A Magyar Nemzeti Bank 4/2019. (IV.1.) számú ajánlása

a közösségi és publikus felhőszolgáltatások igénybevételéről

I. Az ajánlás célja és hatálya

Jelen ajánlás célja, hogy a pénzügyi közvetítőrendszer szereplői számára gyakorlati útmutatást adjon a közösségi és publikus felhőszolgáltatások igénybevételéből eredő kockázatok kezeléséhez, valamint a vonatkozó nemzeti és európai uniós jogszabályokban, egyéb szabályozó eszközökben foglalt rendelkezések[1] egységes alkalmazásához. Ennek érdekében az ajánlás – a felhőszolgáltatás életciklusát és az alapelveket követve – meghatározza a szerződések elvárt minimumkövetelményeit, ismerteti a kezelendő kockázatokat, az elvárt kontrollintézkedéseket és a pénzügyi közvetítőrendszer felügyeletével kapcsolatos feladatkörében eljáró Magyar Nemzeti Bank (a továbbiakban: MNB) jelen ajánlás tárgykörét érintő ellenőrzéseinek fő szempontjait.

Az MNB az Európai Bankhatóság (a továbbiakban: EBA) 2017. december 20-i, a felhőszolgáltatóknak történő kiszervezésről szóló ajánlásait (EBA/REC/2017/03) alapul véve, az abban szereplő előremutató követelményeket és gyakorlatokat értékelve, a jelen ajánlásban határozza meg a felhőszolgáltatások igénybevételével összefüggő, a pénzügyi közvetítőrendszer valamennyi szereplőjére vonatkozó elvárásait.

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

Jelen ajánlás nem utal vissza teljeskörűen a jogszabályi rendelkezésekre az elvek és elvárások megfogalmazásakor, azonban az ajánlás címzettjei továbbra is kötelesek megfelelni a kapcsolódó jogszabályi előírásoknak. Az ajánlás az ágazati és egyéb vonatkozó további jogszabályokban és ajánlásokban foglaltakon felül értelmezendő. Az ajánlás az informatikai rendszer védelméről szóló 7/2017. (VII. 5.) MNB ajánlással, valamint az interneten keresztül nyújtott pénzügyi szolgáltatások biztonságáról szóló 15/2015. MNB ajánlással együtt alkalmazandó.

II. A felhőszolgáltatások meghatározása

1. A számítástechnikai felhőszolgáltatás lehetővé teszi az igény szerinti hálózati hozzáférést megosztott, konfigurálható számítástechnikai erőforrásokhoz (például hálózatokhoz, szerverekhez, tárolókhoz, alkalmazásokhoz és szolgáltatásokhoz), melyeket gyorsan lehet allokálni és használatukat lezárni, minimális menedzsment ráfordítással vagy szolgáltatói közreműködéssel[2]. A felhőszolgáltatás öt lényegi ismérve a következő:

   a) a szolgáltatás igény szerinti, akár önkiszolgáló módon való igénybevétele;

   b) általános hálózati elérés (interneten vagy magánhálózaton keresztül);

   c) megosztottan használt erőforrások; a szolgáltató erőforrásaival több ügyfelet szolgál ki („multi-tenant” modellben), a különböző fizikai és virtuális erőforrásokat dinamikusan allokálja a felhasználói igények függvényében; az ügyfelek jellemzően nem ismerik, és nem

[1] Lásd a mellékletben szereplő felsorolást.

[2] A felhőszolgáltatás ajánlásbeli definíciójának alapját az Amerikai Nemzeti Szabványügyi és Technológiai Intézet (National Institute of Standards and Technology, a továbbiakban: NIST) következő dokumentuma képezi: The NIST Definition of Cloud Computing (SP 800-145) http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

befolyásolhatják az igénybe vett erőforrások pontos helyét, de adott esetben lehetőségük van a hely magasabb absztrakciós szinten való meghatározására (például ország, régió, vagy adatközpont szinten);

d) a változó kapacitás-igények gyors lekövetése;

e) mért szolgáltatás (felhasználással arányos használati díj).

2. A felhőszolgáltatások négy alapvető elérési modelljéből jelen ajánlás a publikus felhő és a közösségi felhő modelljét, illetve hibrid felhő esetén a hibrid felhő publikus vagy közösségi elérési vonatkozását tárgyalja. Publikus felhő alatt a bárki számára elérhető, míg közösségi felhő alatt valamilyen szervező elv mentén több, akár független szereplő (például egy ellátási lánc résztvevői, egy cégcsoporthoz tartozó intézmények vagy kormányzati szervek) számára megosztott módon elérhető felhőszolgáltatást kell érteni. A hibrid felhőszolgáltatás legalább kettő különböző elérési modellű felhőinfrastruktúra használatával jár, melyek között az adatok és a szolgáltatások igény szerinti áramlása biztosított.

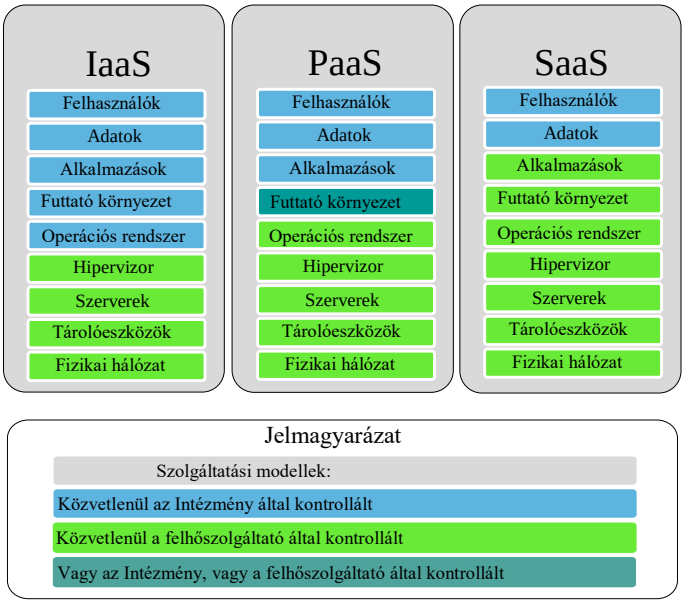
3. A felhő három fő szolgáltatási modellben érhető el:

a) infrastruktúraszolgáltatás (Infrastructure as a Service, IaaS): a szolgáltató virtuális hardvert ad, amelyre minden szoftvert a felhasználó telepít és üzemeltet;

b) platformszolgáltatás (Platform as a Service, PaaS): a szolgáltató virtuális hardver erőforrást és alapszoftvert (jellemzően operációs rendszert, adatbázis-kezelő rendszert, webszervert, alkalmazásszervert) ad, amelyre a felhasználó a saját üzleti alkalmazásait telepíti és üzemelteti;

c) szoftverszolgáltatás (Software as a Service, SaaS): a szolgáltató felhő alapú infrastruktúrában üzemelő virtuális hardveren és az alapszoftvereken ad üzleti megoldást, melyet a felhasználó konfigurál, és részben üzemeltet (például felhasználói jogosultságkezelés).

4. A szolgáltatásban érintett elemek feletti kontrollt gyakorlókat a szolgáltatási modell függvényében az alábbi ábra szemlélteti:



1. ábra: Szolgáltatási modellek és az elemek feletti kontroll közvetlen gyakorlói

III. A felhőszolgáltatások igénybevételének életciklusa

5. Az Intézmény felelőssége azonosítani a kockázatokat és megfelelőségi követelményeket a felhőszolgáltatás életciklusának minden fázisában, és megvalósítani az arányos védelmi intézkedéseket, legalább a következőkben leírt szempontok figyelembevételével.

III.1. Üzleti igény felmerülése, döntés-előkészítés, tervezés

6. Az informatikával kapcsolatos üzleti igények, tulajdonosi elvárások (például költségcsökkentés, rugalmasság, hullámzó kapacitásigény, beruházási költségérzékenység, gyors bevezetés) kielégítése érdekében a felhőszolgáltatás is felmerülhet lehetséges megoldásként. Ebben az esetben az Intézmény megvizsgálja a felhőszolgáltatás létjogosultságát az üzleti igények, a felhőszolgáltatás képességei, költségei és kockázatai, a biztonsági követelmények és a jogszabályi előírások alapján. Az MNB javasolja, hogy a döntés-előkészítés és a tervezés során az Intézmény az alábbiak szerint járjon el.

III.1.1. Jogszabályi megfelelés biztosítása

7. A felhőszolgáltatás igénybevételét megelőzően az Intézmény meggyőződik arról, hogy a felhőszolgáltatás használata során biztosítani tudja a jogszabályoknak való teljes körű megfelelést. A felhőszolgáltatás igénybevétele során a jogszabály szerinti működés teljes felelőssége megmarad az Intézménynél, így az Intézmény már az igénybevételt megelőzően megvizsgálja, hogy a kötelezettségeit miként tudja teljesíteni, illetve az adott felhőszolgáltató miként biztosítja számára a szükséges kontrollokat és monitorozási lehetőséget.

8. Jelen ajánlás alkalmazása során különös figyelmet kell fordítani az ügyfél közvetlen vagy közvetett azonosítására vagy profilalkotásra alkalmas adatok (a továbbiakban: ügyféladat), illetve az adó-, üzleti, bank-, értékpapír-, pénztár-, fizetési, biztosítási vagy foglalkoztatói nyugdíjtitok (a továbbiakban együtt: pénzügyi ágazati titok) körébe tartozó adatokra. A felhőszolgáltatás során megvalósuló adatkezelés, adatfeldolgozás vagy adattárolás vonatkozásában az Intézmény megfelelő garanciális szabályokat határoz meg a vonatkozó hazai jogszabályokkal és uniós jogi aktusokkal összhangban. Ezek a garanciális szabályok biztosítják többek között, hogy az adat kezelője vagy feldolgozója minden ügyféladatot és pénzügyi ágazati titkot csak a célhoz kötöttség elvének megfelelően, az adatkezelés céljának megvalósulásához elengedhetetlen mértékben és ideig kezeljen, dolgozzon fel és tároljon.

9. Amennyiben a felhőszolgáltatás során személyes adatok kezelése, feldolgozása vagy tárolása is történik, akkor az Intézmény biztosítja az adatkezelésre és adatvédelemre vonatkozó nemzetközi és hazai jogszabályi környezetnek való megfelelést.[3]

10. Az Intézmény felméri, hogy a felhőszolgáltatás igénybevétele a hatályos pénzügyi ágazati jogszabályok[4] szerint kiszervezésnek minősül-e. A felmérés eredménye alapján az Intézmény dokumentált döntést hoz arról, hogy – a jogszabályi előírásokkal összhangban – kiszervezésként kezeli-e a szolgáltatást. Amennyiben a jelen ajánlás valamely rendelkezése a „kiszervezés" kifejezést használja, akkor az adott rendelkezés a felhőszolgáltatás igénybevételének azokra az eseteire vonatkozik, amelyek a vonatkozó ágazati jogszabályok alapján kiszervezésnek minősülnek.

[3] Lásd a melléklet 2. pontjában felsorolt jogszabályokat, uniós jogi aktusokat
[4] Lásd a melléklet 1. pontjában felsorolt jogszabályokat.

11. Amennyiben az Intézmény, illetve az általa használt rendszer a pénzügyi ágazathoz tartozó európai vagy nemzeti létfontosságú rendszerelemként került kijelölésre, akkor az Intézmény figyelembe veszi az erre vonatkozó jogszabályi előírásokat is.[5]

III.1.2. Előny-hátrány elemzés

12. Az Intézmény felhőszolgáltatás igénybevételéről szóló döntése megalapozásához előny-hátrány elemzést végez, amely kitér legalább a következőkre:

    a) az üzleti igény megvalósítására alkalmas más (nem felhő alapú) megoldások elemzése, melynek része a szolgáltatás igénybevételéből fakadó kockázatok értékelése potenciális kárnagyságok és becsült kontrollköltségek alkalmazásával (például szolgáltatási szint megállapodások, ellenőrzések, tanúsítások, addicionális biztonsági szolgáltatások költségei);

    b) a felhőszolgáltatásra való áttérés kockázatai és költségei (például alkalmazás- és adatmigráció);

    c) a felhőből való kivezetés (visszavétel) és adatvisszatöltés lehetőségei és becsült költségei.

III.1.3. Lényeges tevékenységek értékelése

13. Az MNB a lényeges tevékenységek értékelése terén jó gyakorlatként javasolja figyelembe venni a következőket: a lényeges tevékenységek fogalmát az Európai Bankfelügyeleti Bizottság kiszervezésről szóló, 2006. december 14-i iránymutatásain belül az 1. iránymutatás f) pontja határozza meg, míg a lényeges tevékenyégek értékelésének követelményével a 4. iránymutatás foglalkozik. Az értékelés szempontjait részletesebben az EBA felhőszolgáltatások igénybevételével való kiszervezésre vonatkozó ajánlásai (EBA/REC/2017/03) 4. fejezetének 1. pontja határozza meg.

14. Az Intézmény a felhőszolgáltatás igénybevételével összefüggésben legalább az alábbi tevékenységeit lényegesnek (materiálisnak) minősíti:

    a) az olyan jelentőségű tevékenységek, amelyek hiányossága, kiesése megakadályozza vagy jelentősen veszélyezteti az Intézmény szabályszerű működését vagy üzletmenetét, szolgáltatásainak nyújtását;

    b) a felügyeleti engedélyhez kötött tevékenységek;

    c) a kockázatkezelési funkciót jelentősen befolyásoló tevékenységek;

    d) a fenti tevékenységek kockázatainak kezeléséhez tartozó tevékenységek.

15. Az Intézmény a felhőszolgáltatás igénybevételével érintett tevékenységek lényegességét a következő szempontok alapján értékeli:

    a) a tevékenység kritikussága és kockázatossága az Intézmény életképessége, üzletmenetének folytonossága és ügyfelei felé vállalt kötelezettségeinek teljesítése vonatkozásában;

    b) a tevékenység kiesésének működési, jogi, reputációs és pénzügyi kockázatai;

    c) a tevékenység által érintett adatok sértetlenségét, bizalmasságát és rendelkezésre állását befolyásoló incidensek lehetséges hatása.

[5] Lásd a melléklet 4. pontjában felsorolt jogszabályokat.

III.1.4. A felhőszolgáltatás igénybevételével érintett tevékenységek nyilvántartása

16. Az Intézmény naprakész nyilvántartást vezet az Intézmény, valamint az Intézmény vállalatcsoportja által igénybe vett felhőszolgáltatással érintett valamennyi olyan tevékenységről – azok lényegességétől függetlenül – amelyek érintik az Intézmény adatait, különös tekintettel az ügyféladatokra. Az MNB a nyilvántartandó információk vonatkozásában jó gyakorlatként javasolja figyelembe venni az EBA felhőszolgáltatások igénybevételével való kiszervezésre vonatkozó ajánlásai (EBA/REC/2017/03) 4. fejezetének 5. pontját, mely a jelen ajánlás 29. a)-g) pontjában foglalt, az MNB részére benyújtandó tájékoztatásban szereplő információkon felül is javasol nyilvántartandó adatokat.

III.2. A felhőszolgáltatás kockázatelemzése

17. Az MNB javasolja, hogy az Intézmény informatikai kockázatelemzése – amelynek fogalmába beleértendő a kockázatok felmérése (azonosításuk és értékelésük a szolgáltatási modell függvényében), valamint a kockázatcsökkentő intézkedések megtervezése – terjedjen ki a jelen és a 37-59. pontban felsorolt követelmények megvalósításának lehetőségeire és a szolgáltatás életciklusának valamennyi fázisára. Az MNB jó gyakorlatnak tartja, hogy a követelmények teljesítésére – a szolgáltatási modell függvényében és az érintett szolgáltatások lényegessége alapján (bizalmasság, sértetlenség, rendelkezésre állás) – az Intézmény a kockázatokkal arányosan vagy saját hatáskörben működtessen informatikai kontrollokat, vagy szerződésben rögzítse azok szolgáltató általi működtetését, és ezek működéséről szerezzen bizonyosságot. Az MNB javasolja, hogy az Intézmény a kockázatelemzés elvégzése során az alábbiak szerint járjon el.

18. Az Intézmény vezetése gondoskodik a kockázatcsökkentő intézkedési tervek[6] kidolgozásáról, az intézkedések végrehajtásához szükséges feltételek biztosításáról, és a megtett intézkedések ellenőrzéséről. Az Intézménynek kockázatcsökkentő intézkedésekkel (kontrollokkal) szükséges kezelnie a jogszabályi meg nem felelést okozó kockázatokat, azaz nem háríthatja át és nem fogadhatja el az ilyen típusú kockázatokat.

III.2.1. Az adatok és az adatkezelés helye[7]

19. Az Intézmény értékeli a felhőszolgáltatás igénybevételével érintett adatok, adatkörök, továbbá az adatkezelés, adatfeldolgozás, adattárolás helyszínével kapcsolatos jogi, politikai, gazdasági, biztonsági és felügyeleti kockázatokat, továbbá csak olyan szintű kockázatot vállal, amely nem okoz jogszabályi meg nem felelést, valamint összhangban áll a felhőszolgáltatás igénybevételével érintett tevékenység lényegességével, az érintett adatok bizalmasságával, sértetlenségével, rendelkezésre állásával kapcsolatos követelményeknek, elvárásoknak. Az Intézmény az Európai Gazdasági Térségen kívüli felhőszolgáltatás esetén az adatvédelmi kockázatok, valamint a felügyeleti tevékenységek gyakorlását veszélyeztető geopolitikai kockázatok miatt különös gondossággal jár el[8]. Ilyen esetben az Intézmény dokumentáltan igazolja, hogy a felhőszolgáltatás igénybevétele során figyelembe vette a harmadik országban történő adatkezelésre vonatkozó előírásokat.

[6] Az intézkedési tervekkel kapcsolatos követelményeket a 7/2017. (VII. 5.) MNB ajánlás tartalmazza.

[7] A vonatkozó jogszabályi követelményeket részletesen a melléklet 2. pontjában felsorolt jogszabályok tartalmazzák.

[8] A határon átnyúló felhőszolgáltatások esetében a szolgáltató földrajzi helyzetével összefüggő kockázatok – köztük az adatvédelmi kockázatok – kezelésével az Európai Bankfelügyeleti Bizottság kiszervezésről szóló, 2006. december 14-i iránymutatásain belül a 4. iránymutatás (illetve annak 4. pontja) foglalkozik; a kapcsolódó szempontokat az EBA felhőszolgáltatások igénybevételével való kiszervezésre vonatkozó ajánlásainak (EBA/REC/2017/03) 4.6. pontja tartalmazza.

III.2.2. A kivezetés kockázatai

20. Az Intézmény felméri és kezeli a felhőszolgáltatás kivezetésének (felhőszolgáltatásból való kilépés) kockázatait, beleértve a váratlan kényszerű kivezetést is, például a szolgáltató vagy a szolgáltatás megszűnésének esetét. Kockázatcsökkentő intézkedésként szolgáltatáskivezetési (exit) stratégiát és akciótervet dolgoz ki.

21. Az Intézmény a kivezetési stratégia részeként:

    a) olyan szerződési feltételeket köt ki, amelyek nehézség nélkül lehetővé teszik a felhőből való kilépést (lásd a 35. pontot), különös figyelemmel a tárolt adatok rendelkezésre bocsátására a felhőszolgáltatástól függetlenül értelmezhető és felhasználható formában (hordozhatóság);
    b) biztosítja – és a kockázatok mértékének megfelelő gyakorisággal és módszerrel ellenőrzi – a felhőszolgáltatás megszűnése esetén az erre támaszkodó üzleti folyamatok működtethetőségét.

III.2.3. Bizonyosságszerzés

22. Az Intézmény dokumentálja, hogy milyen szintű bizonyosság megszerzését tartja szükségesnek a felhőszolgáltató kockázatcsökkentő intézkedéseinek megvalósulásáról, a nyújtott szolgáltatás kontrollkörnyezetére vonatkozóan.

23. A bizonyosságszerzés lehetséges módjai és az általuk nyújtott bizonyosság szintjei a következők:

    a) a szolgáltató által adott nyilatkozat, szerződéses vállalás, felelősségbiztosítás (közepes szintű bizonyosság);
    b) a szolgáltató által megbízott független harmadik felek vizsgálati jelentései, nemzetközi szabványnak való megfelelés tanúsításai[9] (a független felek elismertsége, reputációja[10], a tanúsítás általános elfogadottsága függvényében közepes vagy magas szintű bizonyosság);
    c) az Intézmény által közvetlenül vagy megbízása alapján független harmadik felek által végzett vizsgálat vagy akkreditált tanúsítók által végrehajtott tanúsítás (a saját vizsgálatban részt vevők felhőszolgáltatás-biztonsági szakismerete és vizsgálati tapasztalata függvényében közepes vagy magas szintű bizonyosság).

24. Az Intézmény az igénybe vett szolgáltatás kritikusságának figyelembevételével a lehető legmagasabb szintű bizonyosság elérésére törekszik, és ezt a szintet dokumentáltan rögzíti. Amennyiben az Intézmény saját vizsgálattal kíván bizonyosságot szerezni a felhőszolgáltatás kontrollkörnyezetéről, akkor biztosítja a végrehajtáshoz szükséges felhőbiztonsági és audit szakértelem rendelkezésre állását.

III.3. Szerződéses követelmények

25. Az MNB elvárja, hogy az Intézmény a IV. pontban foglaltakra is figyelemmel – a vonatkozó jogszabályi követelmények teljesítése mellett – gondoskodjon a következők szerződésben való rögzítéséről, meghatározásáról:

    a) egyértelmű eljárásrend meghatározása a szolgáltatási feltételek megváltoztatására vagy a szerződés egyéb módosítására, a szerződés megújítására, új funkciók, kiegészítések, kapcsolódó szoftverek és szolgáltatások bevezetésére;

[9] Például: ISO 27001, ISO 27017, ISO 27018, ISAE 3000, ISAE 3400, ISAE 3402

[10] A független felek értékelésének szempontjai például, de nem kizárólagosan: hasonló vizsgálatokban szerzett tapasztalatok és referenciák; pozitív ügyfélvisszajelzések; megfelelő tartalmú, terjedelmű és értékű felelősségbiztosítás; releváns tanúsítások; stabil pénzügyi háttér; etikai kódex; előadások szakmai rendezvényeken; a tanúsítási tevékenységre delegált munkatársak releváns tapasztalatai, végzettsége, képesítései.

b) a szerződés megszűnése részletes feltételeinek meghatározása mind az Intézmény, mind a szolgáltató részéről való felmondás esetén, a felmondás jogának (rendes, azonnali hatályú) részletes szabályozása, beleértve az adatok megsemmisítését;
c) az informatikai kockázatelemzés és az üzleti igények alapján a felmondási idő, az adat-visszaszolgáltatási és adattörlési eljárások oly módon történő megállapítása, hogy a szolgáltatás kivezetése a szerződés bármilyen okból való megszűnése esetén biztonságosan megvalósítható legyen, és ne járjon az üzleti folyamatok elfogadhatatlan mértékű sérülésével;
d) a szolgáltató és az általa nyújtott szolgáltatás ellenőrzési jogának kikötése az Intézmény, annak megbízottjai és az MNB részére egyaránt, beleértve a helyszíni ellenőrzés jogát;
e) amennyiben az Intézményre releváns, a szolgáltató által nyújtott szolgáltatás tanúsításának kikötése a pénzügyi intézmények, a biztosítók és a viszontbiztosítók, továbbá a befektetési vállalkozások és az árutőzsdei szolgáltatók informatikai rendszerének védelméről szóló 42/2015. (III. 12.) Korm. rendelet szerint;
f) rendelkezések rögzítése a szolgáltató által nyújtott biztosítékok rendszerére, a garanciális jogokra és a kártérítésre, különös tekintettel arra, hogy a biztosítékok arányosak legyenek az esetlegesen okozott kárral;
g) a vis maior esetek és kezelési módjuk meghatározása;
h) a licencek és szellemi alkotások kezelési módjának rögzítése;
i) a szolgáltatás, a kommunikáció nyelvének, formájának, feltételeinek és előírt tartalmának meghatározása;
j) informatikai biztonsági és adatvédelmi feladatok, felelősségek meghatározása, különös tekintettel a tájékoztatási kötelezettségekre, valamint az esetleges szolgáltatási láncra;
k) az adatkezelés, adatfeldolgozás és tárolás pontos, legalább adatközpont szintű helyszíneinek rögzítése;
l) az adatkezelés, adatfeldolgozás vagy adattárolás garanciális szabályainak meghatározása a vonatkozó hazai jogszabályokkal és uniós jogi aktusokkal összhangban, az ügyféladatok és pénzügyi ágazati titkok célhoz kötött, illetve az adatkezelés céljának megvalósulásához elengedhetetlen mértékben és ideig történő kezelése, feldolgozása és tárolása érdekében;
m) erőforrások védelmének, biztonságos üzemeltetési elvárásainak rögzítése;
n) szolgáltatási szintek (a továbbiakban: SLA-k) meghatározása, legalább az alábbiakra kitérve:
   na) a mérendő indikátorok, és azok elvárt értékei;
   nb) a mérések módja és eszközei;
   nc) a szolgáltatás elérhetősége és minimális funkcionalitása;
   nd) a méréseket végző fél, az SLA jelentések elkészítésének felelőssége, jelentések gyakorisága;
   ne) az SLA-k megsértésének kárral arányos következményei és az eszkalációs eljárások rögzítése;
o) a szolgáltató által működtetett folyamatokra vonatkozó elvárások rögzítése, beleértve a biztonságmenedzsmentet, az üzemeltetést és a fejlesztést, valamint humánerőforrással szembeni biztonsági elvárásokat;
p) biztonsági incidens kezelési eljárás rögzítése, beleértve a szolgáltató kötelezettségét arra vonatkozóan, hogy a szolgáltatást és a szolgáltatót az igénybe vett felhőszolgáltatás kapcsán ért biztonsági incidensekről késedelem nélkül tájékoztatást nyújtson;
q) támogatás és adatok biztosítása az Intézménynél esetlegesen előforduló visszaélések felderítéséhez.

III.3.1. Szolgáltatási lánc

26. Az MNB indokoltnak tartja, hogy az Intézmény mérje fel azokat a kockázatokat, amelyek a szolgáltatási lánchoz kapcsolódnak, tehát amelyek azzal függenek össze, hogy a felhőszolgáltatást nyújtó szolgáltató más szereplőket (további szolgáltatókat, alvállalkozókat, beszállítókat, közreműködőket, a továbbiakban együtt: Alvállalkozó) von be a szolgáltatás nyújtásába. Az MNB elvárja, hogy az Intézmény csak akkor vegyen igénybe szolgáltatási lánc keretében nyújtott szolgáltatást, ha az Alvállalkozó teljesíti az Intézmény és a szolgáltató közötti szerződéses kötelezettségeket, ezen belül különösen a felügyeleti hatóság ellenőrzési jogának (ideértve a helyszíni ellenőrzés jogát is) megfelelő biztosítására vonatkozó rendelkezéseket[11].
27. Az MNB elvárja az Intézménytől, hogy a szolgáltatóval kötött szerződésében érvényesítse a következőket:
    a) az Intézmény adataihoz hozzáférő, illetve az adatkezelés vagy adatfeldolgozás folyamatában érintett minden Alvállalkozó, valamint ezek feladatai, felelőssége és számonkérhetősége az Intézmény számára mindenkor aktuálisan azonosítható és átlátható legyen;
    b) a szolgáltató előzetesen tájékoztatja az Intézményt a szolgáltatások nyújtásában érintett Alvállalkozókkal kapcsolatos jelentős változásokról, oly módon, hogy az Intézmény a változással kapcsolatban kockázatelemzést végezhessen a változás megvalósulását megelőzően;
    c) az Intézmény felmondhatja a szolgáltatási szerződést, amennyiben az Alvállalkozókkal kapcsolatos változás hátrányosan hat a felhőszolgáltatás igénybevételével érintett tevékenységekkel kapcsolatos kockázatokra;
    d) az Alvállalkozók szolgáltató általi igénybevétele nem befolyásolja a szolgáltatónak az Intézménnyel kötött szerződéséből eredő kötelezettségeit, feladatait és felelősségeit.
28. Az MNB elvárja, hogy az Intézmény az igénybe vett felhőszolgáltatást a teljes szolgáltatási láncra vonatkozóan felügyelje és kövesse nyomon.

III.4. Az MNB tájékoztatása

29. Az MNB elvárja, hogy az Intézmény – szükség szerint a vonatkozó jogszabályokban előírtakat kiegészítve, azokkal együtt – tájékoztatást küldjön részére a felhőszolgáltatás igénybevételével érintett valamennyi tevékenységről a következő szempontok alapján:
    a) a felhőszolgáltató anyavállalatának adatai, amennyiben ez értelmezhető (ideértve a nevét, székhelyének címét, adószámát);
    b) a felhőszolgáltatás igénybevételével érintett tevékenységek és adatok, adatkörök bemutatása;
    c) a nyújtandó szolgáltatás helyszínéül szolgáló ország vagy országok (ideértve az adatok kezelési, feldolgozási és tárolási helyét);
    d) a szerződés hatályos változatának dátuma;
    e) a következő szerződésmegújítási határidő (adott esetben);
    f) a szerződés kapcsán irányadó jog;
    g) a szerződések és mellékleteik;
    h) a döntés-előkészítés anyagai, így különösen a következők: előny-hátrány elemzés; lényegességi értékelés; kockázatelemzés; az igénybe vett szolgáltatás kiszervezésként való minősülésével kapcsolatos felmérés, döntéshozatal dokumentumai; kivezetési stratégia.

[11] A szolgáltatási lánccal, illetve láncszerű kiszervezésekkel kapcsolatos követelményeket az Európai Bankfelügyeleti Bizottság kiszervezésről szóló, 2006. december 14-i iránymutatásain belül a 10. iránymutatás írja elő; a követelményeket részletesebben az EBA felhőszolgáltatások igénybevételével való kiszervezésre vonatkozó ajánlásain (EBA/REC/2017/03. 28/03/2018) belül pedig a 4.7. pontjában foglaltak határozzák meg.

III.5. A felhőszolgáltatás bevezetése

30. Az MNB indokoltnak tartja, hogy az Intézmény, a IV. pontban foglaltakra figyelemmel, gondoskodjon legalább az alábbiak teljesítéséről, amennyiben az az adott felhőszolgáltatás-bevezetési projekt kapcsán értelmezhető.

III.5.1. A bevezetés előkészítése

31. Az Intézmény a bevezetés előkészítése során végrehajtja a következő lépéseket és azt egyszerű és alkalmas módon dokumentálja:

    a) rögzíti az üzleti, funkcionális (például verziók, modulok), technikai (például IT és biztonsági) és kontrollkörnyezeti követelményeit, és az ezeknek való megfelelést;
    b) meghatározza a szolgáltatás bevezetéséhez kapcsolódó fejlesztések, tesztelések, migrációk és az átállás követelményeit, továbbá az éles bevezetés és a szolgáltatás elfogadási kritériumait, és mindezt ellenőrizhető módon dokumentálja;
    c) kidolgozza a migrációs stratégiát, beleértve az ütemezést, az informatikai és biztonsági elvárások meghatározását, használandó eszközök körét, és a részletes végrehajtási terv kidolgozását;
    d) rögzíti a migráció megvalósításában a szolgáltató együttműködését, feladatait, felelősségeit;
    e) részletes szolgáltatásspecifikációt, teszteseteket és tesztelési forgatókönyvet, valamint a migráció során esetlegesen fellépő rendkívüli események kezelésére vonatkozó tervet – visszaállási tervet – készít és tesztel;
    f) meghatározza az élesbe állítás engedélyezésének kritériumait és a kapcsolódó felelősségi köröket.

III.5.2. A bevezetés végrehajtása

32. Az Intézmény a bevezetés végrehajtása során végrehajtja a következő lépéseket és ezeket ellenőrizhető módon dokumentálja:

    a) implementálja a migrációs eszközöket;
    b) elemi lépésekre lebontott ütemtervet készít mérföldkövek, és erőforrások definiálásával, felelősök kijelölésével, ennek során felkészül egy pesszimista forgatókönyv esetére is;
    c) tesztkörnyezetben, tesztadatokon funkcionális, modul-, regressziós és biztonsági teszteket futtat, a teszteredményeket rögzíti, különös tekintettel az esetlegesen felmerült kritikus hibák javítására;
    d) a teszteredmények függvényében dönt az élesbe állításról vagy annak elhalasztásáról a hibák javításáig;
    e) végrehajtja az éles migrációt a forgatókönyvben definiált lépések alapján;
    f) validációt végez, a migrált adatok helyességét ellenőrzi az elfogadási kritériumok alapján. Amennyiben a migráció az Intézmény kockázatelemzése alapján kritikus funkciót vagy rendszert érint, akkor a migrációt független és a szükséges kompetenciával rendelkező féllel validáltatja a teljeskörűség, a sértetlenség és a bizalmasság szempontjai szerint.

III.6. A szolgáltatás folyamatos ellenőrzése

33. Az MNB indokoltnak tartja, hogy az Intézmény a szolgáltatás megfelelő felügyelete és ellenőrzése érdekében saját maga alkalmazza, illetve a szolgáltatóval betartassa a IV. pontban megfogalmazott követelményeket a felhőszolgáltatásra támaszkodó működés során, különös tekintettel az alábbiakra:

a) hatékony és összehangolt incidenskezelési folyamat kialakítása, működtetése az Intézmény és a szolgáltatója között;
b) katasztrófahelyzet utáni helyreállítási tervek (DR) rendszeres tesztelése;
c) a szolgáltató pénzügyi helyzetének és az SLA-k teljesítésének nyomon követése;
d) kockázatelemzés alapján meghatározott események naplózásának és a naplók sértetlenségének biztosítása, a naplók elemzése;
e) a felhőszolgáltatás kockázatelemzésének felülvizsgálata legalább az Intézmény számára jogszabályban előírt gyakorisággal vagy saját szabályzatai alapján legalább ekkora gyakorisággal, az informatikai biztonsági kockázatelemzéssel egyidejűleg, illetve a felhőszolgáltatással érintett adatkörök és funkciók jelentős megváltozása esetén;
f) csak hivatalosan kiadott, letesztelt, támogatott szolgáltatásverziók használata;
g) hivatalosan átadott, a vonatkozó hazai és uniós elvárásoknak megfelelő adatközpont helyszínek igénybevétele;
h) felkészülés a hibás teljesítés esetére, alternatív felhőszolgáltatók vagy más megoldások felmérése az üzletmenet-folytonosság biztosítására;
i) kivezetési stratégia és akcióterv rendszeres frissítése.

III.7. Kivezetés

34. Az MNB szükségesnek tartja, hogy az Intézmény a felhőszolgáltatás kivezetési fázisában hajtsa végre a 20. pontban meghatározott kivezetési stratégiában és akciótervben foglaltakat, az alábbi eljárásnak megfelelően.

III.7.1. A kivezetés előkészítése

35. Az Intézmény a kivezetés előkészítése során a kivezetés megvalósításához biztosítja a szükséges személyi, tárgyi, technikai, jogi és szerződéses feltételek meglétét, így:

    a) az adatok visszavételéhez és a szolgáltatás működtetéséhez szükséges infrastruktúrát az érintett rendszerekre támaszkodó üzleti folyamatok fennakadás nélküli, vagy legfeljebb az üzleti igények által még tolerálható mértékű fennakadásával járó működéséhez;
    b) a szolgáltatás kivezetéséhez, helyi üzemeltetéséhez, esetleg más szolgáltatóhoz történő továbbításához szükséges szaktudást, projektcsapatot;
    c) a kivezetés részletes végrehajtási tervét, beleértve a kivezetés ütemtervét, az informatikai és biztonsági feltételeket, a használandó eszközök körét, a teszteseteket és tesztelési forgatókönyveket, valamint a tesztelések és a visszavett vagy más szolgáltatóhoz költöztetett (migrált) szolgáltatás elfogadási kritériumait;
    d) részletes, lépésekre lebontott ütemtervet a mérföldkövek, és erőforrások definiálásával, felelősök kijelölésével, valamint pesszimista forgatókönyv kidolgozásával;
    e) a szolgáltatás kivezetésében érintettek együttműködésének, feladatainak, felelősségeinek rögzítettségét;
    f) a kivezetés alatt a szolgáltatás nyújtásának és adatok elérhetőségének, átadásának ütemezését, feltételeit.

III.7.2. A kivezetés végrehajtása

36. Az Intézmény a kivezetés során gondoskodik a kivezetési stratégiában és akciótervben foglalt, alábbi lépések dokumentált végrehajtásáról:

    a) migrációs eszközök telepítése;
    b) az adatok eljuttatása a célrendszerre a IV.1.1. pontban foglalt feltételek figyelembevételével;

c) visszatöltés tesztelésének végrehajtása tesztkörnyezetben;
d) éles adatok visszatöltése, a szolgáltatás-visszavétel végrehajtása a forgatókönyvek alapján;
e) validáció az elfogadási kritériumok alapján, a visszavett adatok helyességének ellenőrzése, és a migráció lezárása;
f) utógondozás biztosítása a migráció utáni javítások elvégzésére;
g) sikeres kivezetést követően a szerződésben meghatározott feltételek alapján a korábbi szolgáltatónál kezelt adatok törlése, amely kiterjed a szolgáltató éles, tartalék és esetleges mentési és archiválási környezetére is; az adatok törlésének végrehajtásáról szolgáltatói bizonyosságnyújtás (nyilatkozat) szükséges;
h) a szükségtelenné vált informatikai, kommunikációs kapcsolatok megszüntetése a szolgáltatóval;
i) a kivezetés tényének bejelentése az MNB felé.

IV. Felhőszolgáltatás-biztonsági alapelvek

37. Az MNB javasolja, hogy az Intézmény a következőkben ismertetett felhőszolgáltatás-biztonsági alapelvek és a megvalósítás lépések figyelembevételével járjon el, illetve szerezzen bizonyosságot a szolgáltató hatáskörébe eső kitételek betartásáról, a 17-25. pontban foglaltaknak megfelelően.

IV.1. Adatbiztonság, adat- és titokvédelem

38. Az MNB javasolja, hogy az adatbiztonság, adat- és titokvédelem megvalósításának előfeltételeként az Intézmény végezze el a következőket:
    a) azonosítja és biztonsági osztályba sorolja a felhőszolgáltatás igénybevételével érintett adatokat, a jogszabályoknak és saját adatvédelmi szabályozásainak megfelelően;
    b) meghatározza az adatbiztonsági és az adatvédelmi követelményeket a biztonsági osztályba sorolás szerint, a releváns szabályozás alapján.
39. Az Intézmény a technikai adatbiztonsági és adatvédelmi követelmények meghatározása, illetve a felhőszolgáltatás igénybevétele során a kockázatokkal arányos védelmet biztosító és a technika mindenkori fejlettségi szintjének megfelelő, nemzetközi szinten is biztonságosnak tekintett technikai megoldásokat (például algoritmusokat, protokollokat és paramétereket) használ.
40. Az Intézmény rendszeresen – a vonatkozó üzleti folyamatban, szolgáltatásban, konfigurációban, jogi környezetben bekövetkezett érdemi változását követően, de legalább évente – bizonyosságot szerez a felhőszolgáltató adatbiztonsági és adatvédelmi követelményeknek való teljes körű megfeleléséről. Az Intézmény a bizonyosságszerzés során a III.2.3. pontban meghatározott elvárásoknak megfelelően, a kockázatokkal arányosan támaszkodhat független harmadik felek ellenőrzésére vagy tanúsítására.
41. Az MNB felhívja a figyelmet, hogy az Intézmény felel az adatok továbbítása és tárolása során azok sértetlenségéért, bizalmasságáért és rendelkezésre állásáért.
42. Az Intézmény biztosítja a személyes adatok és az ügyfélre vonatkozó, a pénzügyi ágazati titoknak minősülő adatok biztonságos kezelését és feldolgozását, figyelemmel a mindenkor hatályos adatvédelmi szabályozásnak[12] való megfelelésre is.

[12] Lásd a mellékletben hivatkozott vonatkozó jogszabályokat.

IV.1.1. Az adatok biztonsága továbbítás közben

43. Az Intézmény és a felhőszolgáltató az adatok továbbítása során érvényesülő biztonsága érdekében gondoskodik az Intézmény és a felhő közti, a felhőben levő erőforrások közti, valamint a felhő és más külső szolgáltatók közti adatforgalom védelméről az illetéktelen megismeréssel és módosítással szemben, továbbá a hálózati kapcsolatok rendelkezésre állásáról és elvárt adatátviteli sebességükről.

44. Az Intézmény és a felhőszolgáltató az alkalmazott felhőszolgáltatási modell függvényében gondoskodnak a hatáskörükbe tartozó rendszerelemek vonatkozásában a következőkről:

    a) biztosítják a szolgáltatás adatforgalmának titkosítását és integritásvédelmét. Ezzel összefüggésben az Intézmény kockázatokkal arányosan alkalmaz további intézkedéseket a távközlési szolgáltatók által esetlegesen biztosított vonali titkosításon és integritásvédelmen felül;
    b) biztosítják a kommunikációban részt vevő eszközök és felhasználók autentikációját;
    c) biztosítják a hálózati kapcsolatok rendelkezésre állását, hibatűrését és az üzemszerű működéshez szükséges hálózati sávszélességeket az elvárt szolgáltatási szinteknek megfelelően.

45. A 43. és 44. pontban leírtak vonatkoznak a szolgáltatás- és rendszermenedzsment folyamatok által generált adatforgalomra is.

46. Amennyiben a felhőt érintő adatfeltöltés vagy letöltés nem csak hálózaton keresztül valósul meg, úgy a felhasznált fizikai adathordozókra is vonatkoznak a 44. pontban felsorolt, bizalmasságot és sértetlenséget biztosító kontroll intézkedések.

IV.1.2. A tárolt adatok biztonsága

47. Az Intézmény és a felhőszolgáltató a tárolt adatok kapcsán, az azokat felhasználó üzleti folyamat biztonsága érdekében gondoskodik a felhőben tárolt adatok rendelkezésre állásáról, illetve az adatok védelméről az illetéktelen megismerés és módosítás ellen.

48. Az Intézmény és a felhőszolgáltató az alkalmazott felhőszolgáltatási modell függvényében gondoskodnak a hatáskörükbe tartozó rendszerelemek vonatkozásában a következőkről:

    a) következetesen érvényesítik a saját hatáskörükben megoldható adatbiztonsági követelményeket, például megfelelő logikai adathozzáférési kontrollok kialakításával (a lehetőségek a felhőszolgáltatási modell függvényében változnak);
    b) az adatok rendelkezésre állásának paramétereit úgy határozzák meg, hogy azok összhangban legyenek az érintett üzleti folyamatok helyreállításának elvárt időtartamaival (RTO) és időpontjaival (RPO[13]);
    c) meghatározzák a tárolt adatok biztonságos törlésének követelményeit, beleértve a mentések és archívumok törléséhez szükséges eszközöket és eljárásokat, és ehhez kapcsolódóan a szolgáltató által nyújtandó bizonyosságot;
    d) a szolgáltató felelősségi körébe tartozó adatbiztonsági követelményeknek való megfelelésről szóló bizonyosságszerzés során kitérnek a bizalmasság, a sértetlenség és a rendelkezésre állás aspektusaira, valamint az adattároló eszközök selejtezése során azok biztonságos megsemmisítésére;
    e) a kockázatelemzés alapján kritikus funkcionalitás vagy rendszer esetén az Intézmény gondoskodik az adatmentések felhőszolgáltatótól független tárolásáról is; a függetlenül tárolt

[13] Az adatvesztés megengedett időtartama.

mentések rendszerességét a kockázatok és jogszabályi elvárások figyelembevételével határozza meg.

IV.1.3. Adatvédelem

49. Az Intézmény az adatok védelme érdekében meggyőződik a rá irányadó adatvédelmi jogszabályok és előírások felhőszolgáltató általi betartásáról.

50. Az adatok védelme érdekében az Intézmény:

    a) feltárja a különbségeket egyrészt az Intézményre vonatkozó releváns adatvédelmi jogi követelmények, másrészt a felhőszolgáltató adatvédelmi vállalásai és gyakorlata, valamint adatszolgáltatási kötelezettségei közt; a különbségek feltárása során:
        aa) összeveti a szolgáltató adatkezelői és adatfeldolgozói gyakorlatát az Intézményre vonatkozó elvárásokkal;

        ab) felméri, hogy a szolgáltató mikor, milyen feltételekkel köteles adatokat kiadni hatóságoknak (például a szolgáltató honos szabályozása alapján), és milyen értesítési eljárást vállal az ilyen kötelezések teljesítése során;

        ac) felméri, hogy a szolgáltató Alvállalkozói, egyéb üzletfelei az adatkezelés céljával összhangban férnek-e hozzá az adatokhoz, az adatkezelés alanya mikor, milyen feltételekkel férhet hozzá a róla tárolt adatokhoz, és kockázat azonosítása esetén mérlegelése szerint nem járul hozzá az Alvállalkozó vagy egyéb harmadik személy igénybevételéhez azzal, hogy az Alvállalkozók felmérése nem jelent az Intézmény oldalán az ellenőrzési jog eredeti célján túlterjeszkedő jogosultságot;

    b) olyan szerződéses feltételeket alkalmaz, amelyek kezelik a feltárt különbségeket, biztosítva a teljes körű megfelelést.

51. Az Intézmény saját felelősségi körében meghozandó, az adatok védelmére irányuló intézkedéseiről a mellékletben felsorolt jogszabályokon, uniós jogi aktusokon, illetve MNB ajánlásokon kívül a Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: NAIH) ajánlásai[14] rendelkeznek.

IV.2. Erőforrások védelme

52. Az MNB elvárja, hogy az Intézmény az erőforrások védelme érdekében meggyőződjön a felhőben a részére allokált erőforrások (feldolgozó és tároló kapacitásainak) illetéktelen fizikai vagy logikai hozzáférés, sérülés és eltulajdonítás elleni védelméről. Az MNB javasolja, hogy ennek során az Intézmény az alábbiak szerint járjon el.

53. Az erőforrások védelme érdekében az Intézmény:

    a) magas szintű bizonyosságot szerez a felhőszolgáltató adatközpontjainak, számítástechnikai, kommunikációs eszközeinek védelméről, a rendelkezésre állás biztosításáról;
    b) magas szintű bizonyosságot szerez a felhőszolgáltató ügyfelei adatainak és rendszereinek elkülönítéséről;
    c) a bizonyosságszerzés részeként kitér – a felhőszolgáltatási modell függvényében – legalább a következőkre:
        ca) a fizikai erőforrások fizikai hozzáférési és környezeti kontrolljaira;

[14] A NAIH ajánlásai elérhetők: https://www.naih.hu/ajanlasok.html

cb) a virtualizációs infrastruktúra logikai hozzáférési kontrolljaira, biztonsági beállításaira, beleértve a hipervizort, a virtuális adattárolókat, a virtuális hálózatokat; valamint ezek menedzsment eszközeinek védelemére;
cc) az operációs rendszerek, a köztes réteg (middleware), az adatbázisok, és az alkalmazások logikai hozzáférési kontrolljaira, biztonsági beállításaira, beleértve a gyártói és iparági ajánlások alapján biztonságilag megerősített konfigurációk használatát;
cd) a különböző ügyfelekhez tartozó erőforrások szétválasztásának technikai megvalósítására, különös tekintettel a menedzsment interfészekre [például webes adminisztrációs felületek, alkalmazásprogramozási interfészek (API-k)];
ce) a kriptográfiai kulcsok menedzsmentjére, beleértve a HSM (Hardware Security Module – hardver biztonsági modul) használatát.

IV.3. Informatikai folyamatok biztonsága

54. Az MNB elvárja, hogy az Intézmény az informatikai folyamatok biztonsága érdekében a felhőszolgáltatás adatbiztonságát, adatvédelmét, valamint az erőforrások védelmét – végső soron a felhőszolgáltatás biztonságát – szabályozott és ellenőrzött információbiztonság-irányítási rendszerrel és biztonságos folyamatokkal valósítsa meg, figyelembe véve az alábbiakat.

IV.3.1. Biztonságmenedzsment

55. Az informatikai folyamatok biztonsága érdekében az Intézmény elvégzi a következő biztonságmenedzsment tevékenységeket.

a) Az Intézmény a III.2.3. pontban ismertetett módon bizonyosságot szerez a szolgáltató információbiztonság-irányítási rendszeréről, folyamatairól, és ezek kontrolljainak működéséről; illetve megosztott hatáskör esetén a saját hatáskörébe tartozó elemekre vonatkozóan kialakítja ezeket, legalább az alábbi hatókörben:
   aa) az információbiztonság-irányítási (ISMS) rendszer nemzetközi szabvány szerinti tanúsítása, amennyiben a bizonyosságszerzés elvárt szintje ezt indokolja;
   ab) az információbiztonsági szervezet struktúrája, szerepkörök szétválasztása;
   ac) az információbiztonsági kockázatkezelési rendszer, beleértve a humánkockázat kezelését is: az Intézmény elvárja a szolgáltató munkavállalóira és Alvállalkozóira vonatkozó humánkockázati szűrést, továbbá rendszeres információbiztonsági tudatossági oktatást;
   ad) a belső és külső biztonsági ellenőrzési funkciók működése és eredményei: az Intézmény a kockázatokkal arányosan elvárja az általános biztonsági vizsgálatokat, sérülékenység-vizsgálatokat, betörési teszteket, nemzetközi biztonsági szabványok szerinti tanúsításokat;
   ae) a felfedezett biztonsági sérülékenységek kijavításának gyors és hatásos folyamata, és az erről való tájékoztatás;
   af) konfigurációkezelési rendszerek naprakészen tartása,
   ag) az üzletmenet-folytonosság kezelése, rendelkezésre állás biztosítása, mentési rendszer és katasztrófahelyzet esetén a visszaállást támogató megoldások: az Intézmény elvárja a BCP/DRP tervek rendszeres tesztelését és a tervek rendszeres frissítését;
   ah) biztonságos architektúratervezés, a legjobb gyakorlatnak megfelelő hálózatbiztonsági kontrollok;

ai) felhasználó- és jogosultságkezelés: az Intézmény elvárja, hogy a felhőben allokált erőforrásaihoz kizárólag a szolgáltató feljogosított munkatársai férhetnek hozzá, dokumentált jóváhagyási folyamat mentén;

aj) biztonsági naplózás és monitorozás: az Intézmény elvárja, hogy a szolgáltatást vagy a szolgáltatót a felhőszolgáltatás kapcsán ért biztonsági eseményekről, incidensekről riasztások, naplóbejegyzések készüljenek, és ezek legyenek megfelelően védettek és igény esetén kerüljenek megosztásra az Intézménnyel;

ak) biztonsági incidensek kezelése, értesítési rendszere: az Intézmény elvárja a rá hatással levő biztonsági incidensekről és megoldásukról való késedelem nélküli értesítést;

al) visszaélés-felderítési vizsgálatok: az Intézmény elvárja az ilyen vizsgálatok elvégzésének szolgáltató általi támogatását, és a folyamat szabályozását;

am) rosszindulatú kódok elleni védelem, beleértve a védelmi eszközök telepítését, rendszeres frissítését és központi felügyeletét, valamint a hálózat és az eszközök rendszeres vírusvédelmi vizsgálatát;

an) mobileszköz-menedzsment, beleértve a mobil menedzsmenteszközök, a végfelhasználói mobileszközök kapcsán mobil eszközök azonosítását, nyilvántartását, a biztonsági követelményeik meghatározását és betartatását (például hozzáférés-védelem, titkosítás, adatszivárgás elleni védelem;

ao) határvédelem, beleértve a megfelelően szabályozott hálózati kapcsolati szabályrendszer kialakítását és technológiai eszközökkel történő kikényszerítését, az adatszivárgás elleni védelem biztosítását, valamint a behatolásérzékelést és -megelőzést.

b) Az Intézmény igénybe veszi a szolgáltató által esetlegesen működtetett megfelelőségi (compliance) és biztonsági programokat, melyek által lehetősége nyílik például:

ba) közvetlen kapcsolat, kommunikáció kialakítására a szolgáltató biztonsági és compliance felelőseivel, szakértőivel, belső és külső ellenőreivel;

bb) a jogszabályi megfelelés biztosításához szükséges tanúsítási, kockázatkezelési és auditjelentések részleteinek megismerésére;

bc) egyedi igények benyújtására a kontrollkörnyezet bővítése, javítása és tanúsítása érdekében;

bd) a biztonságos és átlátható működést lehetővé tevő további szolgáltatások igénybevételére (például rendszeres betörési tesztelés, közös DRP tesztelés, biztonsági fórumban való részvétel).

c) Az Intézmény igénybe veszi a szolgáltató által esetlegesen működtetett kiterjesztett hatókörű értesítési rendszert a biztonsági incidensekről, amely az Intézményt közvetlenül érintő incidenseken túlmenően kiterjed a szolgáltatót vagy más ügyfeleit érintő eseményekre is, valamint a sikertelen (DRP és biztonsági) tesztelésekre, mivel mindezek közvetlen, vagy közvetett fenyegetést jelenthetnek az Intézményre.

IV.3.2. Üzemeltetés biztonsága

56. Az üzemeltetés biztonsága érdekében az Intézmény bizonyosságot szerez a szolgáltató informatikai üzemeltetési folyamatainak kontrollállt működéséről, illetve megosztott hatáskör esetén a saját hatáskörébe tartozó elemekre vonatkozóan kialakítja ezeket, legalább az alábbi hatókörben:

a) üzemeltetési eljárások és felelősségek meghatározása, dokumentálása;
b) mentési és visszatöltési eljárások;
c) üzemeltetési felügyelet (monitorozás) és naplózás;
d) eszközkezelés (eszközök azonosítása, nyilvántartása és kezelése azok teljes életciklusán keresztül);
e) változtatás- és verziókezelés, konfigurációmenedzsment;
f) incidens-, probléma- és igénykezelés, valamint az ezekhez kapcsolódó értesítési eljárások;
g) SLA-k elvárásai, kezelése, monitorozása, jelentése.

IV.3.3. Fejlesztés biztonsága

57. A fejlesztési tevékenységek biztonsága érdekében az Intézmény bizonyosságot szerez a szolgáltatást érintő fejlesztési folyamatok kontrollállt működéséről, illetve megosztott hatáskör esetén a saját hatáskörébe tartozó elemekre vonatkozóan kialakítja ezeket, legalább az alábbi hatókörben:

    a) dokumentált fejlesztési irányelvek, módszertanok alkalmazása, különös tekintettel a biztonságos fejlesztési módszerekre és gyakorlatokra;
    b) biztonsági elvárások dokumentálása és beépítése a fejlesztésekbe;
    c) fejlesztési és tesztelési környezetek kialakítása, szeparáltságuk biztosítása;
    d) biztonsági és betörési tesztek alkalmazása az éles üzembe helyezést megelőzően, majd az üzembe helyezést követően legalább éves rendszerességgel;
    e) Alvállalkozók fejlesztéseinek minőségbiztosítása és kontrollja.

IV.4. Felhasználó- és jogosultságkezelés[15]

58. Az MNB elvárja, hogy az Intézmény a felhasználó- és jogosultságkezelés biztonságának érdekében gondoskodjon a felhőszolgáltatáshoz való hozzáférések szükséges és elégséges szintre korlátozásáról, az üzleti igényekkel összhangban, megfelelő azonosítási, hitelesítési (autentikációs) és jogosultsági (autorizációs) megoldások használatával, az alábbiaknak megfelelően.

59. A felhasználó- és jogosultságkezelés biztonságának érdekében az Intézmény és a felhőszolgáltató az alkalmazott felhőszolgáltatási modell függvényében gondoskodik a hatáskörükbe tartozó rendszerelemek vonatkozásában a következőkről:

    a) az Intézmény a lokális rendszereivel legalább azonos szintű, dokumentált és jóváhagyott felhasználó- és jogosultságkezelési eljárást alakít ki a felhőszolgáltatáshoz való hozzáférés kontrolljára, amely kiterjed az igénylés, az engedélyezés, a beállítás, a rendszeres felülvizsgálat, és a visszavonás folyamataira;
    b) a kockázatokkal arányos módon mérlegelik a többfaktoros autentikációval történő azonosítást legalább a kiemelt (privilegizált) felhasználók vonatkozásában;
    c) a kiemelt felhasználók szolgáltatással összefüggő tevékenységét naplózzák, a naplókat pedig rendszeresen ellenőrzik, és az ellenőrzést az Intézmény számára is biztosítják;
    d) az Intézmény meghatározza a felhőszolgáltatással kapcsolatos összeférhetetlen szerepköröket és jogosultságokat;
    e) az Intézmény teljes körű, naprakész, a beállításokkal összevethető nyilvántartással rendelkezik az engedélyezett felhasználókról és jogosultságaikról, beleértve a kiemelt, a technikai és a külső/távoli felhasználókat is;

[15] Ez a pont az Intézmény érdekkörébe tartozó felhasználók és jogosultságaik kezelésére vonatkozó követelményeket rögzíti. A felhőszolgáltató érdekkörébe tartozó felhasználók és jogosultságaik kezelésére vonatkozó követelmények az 55. pont ai) alpontjában találhatók.

f) a felhasználó- és jogosultságkezelést végzők tevékenysége rendszeresen ellenőrzött (ki, mikor, mit igényelt, engedélyezett, állított be, vizsgált felül, vont vissza).

V. Felügyeleti ellenőrzés

60. Az MNB a vonatkozó jogszabályi előírások alapján az Intézménynél és rajta keresztül a felhőszolgáltatást nyújtó szolgáltatónál, valamint az Alvállalkozónál is ellenőrizheti a felhőszolgáltatás kontrollkörnyezetét. Az Intézmény a szolgáltatás szerződéses feltételeivel köteles biztosítani, hogy a felhőszolgáltatás igénybevétele ne akadályozza az MNB-t feladatai teljesítésében, illetve a szolgáltató és az Alvállalkozó működjön együtt az MNB-vel, az MNB a felhőszolgáltatás vizsgálata során helyszíni vagy helyszínen kívüli vizsgálatot végezhessen a szolgáltatónál és az Alvállalkozónál is.

61. A felhőszolgáltatás vizsgálatának elsődleges célja megállapítani a következőket:

    a) biztosított-e az Intézmény zavartalan működéséhez és az üzleti célok teljesítéséhez szükséges informatikai megoldás, illetve ennek folyamatos működtetéséhez és továbbfejlesztéséhez a feltételek rendelkezésre állnak-e;
    b) az Intézmény vezetése felmérte-e és kellő módon értékelte-e a felhőszolgáltatás és annak továbbfejlesztésével kapcsolatos biztonsági kockázatokat, kiépítette-e a kockázatokkal arányos kontrollokat, megteremtette-e a kontrollok folyamatos működéséhez szükséges szerződéses, szabályozási, vezetési, személyi, technikai és ellenőrzési feltételeket;
    c) a szerződésben rögzített kontrollok működnek-e, azok működését milyen eszközökkel biztosítják, és hogyan ellenőrzik;
    d) az Intézmény és a szolgáltató, valamint az Alvállalkozó betartja-e a vonatkozó jogszabályokat a felhőszolgáltatás igénybevétele során.

62. A 61. pontban meghatározott célok teljesítése érdekében az MNB vizsgálata, figyelemmel a jelen ajánlásra, hangsúlyt helyez a következők ellenőrzésére:

    a) a döntés-előkészítés anyagai, különösen az előny-hátrány elemzés, követelménylisták, lényegességi értékelés;
    b) a kockázatelemzés és a kockázatcsökkentő intézkedések;
    c) a szolgáltatáskivezetési stratégia és akcióterv;
    d) a felhőszolgáltatásról szóló szerződés(ek) és kiegészítései(k);
    e) az informatikai biztonsági és adatvédelmi követelmények meghatározása és érvényesítése, az IT kontrollok megfelelősége;
    f) az Intézmény bizonyosságszerzésének megfelelősége;
    g) BCP/DRP tervek, tesztjegyzőkönyvek;
    h) a függetlenül tárolt mentések ellenőrzése.

VI. Záró rendelkezések

63. Az ajánlás a Magyar Nemzeti Bankról szóló 2013. évi CXXXIX. törvény 13. § (2) bekezdés i) pontja szerint kiadott, a felügyelt Intézményekre 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.

64. Az ajánlásnak való megfelelést az MNB az általa felügyelt Intézmények körében az ellenőrzési és monitoringtevékenysége során figyelemmel kíséri és értékeli, összhangban az általános európai felügyeleti gyakorlattal.

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

66. Az MNB a jelen ajánlás alkalmazását 2019. május 1-től várja el az érintett Intézményektől.

67. 2019. május 1-én hatályát veszti a Magyar Nemzeti Banknak a közösségi és publikus felhőszolgáltatások igénybevételéről szóló 2/2017. (I. 12.) számú ajánlása.

Dr. Matolcsy György sk.
a Magyar Nemzeti Bank elnöke

1. melléklet a 4/2019. (IV.1.) számú MNB ajánláshoz

Egyes kapcsolódó jogszabályok, ajánlások, iránymutatások

1. Pénzügyi ágazati jogszabályok és uniós jogi aktusok

1.1. az Önkéntes Kölcsönös Biztosító Pénztárakról szóló 1993. évi XCVI. törvény;

1.2. a magánnyugdíjról és a magánnyugdíjpénztárakról szóló 1997. évi LXXXII. törvény;

1.3. a foglalkoztatói nyugdíjról és intézményeiről szóló 2007. évi CXVII. törvény;

1.4. a tőkepiacról szóló 2001. évi CXX. törvény;

1.5. a befektetési vállalkozásokról és az árutőzsdei szolgáltatókról, valamint az általuk végezhető tevékenységek szabályairól szóló 2007. évi CXXXVIII. törvény;

1.6. a pénzforgalmi szolgáltatás nyújtásáról szóló 2009. évi LXXXV. törvény;

1.7. a Magyar Nemzeti Bankról szóló 2013. évi CXXXIX. törvény;

1.8. az egyes fizetési szolgáltatókról szóló 2013. évi CCXXXV. törvény;

1.9. a hitelintézetekről és a pénzügyi vállalkozásokról szóló 2013. évi CCXXXVII. törvény;

1.10. a kollektív befektetési formákról és kezelőikről, valamint egyes pénzügyi tárgyú törvények módosításáról szóló 2014. évi XVI. törvény;

1.11. a biztosítási tevékenységről szóló 2014. évi LXXXVIII. törvény;

1.12. a pénzügyi intézmények, a biztosítók és a viszontbiztosítók, továbbá a befektetési vállalkozások és az árutőzsdei szolgáltatók informatikai rendszerének védelméről szóló 42/2015. (III. 12.) Korm. rendelet;

1.13. a biztosítási és viszontbiztosítási üzleti tevékenység megkezdéséről és gyakorlásáról szóló 2009/138/EK európai parlamenti és tanácsi irányelv (Szolvencia II) kiegészítéséről szóló 2014. október 10-i (EU) 2015/35 felhatalmazáson alapuló bizottsági rendelet;

1.14. az üzleti titok védelméről szóló 2018. évi LIV. törvény.

2. Adatvédelmi, információbiztonsági jogszabályok

2.1. az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény;

2.2. az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény és végrehajtási rendeletei;

2.3. 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 (EU) 2016/679 európai parlamenti és tanácsi rendelet (általános adatvédelmi rendelet – GDPR).

3. Ajánlások, iránymutatások

3.1. az Európai Bankfelügyeleti Bizottság kiszervezésről szóló, 2006. december 14-i iránymutatása;[16]

3.2. az Európai Biztosítás- és Foglalkoztatóinyugdíj-hatóság irányítási rendszerre vonatkozó iránymutatásai (EIOPA-BoS-14/253)[17], valamint az azokkal kapcsolatban közzétett jelentés („Final Report on Public Consultation No. 14/017 on Guidelines on System of Governance”);[18]

3.3. az EBA felhőszolgáltatások igénybevételével való kiszervezésre vonatkozó ajánlásai (EBA/REC/2017/03);

3.4. az interneten keresztül nyújtott pénzügyi szolgáltatások biztonságáról szóló 15/2015. MNB ajánlás;

3.5. a belső védelmi vonalak kialakításáról és működtetéséről, a pénzügyi szervezetek irányítási és kontroll funkcióiról szóló 27/2018. (XII. 10.) MNB ajánlás;

3.6. a biztosítók és viszontbiztosítók irányítási rendszeréről szóló 4/2016. (VI. 06.) MNB ajánlás;

3.7. az informatikai rendszer védelméről szóló 7/2017. (VII. 5.) MNB ajánlás.

4. A létfontosságú rendszerek és létesítmények kijelölésével kapcsolatos jogszabályok

4.1. a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény;

4.2. a pénzügyi ágazathoz tartozó létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 330/2015. (XI. 10.) Korm. rendelet.

[16] Az Európai Bankfelügyeleti Bizottság irányelvei elérhetők: https://www.eba.europa.eu/documents/10180/104404/GL02OutsourcingGuidelines.pdf.pdf

[17] Az EIOPA irányelvei elérhetők: https://eiopa.europa.eu/guidelinessii/eiopa_guidelines_on_system_of_governance_en.pdf

[18] Az EIOPA jelentése elérhető: https://eiopa.europa.eu/publications/consultations/eiopa_eiopa-bos-14-253-final%20report_governance.pdf

Tartalomjegyzék