A Magyar Nemzeti Bank 2/2017. (I.12.) számú ajánlása

a közösségi és publikus felhőszolgáltatások igénybevételéről

I. Az ajánlás célja és hatálya

Jelen ajánlás célja, hogy a pénzügyi szervezetek számára gyakorlati útmutatást adjon a közösségi és publikus felhőszolgáltatások igénybevételéből eredő kockázatok kezeléséhez és a vonatkozó jogszabályi rendelkezések egységes alkalmazásához.

Az ajánlás – a felhőszolgáltatás életciklusát és az alapelveket követve – útmutatást ad a jogszabályi előírások betartásához, 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) ellenőrzéseinek fő szempontjait.

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

Jelen ajánlás nem érinti az informatikai rendszer védelméről szóló 1/2015. MNB ajánlásban, valamint az interneten keresztül nyújtott pénzügyi szolgáltatások biztonságáról szóló 15/2015. MNB ajánlásban foglaltakat, az MNB a hivatkozott ajánlásokban foglaltaknak való megfelelést továbbra is elvárja.

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[1]. A felhőszolgáltatás öt lényegi ismérve a következő:
   a) a szolgáltatás igény szerinti, akár önkiszolgáló módon való igénybe vétele;
   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 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

[1] A felhőszolgáltatás ajánlásbeli definíciójának alapját a NIST következő dokumentuma képezi: *The NIST Definition of Cloud Computing (SP 800-145)* http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

tartozó intézmények vagy kormányzati szervek) számára megosztott módon elérhető felhőszolgáltatást értünk.

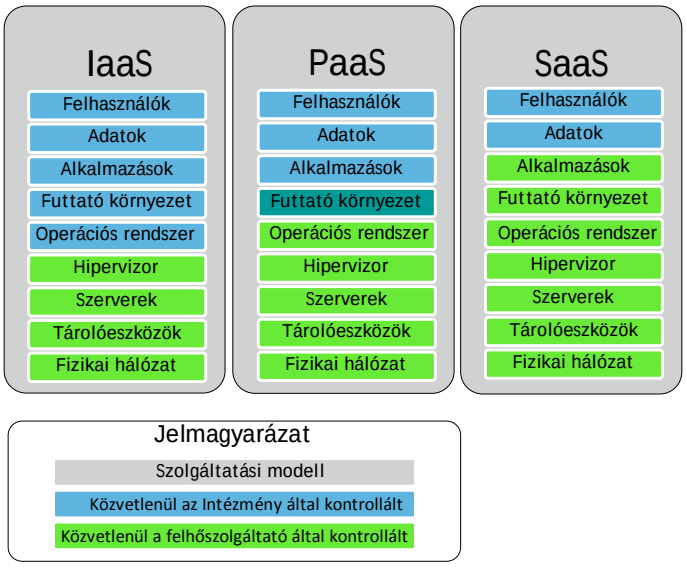
3. A felhő három fő szolgáltatási modellben érhető el:

   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. A pénzügyi szervezet felelőssége azonosítani a kockázatokat a felhőszolgáltatás életciklusának minden fázisában, és megvalósítani az arányos védelmi intézkedéseket, legalább a következőkben leírt szempontok figyelembe vételével.

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

6. Az informatikával kapcsolatos üzleti igények, tulajdonosi elvárások (például költségcsökkentés, rugalmasság, hullámzó kapacitás igény, beruházási költségérzékenység, gyors bevezetés) kielégítése érdekében felmerülhet a felhőszolgáltatás is lehetséges megoldásként. A felhőszolgáltatás iránti igény felmerülése esetén a pénzügyi szervezet megvizsgálja a felhőszolgáltatás létjogosultságát az üzleti igények, a felhőszolgáltatás képességei, költségei és kockázatai, a biztonsági követelmények és a jogszabályi előírások alapján. A döntés-előkészítés és a tervezés során a pénzügyi szervezet az alábbiak szerint jár el.

III.1.1. Jogszabályi megfelelés biztosítása

7. A felhőszolgáltatás igénybevétele a hatályos pénzügyi ágazati jogszabályok[2] szerint kiszervezésnek minősül, amennyiben személyes adatot vagy az ügyfélre vonatkozó, a pénzügyi ágazati törvények által védett titoknak minősülő adatot érint. A pénzügyi szervezet felméri a kiszervezésre (és így a felhőszolgáltatásokra is) vonatkozó jogszabályi előírásoknak való tételes megfeleléshez szükséges tennivalóit már a döntés-előkészítési fázisban[3]. A felhőszolgáltatás igénybevételével a jogszabály szerinti működés felelőssége megmarad a pénzügyi szervezetnél, így a pénzügyi szervezet annak igénybevételét megelőzően megvizsgálja, hogy a kötelezettségeit miként tudja teljesíteni, illetve az adott felhőszolgáltató miként biztosítja számára a szükséges kontrollokat és monitorozási lehetőséget.
8. A felhőszolgáltatás igénybevételét megelőzően a pénzügyi szervezet meggyőződik a felhőszolgáltatás jogszabályi megfelelésének teljes körű biztosíthatóságáról.
9. Amennyiben a pénzügyi szervezetet, illetve az általa használt rendszer a pénzügyi ágazathoz tartozó európai vagy nemzeti létfontosságú rendszerelemként került kijelölésre, akkor a pénzügyi szervezetnek figyelembe kell vennie az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény – különösen annak 3. § (2) bekezdése –, illetve a törvény végrehajtására kiadott 77/2013. (XII. 19.) NFM rendelet[4] vonatkozó rendelkezéseit.

III.1.2. Költség-haszon elemzés

10. A pénzügyi szervezet felhőszolgáltatás igénybevételéről szóló döntése megalapozásához költség-haszon 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 kontroll-költségek 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 adat-visszatöltés lehetőségei és becsült költségei.

[2] Lásd a melléklet 1. pontjában felsorolt jogszabályokat.

[3] A releváns jogszabályhelyek megjelölése az 1. melléklet 1. pontjában foglalt, a szabályozás szempontjából érintett jogszabályoknál található.

[4] A nemzeti fejlesztési miniszter 77/2013. (XII. 19.) NFM rendelete az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, valamint a biztonsági osztályba és biztonsági szintbe sorolási követelményeiről

III.2. A felhőszolgáltatás kockázatelemzése

11. A pénzügyi szervezet informatikai kockázatelemzése – amelynek fogalmába beleértendő a kockázatok felmérése (azonosításuk és értékelésük), valamint a kockázatcsökkentő intézkedések megtervezése – kitér a jelen és a 25-47. pontokban felsorolt követelmények megvalósításának lehetőségeire, és a szolgáltatás életciklusának valamennyi fázisára. Ezen követelmények teljesítésére – a szolgáltatási modell függvényében – a pénzügyi szervezet saját hatáskörben működtet kontrollokat vagy szerződésben rögzíti azok szolgáltató általi működtetését, melyek működéséről bizonyosságot szerez.

12. A pénzügyi szervezet vezetése gondoskodik a kockázatcsökkentő intézkedési tervek kidolgozásáról, az intézkedések végrehajtásához szükséges feltételek biztosításáról, és a megtett intézkedések ellenőrzéséről. A pénzügyi szervezetnek kockázatcsökkentő intézkedésekkel (kontrollokkal) kell kezelnie a jogszabályi meg nem felelést okozó kockázatokat, azaz nem háríthatja át és nem fogadhatja el az ilyen típusú kockázatokat.

III.2.1. A kivezetés kockázatai

13. A pénzügyi szervezet 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 szolgáltatás-kivezetési (exit) stratégiát és akciótervet dolgoz ki.

14. A pénzügyi szervezet a kivezetési stratégia részeként:

    a) olyan szerződési feltételeket köt ki, amelyek nehézség nélkül lehetővé teszik a felhőből való kilépést (lásd a 18. pontot), különös figyelemmel a tárolt adatok rendelkezésre bocsátására a felhőszolgáltatástól függetlenül értelmezhető és felhasználható formában;
    b) biztosítja és a kockázatok mértékének megfelelő gyakorisággal és módszerrel ellenőrzi a felhőszolgáltatás megszűnése esetén az erre támaszkodó üzleti folyamatok működtethetőségét.

III.2.2. Bizonyosságszerzés

15. A pénzügyi szervezet dokumentálja, hogy milyen szintű bizonyosságot kell szereznie a felhőszolgáltató kockázatcsökkentő intézkedéseinek megvalósulásáról, a nyújtott szolgáltatás kontrollkörnyezetére vonatkozóan.

16. 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 harmadik felek vizsgálati jelentései, nemzetközi szabványnak való megfelelés tanúsításai[5] (a független felek elismertsége, reputációja, a tanúsítás általános elfogadottsága függvényében közepes vagy magas szintű bizonyosság);

    c) a pénzügyi szervezet által közvetlenül, vagy megbízása alapján 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).

[5] ISO 27001, ISO 27017, ISO 27018, ISAE 3000, ISAE 3400, ISAE 3402

17. A pénzügyi szervezet a bizonyosságszerzés szükséges szintjét az adott terület kockázatosságával összhangban határozza meg, a minél magasabb szintű bizonyosságszerzés érdekében. Amennyiben a pénzügyi szervezet saját vizsgálattal kíván bizonyosságot szerezni a felhőszolgáltatás kontrollkörnyezetéről, akkor biztosítania kell a végrehajtáshoz szükséges felhőbiztonsági és -audit szakértelem rendelkezésre állását.

III.3. Szerződéses követelmények

18. Elvárt, hogy a pénzügyi szervezet a IV. fejezetben foglaltakra figyelemmel gondoskodjon a következők szerződésben való teljesüléséről:

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

    b) a szerződés megszűnése részletes feltételeinek meghatározása mind a pénzügyi szervezet, mind a szolgáltató részéről való felmondás esetén, a felmondás jogának (rendes, azonnali hatályú) részletes szabályozása;

    c) az informatikai kockázatelemzés és az üzleti igények alapján a felmondási időt, az adat-visszaszolgáltatási és adattörlési eljárásokat úgy kell megállapítani, 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 és – a 42/2015. (III. 12.) Korm. rendelet szerinti – tanúsítási jogának kikötése a pénzügyi szervezet, annak megbízottai és az MNB részére egyaránt, beleértve a helyszíni ellenőrzés jogát is azzal, hogy az ellenőrzés jogának gyakorlását csak ésszerű keretek között lehet korlátozni, melyek nem gátolják, vagy jelentősen nem hátráltatják az ellenőrzés végrehajtását;

    e) rendelkezések rögzítése a biztosítéki rendszerre, a garanciális jogokra és a kártérítésre, különös tekintettel arra, hogy a biztosítékok arányosak legyenek az esetlegesen okozott kárral;

    f) a vis maior esetek és kezelési módjuk meghatározása;

    g) a licencek és szellemi alkotások kezelési módjának rögzítése;

    h) a szolgáltatás, a kommunikáció nyelvének, formájának, feltételeinek és előírt tartalmának meghatározása;

    i) informatikai biztonsági és adatvédelemi kötelezettségvállalások, az adatkezelés, adatfeldolgozás és tárolás pontos, legalább adatközpontú helyszíneinek rögzítése, különös tekintettel az adatok átadhatóságával, továbbadhatóságával kapcsolatos előírásokra;

    j) annak biztosítása, hogy a pénzügyi szervezet adataihoz hozzáférő, illetve az adatkezelés vagy adatfeldolgozás folyamatában érintett minden alvállalkozó, közreműködő, beszállító, valamint ezek feladatai, felelőssége és számonkérhetősége a pénzügyi szervezet számára mindenkor aktuálisan azonosítható és átlátható legyen;

    k) erőforrások védelmének, biztonságos üzemeltetési elvárásainak rögzítése;

    l) szolgáltatási szintek (a továbbiakban: SLA-k) meghatározása, legalább az alábbiakra kitérve:

        la) a mérendő indikátorok, és azok elvárt értékei;

        lb) a mérések módja és eszközei;

        lc) a szolgáltatás elérhetősége és minimális funkcionalitása;

        ld) a méréseket végző fél, az SLA jelentések elkészítésének felelőssége, jelentések gyakorisága.

le) az SLA-k megsértésének kárral arányos következményei és az eszkalációs eljárások rögzítése;

m) a szolgáltató által működtetett informatikai folyamatokra vonatkozó elvárások rögzítése, beleértve a biztonságmenedzsmentet, az üzemeltetést és a fejlesztést, valamint humánerőforrással szembeni biztonsági elvárásokat;

n) biztonsági incidens kezelési eljárás rögzítése, beleértve a szolgáltató kötelezettségét arra vonatkozóan, hogy a szolgáltatást és a szolgáltatót a felhőszolgáltatás kapcsán ért biztonsági incidensekről késedelem nélkül tájékoztatást nyújtson;

o) támogatás és adatok biztosítása a pénzügyi szervezetnél előfordult visszaélések felderítéséhez.

III.4. A felhőszolgáltatás bevezetése

19. A pénzügyi szervezet meghatározza a szolgáltatás bevezetéséhez kapcsolódó fejlesztések, tesztelések és az átállás követelményeit, továbbá az éles bevezetés és a szolgáltatás elfogadási kritériumait.

20. A pénzügyi szervezet, a IV. fejezetben foglaltakra figyelemmel, gondoskodik legalább az alábbiak teljesítéséről, amennyiben az az adott felhőszolgáltatás-bevezetési projekt kapcsán értelmezhető.

III.4.1. A bevezetés előkészítése

21. A pénzügyi szervezet a bevezetés előkészítése során végrehajtja a következő lépéseket:

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, továbbá a szolgáltatás elfogadási kritériumait;

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 szolgáltatás-specifikációt, 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.4.2. A bevezetés végrehajtása

22. A pénzügyi szervezet a bevezetés végrehajtása során végrehajtja a következő lépéseket:

a) Implementálja a migrációs eszközöket.

b) elemi lépésekre lebontott ütemtervet készít mérföldkövek, és erőforrások definiálásával, felelősök kijelölésével, mely legyen felkészítve egy negatív, pesszimista forgatókönyv (worst case scenario) 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 az elfogadási kritériumok alapján, a migrált adatok helyességét ellenőrzi. Amennyiben a migráció a pénzügyi szervezet kockázatelemzése alapján kritikus funkciót vagy rendszert érint, akkor a migrációt független és a szükséges kompetenciával rendelkező féllel validáltatja a teljes körűség, a sértetlenség és a bizalmasság szempontjai szerint.

III.5. Üzemeltetés

23. A pénzügyi szervezet saját maga alkalmazza, illetve a szolgáltatóval betartatja a IV. fejezetben megfogalmazott követelményeket a felhőszolgáltatásra támaszkodó működés során, különös tekintettel az alábbiakra:

a) a szolgáltatás megfelelő felügyelete és ellenőrzése;

b) hatékony és összehangolt incidenskezelési folyamat kialakítása, működtetése a pénzügyi szervezet és a szolgáltatója között;

c) rendszeres katasztrófa utáni helyreállítási (DR) tesztek;

d) a szolgáltató pénzügyi helyzetének és az SLA-k teljesítésének nyomon követése;

e) felkészülés a hibás teljesítés esetére, alternatív felhőszolgáltatók vagy más megoldások felmérése az üzletmenet-folytonosság biztosítására;

f) kockázatelemzés alapján meghatározott események naplózásának és a naplók sértetlenségének biztosítása, a naplók elemzése;

g) a felhőszolgáltatás kockázatelemzésének rendszeres frissítése;

h) kivezetési stratégia és akcióterv rendszeres frissítése;

i) csak hivatalosan kiadott, letesztelt, támogatott, a vonatkozó hazai és uniós elvárásoknak megfelelő szolgáltatás-verziók és adatközpont helyszínek igénybevétele.

III.6. Kivezetés

24. A pénzügyi szervezet a felhőszolgáltatás kivezetési fázisában végrehajtja a 14. pontban meghatározott kivezetési stratégiában és akciótervben foglaltakat.

III.6.1. A kivezetés előkészítése

25. A pénzügyi szervezet 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 (worst case scenario) kidolgozásával;

e) a szolgáltatás kivezetésében érintettek együttműködésének, feladatainak, felelősségeinek rögzítettségét;

f) a kivezetés alatt a szolgáltatás nyújtásának és adatok elérhetőségének, átadásának ütemezését, feltételeit.

III.6.2. A kivezetés végrehajtása

26. A pénzügyi szervezet a kivezetés során gondoskodik a kivezetési stratégiában és akciótervben foglalt, alábbi lépések végrehajtásáról:

a) migrációs eszközök telepítése;

b) visszatöltés tesztelésének végrehajtása tesztkörnyezetben;

c) éles adat-visszatöltés, a szolgáltatás-visszavétel végrehajtása a forgatókönyvek alapján;

d) validáció az elfogadási kritériumok alapján, a visszavett adatok helyességének ellenőrzése, és a migráció lezárása;

e) utógondozás biztosítása a migráció utáni javítások elvégzésére;

f) sikeres kivezetést követően a szerződésben meghatározott feltételek alapján a szolgáltató adattörlése, amely kiterjed a szolgáltató éles, tartalék és esetleges mentési és archiválási környezetére is; az adatok törlésének végrehajtásáról szolgáltatói bizonyosságnyújtás (nyilatkozat) szükséges;

g) a szükségtelenné vált informatikai, kommunikációs kapcsolatok megszüntetése a szolgáltatóval.

IV. Felhőszolgáltatás-biztonsági alapelvek

27. A pénzügyi szervezet betartja a következőkben ismertetett felhőszolgáltatás-biztonsági alapelveket és a megvalósítás lépéseit, illetve bizonyosságot szerez a szolgáltató hatáskörébe eső kitételek betartásáról, a 11-17. pontban foglaltaknak megfelelően.

IV.1. Adatbiztonság és adatvédelem

28. Az adatbiztonság és adatvédelem megvalósításának előfeltételeként a pénzügyi szervezet elvégzi a következőket:

a) azonosítja és biztonsági osztályba sorolja a felhőszolgáltatásba kiszervezni tervezett adatokat, a jogszabályoknak és saját adatvédelmi szabályzatának megfelelően;

b) meghatározza az adatbiztonsági és az adatvédelmi követelményeket a biztonsági osztályba sorolás szerint, a releváns szabályozás alapján.

29. A pénzügyi szervezet a technikai adatbiztonsági és adatvédelmi követelmények meghatározásakor és alkalmazásakor 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.

30. A pénzügyi szervezet 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. A pénzügyi szervezet a bizonyosságszerzés során támaszkodik független harmadik felek ellenőrzésére vagy tanúsítására.

31. A pénzügyi szervezet felel az adatok továbbítása és tárolása során azok sértetlenségéért, bizalmasságáért és rendelkezésre állásáért.

32. Az adatvédelem terén a pénzügyi szervezet biztosítja a személyes adatok és az ügyfélre vonatkozó, a pénzügyi ágazati törvények által védett titoknak minősülő adatok biztonságos kezelését és feldolgozását, figyelemmel a mindenkor hatályos adatvédelmi szabályozásnak[6] való megfelelésre.

IV.1.1. Az adatok biztonsága továbbítás közben

33. A pénzügyi szervezet „az adatok biztonsága továbbítás közben" alapelv teljesülése érdekében gondoskodik a pénzügyi szervezet és a felhő közti, a felhőben levő erőforrások közti, valamint a felhő és más külső szolgáltatók közti adatforgalom védelméről az illetéktelen megismerés és módosítás ellen, továbbá a hálózati kapcsolatok rendelkezésre állásáról és elvárt adatátviteli sebességükről.

34. A 33. pontban foglalt alapelv érvényesülése érdekében a pénzügyi szervezet és a felhőszolgáltató az alkalmazott felhőszolgáltatási modell függvényében gondoskodik a hatáskörükbe tartozó rendszerelemek vonatkozásában a következőkről:

    a) biztosítják a szolgáltatás adatforgalmának titkosítását és integritásvédelmét. Ezzel összefüggésben a pénzügyi 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; a privilegizált felhasználókat többfaktoros autentikációval azonosítják;
    c) biztosítják a hálózati kapcsolatok magas rendelkezésre állását és az üzemszerű működéshez szükséges hálózati sávszélességeket.

35. A 33-34. pontban leírtak vonatkoznak a szolgáltatás- és rendszer-menedzsment folyamatok által generált adatforgalomra is.

36. Amennyiben a felhőt érintő adatfeltöltés vagy -letöltés nem csak hálózaton keresztül valósul meg, úgy a felhasznált fizikai adathordozókra is alkalmazzák a 33-34. pontban felsorolt, bizalmasságot és sértetlenséget biztosító kontrollokat.

IV.1.2. A tárolt adatok biztonsága

37. A pénzügyi szervezet „a tárolt adatok biztonsága" alapelv teljesülése érdekében gondoskodik a felhőben tárolt adatok rendelkezésre állásáról, illetve az adatok védelméről az illetéktelen megismerés és módosítás ellen.

[6] Lásd az 1. melléklet 2. pontjában hivatkozott jogszabályokat.

38. A 37. pontban foglalt alapelv érvényesülése érdekében a pénzügyi szervezet és a felhőszolgáltató az alkalmazott felhőszolgáltatási modell függvényében gondoskodik 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[7]);

    c) meghatározzák a tárolt adatok biztonságos törlését, beleértve a mentések és archívumok törlését is, 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 a pénzügyi szervezet gondoskodik az adatmentések felhőszolgáltatótól független tárolásáról is; a függetlenül tárolt mentések rendszerességét a kockázatok és jogszabályi elvárások figyelembevételével határozza meg.

IV.1.3. Adatvédelem

39. A pénzügyi szervezet az adatvédelem alapelv teljesülése érdekében meggyőződik a rá irányadó adatvédelmi jogszabályok és előírások felhőszolgáltató általi betartásáról.

40. A 39. pontban foglalt alapelv érvényesülése érdekében a pénzügyi szervezet

    a) feltárja a különbségeket egyrészt a pénzügyi szervezetre 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, vagy az adatkezelés alanya mikor, milyen feltételekkel férhet hozzá az adatokhoz és kockázat azonosítása esetén mérlegelése szerint nem járul hozzá az alvállalkozó vagy egyéb harmadik személy igénybevételéhez azzal, hogy az alvállalkozók felmérése nem jelent a pénzügyi szervezet oldalán az ellenőrzési jog eredeti célján túlterjeszkedő jogosultságot;

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

[7] Az adatvesztés megengedett időtartama

41. A pénzügyi szervezet saját felelősségi körében meghozandó, az adatok védelmére irányuló intézkedéseiről az 1. melléklet 2.2., illetve 2.3. pontjában felsorolt jogszabályokon, uniós jogi aktusokon, illetve MNB ajánlásokon kívül a Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: NAIH) ajánlásai[8] rendelkeznek.

IV.2. Erőforrások védelme

42. A pénzügyi szervezet „az erőforrások védelme" alapelv teljesülése érdekében meggyőződik a felhőben allokált erőforrásainak (feldolgozó és tároló kapacitásainak) illetéktelen fizikai vagy logikai hozzáférés, sérülés és eltulajdonítás elleni védelméről.

43. A 42. pontban foglalt alapelv érvényesülése érdekében a pénzügyi szervezet

    a) magas szintű bizonyosságot szerez a felhőszolgáltató adatközpontjainak, számítástechnikai, kommunikációs eszközeinek védelméről, a magas 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;

        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 használatára;

        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) használatára.

IV.3. Informatikai folyamatok biztonsága

44. A pénzügyi szervezet „az informatikai folyamatok biztonsága" alapelv teljesülése érdekében a felhőszolgáltatás adatbiztonságát, adatvédelmét, valamint az erőforrások védelmét – végső soron a felhőszolgáltatás biztonságát – szabályozott, biztonságos és ellenőrzött informatikai irányítási rendszerrel és folyamatokkal valósítja meg.

[8] A NAIH ajánlásai elérhetőek: https://www.naih.hu/ajanlasok.html

IV.3.1. Biztonságmenedzsment

45. A 44. pontban foglalt alapelv érvényesülése érdekében a pénzügyi szervezet a biztonságmenedzsment terén

a) bizonyosságot szerez a szolgáltató információbiztonság-irányítási rendszeréről, folyamatairól, és ezek kontrolljainak működéséről, legalább az alábbi hatókörben:

aa) információbiztonság-irányítási (ISMS) rendszer és annak az ISMS releváns nemzetközi szabvány szerinti tanúsítása;

ab) az információbiztonsági szervezet struktúrája, szerepkörök szétválasztása;

ac) az információbiztonsági kockázatkezelési rendszer, beleértve a humánkockázat kezelését is: a pénzügyi szervezet elvárja a szolgáltató munkavállalóira, alvállalkozóira és közreműködőire vonatkozó humánkockázati szűrést, továbbá rendszeres információbiztonsági tudatossági oktatást;

ad) a belső és külső biztonsági ellenőrzési funkciók működése és eredményei: a pénzügyi szervezet elvárja az általános biztonsági vizsgálatokat, sérülékenység-vizsgálatokat, betörési teszteket, nemzetközi biztonsági szabványok szerinti tanúsításokat;

ae) az üzletmenet-folytonosság kezelése, magas rendelkezésre állás biztosítása, mentési rendszer és katasztrófahelyzet esetén a visszaállást támogató megoldások: a pénzügyi szervezet elvárja a BCP/DRP tervek rendszeres tesztelését és a tervek rendszeres frissítését;

af) konfigurációkezelési rendszerek naprakészen tartása, a felfedezett biztonsági sérülékenységek kijavításának gyors és hatásos folyamata, és az erről való tájékoztatás;

ag) biztonságos architektúra tervezés, a legjobb gyakorlatnak megfelelő hálózatbiztonsági kontrollok;

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

ai) biztonsági naplózás és monitorozás: a pénzügyi szervezet 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 a pénzügyi szervezettel;

aj) biztonsági incidensek kezelése, értesítési rendszere: a pénzügyi szervezet elvárja a rá hatással levő biztonsági incidensekről és megoldásukról való késedelem nélküli értesítést;

ak) visszaélés-felderítési vizsgálatok: a pénzügyi szervezet elvárja az ilyen vizsgálatok elvégzésének szolgáltató általi támogatását, és a folyamat szabályozását;

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

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

b) a pénzügyi szervezet 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 DR tesztelés, biztonsági fórumban való részvétel);

c) a pénzügyi szervezet igénybe veszi a szolgáltató által esetlegesen működtetett kiterjesztett hatókörű értesítési rendszert a biztonsági incidensekről, amely a pénzügyi szervezetet közvetlenül érintő incidenseken túlmenően kiterjed azon eseményekre is, melyek magát a szolgáltatót vagy más ügyfeleit érintik, valamint a sikertelen (DRP és biztonsági) tesztelésekre is, mivel mindezek közvetlen, vagy közvetett fenyegetést jelenthetnek az intézményre.

IV.3.2. Üzemeltetés biztonsága

46. A 44. pontban foglalt alapelv érvényesülése érdekében a pénzügyi szervezet az üzemeltetés biztonsága terén

a) bizonyosságot szerez a szolgáltató informatikai üzemeltetési folyamatainak kontrollállt működéséről, legalább az alábbi hatókörben:

   aa) üzemeltetési eljárások és felelősségek meghatározása, dokumentálása;

   ab) mentési és visszatöltési eljárások;

   ac) üzemeltetési felügyelet (monitorozás) és naplózás;

   ad) eszközkezelés (eszközök azonosítása, nyilvántartása és kezelése azok teljes életciklusán keresztül);

   ae) változtatás- és verziókezelés, konfigurációmenedzsment;

   af) incidens-, probléma-, és igénykezelés, valamint az ezekhez kapcsolódó értesítési eljárások;

   ag) SLA-k elvárásai, kezelése, monitorozása, jelentése.

IV.3.3. Fejlesztés biztonsága

47. A 44. pontban foglalt alapelv érvényesülése érdekében a pénzügyi szervezet a fejlesztés biztonsága terén

a) bizonyosságot szerez a szolgáltatást érintő fejlesztési folyamatok kontrollállt működéséről, legalább az alábbi hatókörben:

   aa) dokumentált fejlesztési irányelvek, módszertanok alkalmazása, különös tekintettel a biztonságos fejlesztési módszerekre és gyakorlatokra;

   ab) biztonsági elvárások dokumentálása és beépítése a fejlesztésekbe;

   ac) fejlesztési és tesztelési környezetek kialakítása, szeparáltságuk biztosítása;

   ad) biztonsági és betörési tesztek alkalmazása az éles üzembe helyezést megelőzően, majd az üzembe helyezést követően legalább éves rendszerességgel;

   ae) alvállalkozók fejlesztéseinek minőségbiztosítása és kontrollja.

IV.4. Felhasználó- és jogosultságkezelés[9]

48. A pénzügyi szervezet a felhasználó-és jogosultságkezelés alapelv teljesülése érdekében gondoskodik a felhőszolgáltatáshoz való hozzáférések szükséges és elégséges szintre korlátozásáról, az üzleti igényekkel összhangban, megfelelő azonosítási, hitelesítési (autentikációs) és jogosultsági (autorizációs) megoldások használatával.

49. A 48. pontban foglalt alapelv érvényesülése érdekében a pénzügyi szervezet és a felhőszolgáltató az alkalmazott felhőszolgáltatási modell függvényében gondoskodik a hatáskörükbe tartozó rendszerelemek vonatkozásában a következőkről:

    a) a pénzügyi szervezet 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 kiemelt (privilegizált) felhasználókat többfaktoros autentikációval azonosítják, a szolgáltatással összefüggő tevékenységüket naplózzák, a naplókat pedig rendszeresen ellenőrzik, és az ellenőrzést a pénzügyi szervezet számára is biztosítják;
    c) a pénzügyi szervezet meghatározza a felhőszolgáltatással kapcsolatos összeférhetetlen szerepköröket és jogosultságokat;
    d) a pénzügyi szervezet teljes körű, naprakész, a beállításokkal összevethető nyilvántartással rendelkezik az engedélyezett felhasználókról és jogosultságaikról, beleértve a kiemelt (privilegizált), a technikai, és a külső/távoli felhasználókat is;
    e) a felhasználó- és jogosultságkezelést végzők tevékenysége rendszeresen ellenőrzött (ki mikor mit igényelt, engedélyezett, állított be, vizsgált felül, vont vissza).

V. Felügyeleti ellenőrzések

50. Az MNB a pénzügyi szervezetnél és rajta keresztül a szolgáltatónál is ellenőrizheti a felhőszolgáltatás kontrollkörnyezetét. A pénzügyi szervezet a szolgáltatás szerződéses feltételeivel köteles biztosítani, hogy az MNB a felhőszolgáltatás vizsgálata során helyszíni vagy helyszínen kívüli vizsgálatot végezhessen a szolgáltatónál (a kiszervezett tevékenységet végzőnél) is.

51. A felhőszolgáltatás vizsgálatának elsődleges célja megállapítani, hogy

    a) biztosított-e a pénzügyi szervezet zavartalan működéséhez és az üzleti célok teljesítéséhez szükséges informatikai megoldás, illetve ennek folyamatos működtetéséhez és továbbfejlesztéséhez a feltételek rendelkezésre állnak-e;
    b) a pénzügyi szervezet 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) a pénzügyi szervezet és a szolgáltató (a kiszervezett tevékenységet végző) betartja-e a vonatkozó jogszabályokat a felhőszolgáltatás igénybevétele során.

[9] Ez a pont a pénzügyi szervezet érdekkörébe tartozó felhasználók és jogosultságaik kezelésére vonatkozó követelményeket rögzíti. A felhőszolgáltató érdekkörébe tartozó felhasználók és jogosultságaik kezelésére vonatkozó követelmények a 45. a) ah). pontban találhatók.

52. Az 51. pontban meghatározott célok teljesítése érdekében a vizsgálat, figyelemmel a jelen ajánlásra, hangsúlyt helyez a következők ellenőrzésére:
    a) a döntés-előkészítés anyagai, különösen a költség-haszon elemzés, követelménylisták;
    b) a kockázatelemzés és a kockázatcsökkentő intézkedések;
    c) a szolgáltatás-kivezetési stratégia és akcióterv;
    d) a felhőszolgáltatásról szóló szerződés(ek) és kiegészítései(k);
    e) az informatikai biztonság 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

53. Az ajánlás a 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.
54. 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.
55. 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 ajánlásnak. 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.
56. Az MNB a jelen ajánlás alkalmazását 2017. március 1-től várja el az érintett pénzügyi szervezetektől.
57. Az MNB a Pénzügyi Szervezetek Állami Felügyelete által pénzügyi szervezeteknél a közösségi és publikus felhőszolgáltatás igénybevételéből eredő kockázatokról kiadott 4/2012. vezetői körlevelet 2017. március 1-jei hatállyal visszavonja.

Dr. Matolcsy György sk.
a Magyar Nemzeti Bank elnöke

Kapcsolódó jogszabályok és MNB ajánlások

1. Pénzügyi ágazati jogszabályok és uniós jogi aktusok

1.1. az Önkéntes Kölcsönös Biztosító Pénztárakról szóló 1993. évi XCVI. törvény [az informatikai rendszer védelmére és a kiszervezésre vonatkozó rendelkezések: 40/C.-40/D. §];

1.2. a magánnyugdíjról és a magánnyugdíjpénztárakról szóló 1997. évi LXXXII. törvény [az informatikai rendszer védelmére és a kiszervezésre vonatkozó rendelkezések: 77/A. és 77/B §];

1.3. a tőkepiacról szóló 2001. évi CXX. törvény [a tőzsdei tevékenységet érintően a kiszervezésre és az informatikai rendszer védelmére és vonatkozó rendelkezések: 318/A-318/D. §];

1.4. a befektetési vállalkozásokról és az árutőzsdei szolgáltatókról, valamint az általuk végezhető tevékenységek szabályairól szóló 2007. évi CXXXVIII. törvény [az informatikai rendszer védelmére és a kiszervezésre vonatkozó rendelkezések: 12. §, 79-81. §];

1.5. az egyes fizetési szolgáltatókról szóló 2013. évi CCXXXV. törvény [az informatikai rendszer védelmére és a kiszervezésre vonatkozó rendelkezések: 12/A. és 14. §];

1.6. a hitelintézetekről és a pénzügyi vállalkozásokról szóló 2013. évi CCXXXVII. törvény [az informatikai rendszerre és a kiszervezésre vonatkozó rendelkezések: 67/A. és 68. §];

1.7. a kollektív befektetési formákról és kezelőikről, valamint egyes pénzügyi tárgyú törvények módosításáról szóló 2014. évi XVI. törvény [ÁÉKBV-alapkezelőre, illetve ABAK-ra vonatkozó kiszervezési szabályok: 39-42. §];

1.8. a biztosítási tevékenységről szóló 2014. évi LXXXVIII. törvény [a kiszervezésre vonatkozó rendelkezések: 90-92. §];

1.9. 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;

1.10. 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 [kiszervezésre vonatkozó rendelkezések: 274. cikk].

2. Adatvédelmi, információbiztonsági jogszabályok, uniós jogi aktusok

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

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) (a rendeletet 2018. május 25-től kell alkalmazni).

3. MNB ajánlások

3.1. az informatikai rendszer védelméről szóló 1/2015. MNB ajánlás;

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

Tartalomjegyzék

I. Az ajánlás célja és hatálya 1
II. A felhőszolgáltatások meghatározása 1
III. A felhőszolgáltatások igénybevételének életciklusa 2
III.1. Üzleti igény felmerülése, döntés-előkészítés, tervezés 3
III.1.1. Jogszabályi megfelelés biztosítása 3
III.1.2. Költség-haszon elemzés 3
III.2. A felhőszolgáltatás kockázatelemzése 4
III.2.1. A kivezetés kockázatai 4
III.2.2. Bizonyosságszerzés 4
III.3. Szerződéses követelmények 5
III.4. A felhőszolgáltatás bevezetése 6
III.4.1. A bevezetés előkészítése 6
III.4.2. A bevezetés végrehajtása 6
III.5. Üzemeltetés 7
III.6. Kivezetés 7
III.6.1. A kivezetés előkészítése 7
III.6.2. A kivezetés végrehajtása 8
IV. Felhőszolgáltatás-biztonsági alapelvek 8
IV.1. Adatbiztonság és adatvédelem 8
IV.1.1. Az adatok biztonsága továbbítás közben 9
IV.1.2. A tárolt adatok biztonsága 9
IV.1.3. Adatvédelem 10
IV.2. Erőforrások védelme 11
IV.3. Informatikai folyamatok biztonsága 11
IV.3.1. Biztonságmenedzsment 12
IV.3.2. Üzemeltetés biztonsága 13
IV.3.3. Fejlesztés biztonsága 13
IV.4. Felhasználó- és jogosultságkezelés 14
V. Felügyeleti ellenőrzések 14
VI. Záró rendelkezések 15
1. melléklet a …/2017. (… …) számú MNB ajánláshoz 16