legkisebb jogosultság elvét szem előtt tartva. Ennek érdekében az MNB elvárja:
    a) a megfelelő távoli hozzáférési csoportok és a hozzájuk tartozó jogosultságok kialakítását az intézményi adatokhoz való hozzáférés személyre szabásához a „legkisebb jogosultság” elvét követve;
    b) az élesüzemi, a teszt-, az oktatói, illetve a fejlesztői hozzáférések szétválasztását;
    c) a kiemelt felhasználói (pl. adminisztrátori és rendszergazdai) hozzáférések szerepkörök szerinti szétválasztását, egyedi szabályozását;

[6] ESMA35-43-2348 6. pontja
[7] ESMA35-43-2348 7. pontja

d) a távmunka során történő nyomtatás alapértelmezett tiltását, indokolt esetben megfelelő szabályozását;
e) a távmunka során az intézményi adatok lokális gépre történő letöltésének szabályozását; és
f) azt, hogy az intézmény biztosítsa a lokális eszközökön keletkezett intézményi adatok eszközön kívüli mentését.

VIII. Távoli hozzáférés ellenőrzése

28. A távmunka során a megnövekedett számú és forgalmú távoli hozzáféréshez szükséges hálózati kapcsolatokat és az azokon átfolyó adatforgalmat a kockázatokkal arányosan szükséges kezelni. Ennek érdekében az MNB elvárja az intézménytől, hogy:
    a) folyamatosan monitorozza a távoli hozzáféréssel felépített hálózatikapcsolatokat és a rajtuk átfolyó adatfolyamot, és folyamatosan biztosítsa a távoli hozzáféréshez szükséges kapacitásokat;
    b) határozza meg a távoli hozzáférést, távmunkát biztosító informatikai infrastruktúra naplózási követelményeit, és biztosítsa azok érvényesítését;
    c) biztosítsa a távoli hozzáférést, távmunkát biztosító informatikai infrastruktúra biztonsági naplóinak a központi naplógyűjtő és -elemző rendszerbe való bekötését, a naplóállományok rendszeres elemzését, a riasztási szintek beállítását, a riasztások elküldését és a belőlük fakadó intézkedések nyomonkövetését. A kockázatokkal arányosan biztosítsa a távoli hozzáférések során keletkező naplóesemények közötti összefüggések keresését a különböző forrásokból származó biztonsági naplókban, hogy ezáltal lehetővé tegye az anomáliák és a kapcsolódó incidensek meghatározását;
    d) fordítson kiemelt figyelmet a távmunka során a kiemelt jogosultsággal végzett tevékenységek naplózására, riasztások beállítására, ezen naplóállományok védelmére, valamint ezen tevékenységek rendszeres ellenőrzésére;
    e) dolgozzon ki intézkedési tervet az elvárható működési paraméterektől való eltérés (megnövekedett távoli hozzáférés, megnövekedett forgalom stb.) kezelésére és ellenőrzésére; továbbá
    f) rendszeresen ellenőrizze, hogy a távoli hozzáférést, távmunkát biztosító informatikai infrastruktúra és a végponti eszközök megfelelnek-e a vonatkozó információbiztonsági és informatikai szabályzatainak, elvárásainak és gondoskodjon a rendszeres sebezhetőségi vizsgálatok elvégzéséről. A technikai megfelelőség ellenőrzései során a kockázatokkal arányos mértékben használjon automatizált eszközöket is.

IX. Záró rendelkezések

29. Az ajánlás Magyar Nemzeti Bankról szóló 2013. évi CXXXIX. törvény 13. § (2) bekezdés i) pontja szerint kiadott, a felügyelt pénzügyi szervezetekre kötelező erővel nem rendelkező szabályozó eszköz. Az MNB által kiadott ajánlás tartalma kifejezi a jogszabályok által

támasztott követelményeket, az MNB jogalkalmazási gyakorlata alapján alkalmazni javasolt elveket, illetve módszereket, a piaci szabványokat és szokványokat.

30. Az ajánlásnak való megfelelést az MNB az általa felügyelt pénzügyi szervezetek körében az ellenőrzési és monitoring tevékenysége során figyelemmel kíséri és értékeli, összhangban az általános európai felügyeleti gyakorlattal.

31. Az MNB felhívja a figyelmet arra, hogy a pénzügyi szervezet az ajánlás tartalmát szabályzatai részévé teheti. Ebben az esetben a pénzügyi szervezet jogosult feltüntetni, hogy vonatkozó szabályzatában foglaltak megfelelnek az MNB által kiadott vonatkozó számú ajánlásának. Amennyiben a pénzügyi szervezet csupán az ajánlás egyes részeit kívánja szabályzataiban megjeleníteni, úgy az ajánlásra való hivatkozást kerülje, illetve csak az ajánlásból átemelt részek tekintetében alkalmazza.

32. Az MNB a jelen ajánlás alkalmazását 2021. január 1-jétől várja el az érintett pénzügyi szervezetektől, azzal, hogy az MNB jó gyakorlatnak tartja, ha az újonnan kialakítandó vagy az ajánlás megjelenésekor módosítás alatt álló fejlesztéseknél a pénzügyi szervezetek már ezt megelőzően is figyelembe veszik a jelen ajánlásban foglalt elvárásokat.

Dr. Matolcsy György sk.
a Magyar Nemzeti Bank elnöke