PRUDENCIÁLIS MODELLEZÉSI ÉS IT FELÜGYELETI IGAZGATÓSÁG

Gyakori kérdések és válaszok felhőszolgáltatások igénybevételével kapcsolatban (GYIK)

1. Konzultáció

1.1. Van-e lehetőség a Felügyelettel konzultálni felhőszolgáltatások igénybevételével kapcsolatban?

Igen, van lehetőség a Felügyelettel konzultálni, melyet az Intézmény az MNB kijelölt intézményi felügyelőjén vagy az Informatikai felügyelet honlapján[1] keresztül kezdeményezhet. Felügyelt intézmény innovatív pénzügyi megoldásával kapcsolatos komplex, több felügyeleti szakterület bevonását igénylő esetben, továbbá olyan innovatív megoldások esetén, amikor a FinTech innovátor még nem rendelkezik felügyeleti engedéllyel, az MNB Innovation Hub (Pénzügyi Innovációs Platform, https://www.mnb.hu/innovation-hub) platformon keresztül van lehetőség felhőszolgáltatások igénybevételével kapcsolatos szabályozói támogatás kérésére. Az MNB Innovation Hub-bal a platformon elérhető kérdőív[2] kitöltésével lehet kapcsolatba lépni.

1.2. Milyen esetben indokolt a Felügyeleti konzultáció?

A konzultáció nem kötelező, de javasolt, hogy az Intézmények nagy horderejű, kritikus funkciókat érintő felhő kiszervezés esetén konzultáljanak az MNB-vel, illetve szükség esetén kérjenek állásfoglalást felhőszolgáltatások igénybevétele kapcsán.

2. Szabályozás

2.1. Mi szabályozza a felhőszolgáltatások igénybevételét?

A pénzügyi szektorra vonatkozó információbiztonsági követelményeket jellemzően 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, illetve a vonatkozó ágazati jogszabályok szabályozzák.
A felhőszolgáltatások igénybevételét specifikusan a közösségi és publikus felhőszolgáltatások igénybevételéről szóló (jelenleg) 4/2019. (IV.1.) MNB ajánlás[3] (Felhő ajánlás), az informatikai rendszer védelméről szóló (jelenleg) 8/2020. (VI.22.) MNB ajánlás[4] (Informatikai rendszer védelméről szóló ajánlás), az EBA[5] iránymutatása a kiszervezésről (jelenleg: EBA/GL/2019/02), az EIOPA[6] iránymutatásai a

[1] https://www.mnb.hu/felugyelet/szabalyozas/informatikai-felugyelet

[2] https://mnbpoll.mnb.hu/Survey.aspx?surveyid=70754442&lng=hu-HU

[3] https://www.mnb.hu/letoltes/4-2019-felho.pdf

[4] https://www.mnb.hu/letoltes/8-2020-informatikai-rendsz-vedelmerol.pdf

[5] Európai Bankhatóság

[6] Európai Biztosítás- és Foglalkoztatóinyugdíj-hatóság

felhőszolgáltatókhoz történő kiszervezésről (jelenleg: EIOPA-BoS-20-002), illetve az ESMA[7] előkészítés alatt álló felhő iránymutatásai szabályozzák. A külső szolgáltatások igénybevételét a külső szolgáltatók igénybevételéről szóló (jelenleg) 7/2020. (VI.3.) MNB ajánlás rögzíti. A további kapcsolódó jogszabályokat, ajánlásokat, iránymutatásokat az MNB felhő ajánlása meghatározza.

3. Fogalmak

3.1. Mi határozza meg, hogy egy vállalatcsoportnál a felhőszolgáltatási modell magán- vagy közösségi felhőnek minősül?

Ha a szolgáltatás megfelel a felhőszolgáltatás ismérveinek, de az Intézmény irányítása alatt áll a felhőszolgáltatást nyújtó informatikai infrastruktúra, és a szolgáltatást csak az Intézmény használja, akkor magánfelhő (private cloud). Ha kizárólag közösséget alkotó jogi személyek használják az adott felhőszolgáltatást, mint például a vállalatcsoporton belüli felhőszolgáltatás esetében, az közösségi felhő (community cloud). Amennyiben egy vállalatcsoport közösen használ egy publikus felhőszolgáltatást, az publikus felhőnek (public cloud) minősül.

3.2. Mit jelent a magánfelhő (private cloud)?

A magánfelhő lényege, hogy minden számítástechnikai berendezés és szoftver az adott felhasználó szervezet irányítása alatt áll, tehát kizárólagosan saját használatú a hardver, a szoftver, az egész infrastruktúra és természetesen a rendelkezésre állással kapcsolatos felelősség is. Tehát ezeket az erőforrásokat a szervezet nem osztja meg külsősökkel, csak a felhasználó szervezet keretein belül hozzáférhetők.

3.3. Magánfelhőnek minősül-e a „menedzselt magánfelhő”?

Alapesetben nem. A „menedzselt magánfelhő” kifejezést az ajánlás nem használja, értelmezése és használata a szakmában változó, ellentmondásos. Egy elterjedt értelmezése alapján a menedzselt felhőszolgáltatás az ügyfél adatközpontjában és fizikai eszközein valósul meg, de a felhőinfrastruktúra működtetését, üzemeltetését egy szolgáltató biztosítja. Más értelmezés alapján a szolgáltató a saját felhőinfrastruktúráján belül az Intézmény számára az Intézmény kizárólagos használatára elkülönített eszközök felhasználásával nyújt felhőszolgáltatást. Az MNB álláspontja alapján egy felhőszolgáltatás csak abban az esetben minősülhet magánfelhőnek, ha az Intézménynek nyújtott szolgáltatásokat kiszolgáló informatikai infrastruktúrában hardverszintű elkülönítés valósul meg. Amennyiben ez megvalósul, abban az esetben is szükséges a kiszervezésre vonatkozó előírásokat érvényesíteni.

3.4. Magánfelhőnek minősül-e a kizárólag a vállalatcsoport tagjai által, közösen használt felhő?

Nem, ez közösségi felhőnek minősül. Részletesen lásd a 3.1. kérdésben.

[7] Európai Értékpapír-piaci Hatóság

4. A felhő ajánlás hatálya

4.1. Ügynöki tevékenység keretében végzett tevékenység során igénybe vett felhőszolgáltatás az ajánlás hatálya alá tartozik-e?

Amennyiben az ügynöki tevékenység keretében ügyfelek – ide értve az ügynök ügyfeleit is – adatainak kezelése felhőszolgáltatás igénybevételéve valósul meg, akkor az is a Felhő ajánlás hatálya alá tartozik. A Felhő ajánlást azokban az esetekben is szükséges figyelembe venni, ha nem kiszervezési szerződés keretében történik a felhőszolgáltatás igénybevétele.

5. Megfelelés

5.1. Ha egy felhőszolgáltatás megfelel az EBA/EIOPA/ESMA előírásainak, akkor szükséges-e az MNB ajánlásnak való megfelelés biztosítása is?

Az MNB felhő ajánlása tartalmazza az EBA/EIOPA/ESMA felhő irányelveiben foglalt követelményeket, azonban ezen irányelveken túlmenően is határoz meg információbiztonsági követelményeket, a szolgáltatás teljes életciklusára kiterjedő módon, a magyar jogszabályi környezetet is figyelembe véve. Ebből adódóan az MNB felhő ajánlásnak való megfelelés biztosítása is szükséges.

5.2. Melyek a Felügyelet által elfogadott felhőszolgáltatási modellek, megoldások, szolgáltatók?

A Felügyelet szállító- és technológia semlegesen határozta meg elvárásait, mivel a Felügyelet számára a felhőszolgáltatások igénybevétele kapcsán az adatok megfelelő védelme, a transzparencia, a felmerülő kockázatok megfelelő kezelése, a kontrollintézkedések megfelelősége és a jogszabályi kötelezettségek teljesítése a legfontosabb szempont.

5.3. Kiterjed-e a közösségi és publikus felhőszolgáltatások igénybevételéről szóló 4/2019. (IV.1.) MNB ajánlás hatálya az ideiglenes jelleggel igénybe vett felhőszolgáltatásokra?

Az ajánlást akkor is figyelembe kell venni, ha a szolgáltatást az Intézmény csak meghatározott ideig (pl. jelentős számításigényű műveletek ideiglenes támogatása céljából) veszi igénybe. Egy ilyen szolgáltatás esetében is megvalósul a felhőszolgáltatásokra jellemző teljes életciklus, így valamennyi, az ajánlásban meghatározott elvárásnak teljesülnie szükséges (beleértve a nyilvántartásra és az MNB tájékoztatására vonatkozó ajánlást is).

5.4. A Nemzeti Kibervédelmi Intézet által bejelentés-köteles szolgáltatóként nyilvántartásba vett, felhőalapú számítástechnikai szolgáltatások esetében szükséges-e az MNB ajánlásnak való megfelelés biztosítása is?

Igen, amennyiben az érintett Intézmény, szervezet, személy vagy tevékenység a Magyar Nemzeti Bankról szóló 2013. évi CXXXIX. törvény 39. §-ában meghatározott jogszabályok hatálya alá tartozik.

5.5. Milyen szolgáltatások szervezhetők ki a felhőbe?

A kiszervezhető szolgáltatások terén az ágazati jogszabályok, továbbá a belső védelmi vonalak kialakításáról és működtetéséről, a pénzügyi szervezetek irányítási és kontroll funkcióiról szóló 27/2018 (XII.10.) MNB ajánlás, valamint a külső szolgáltatók igénybevételéről szóló 7/2020. (VI.3.) MNB ajánlás határozzák meg a

kereteket. Az általánosságban kiszervezhető szolgáltatások – a kockázatok megfelelő kezelése esetén – a felhőbe is kiszervezhetők. Abban az esetben is szükséges a Felhő ajánlást betartani, ha a kiszervezett tevékenységet végző szolgáltató vesz igénybe felhőszolgáltatást közreműködőként.

5.6. Milyen kockázatelemzési módszertan elfogadott a felhőszolgáltatás igénybevétele esetén?

Nincs konkrét elfogadott kockázatelemzési módszertan a felhőszolgáltatás igénybevételére vonatkozóan, azonban a kockázatelemzésnek a vonatkozó ágazati jogszabályokat, a Felhő ajánlás és az Informatikai rendszer védelméről szóló ajánlás követelményeit kimutathatóan teljesítenie kell.

5.7. A szerződéses követelmények meghatározása során mire kell tekintettel lenni?

A szerződés fedje le a szolgáltatás igénybevételének életciklusát és az ennek során felmerülő kockázatokat. Előfordulhat, hogy a szolgáltató szerződései nem elég rugalmasak az Intézmény igényeinek és a vonatkozó szabályozási környezetnek történő megfelelésre. Érdemes a szolgáltatók pénzügyi ágazati szolgáltatáscsomagját igénybe venni. A szerződéses feltételek terén javasolt kitérni legalább a következőkre:

- felmondási feltételekre, felmondási idő szabályozására;
- feltétel nélküli ellenőrzési jogra;
- adatkezelési és -feldolgozási helyszínekre;
- adatbiztonsági és adatvédelmi elvárásokra – a szolgáltatási láncra kiterjedően is;
- folyamatok és rendszerek biztonsági elvárásaira;
- incidenskezelésre és csalásfelderítési (forensic) eljárásokra és az
- exit stratégiára.

A szerződéses követelményeket részletesen szabályozza a Felhő ajánlás, melyen túl szükséges figyelembe venni a kiszervezésre vonatkozó ágazati jogszabályokat, valamint az európai felügyeleti hatóságok felhő irányelveiben foglaltakat is.

5.8. Mi a jellemző jó gyakorlat az exit stratégia részletezettségére és dokumentálása vonatkozóan?

A felhőszolgáltatás igénybevételének megszüntetésére exit stratégiát és akciótervet is kell készíteni. Az exit stratégia tartalmazza a kilépés feltételeit, a végrehajtás időtávját, szerepeljenek benne a végrehajtás fő lépései és felelősei. Tartalmazza például, hogy az adatok kinyerése honnan, milyen csatornán, milyen eszközökkel, milyen szerkezetben történik, illetve milyen megoldással (saját üzemeltetésben, másik szolgáltatóval) biztosítják a továbbiakban a szolgáltatás működését. A terveknek ki kell terjednie a szolgáltatásból való nem tervezett kilépés lehetőségére is.
A kilépés feltételeit és költségeit a szolgáltatási szerződésben is szükséges rögzíteni.

6. Információbiztonság

6.1. Elegendő-e felhőszolgáltatás igénybevétele esetén az adatközponton belül megvalósított redundancia?

Nem, mivel ez a megoldás nem nyújt védelmet a potenciálisan egy adatközpont kiesésével járó kockázatokkal (például természeti csapások) szemben, illetve egy régiót érintő internetkapcsolat vagy tápáramellátás tartós kiesése esetén. A biztonsági mentések elhelyezése is olyan eltérő helyszíneken indokolt, melyeket ugyanazon kockázat nem érint, emiatt sem elégséges az ugyanazon adatközpontban történő elhelyezés. Lásd még a 8/2020.(VI.22.) MNB ajánlás 11.2.7. pontját.

6.2. Minden esetben szükséges a Felhőszolgáltatótól független mentést biztosítani?

A felhőszolgáltatótól független mentést[8] az érintett funkciók és adatok kritikusságának megfelelően és a kapcsolódó kockázatok figyelembevételével szükséges biztosítani. Ennek során részletesen meg kell határozni a független mentés szükségességét, mire terjedjen ki, milyen módszerrel és milyen gyakorisággal készüljön, tárolása hogyan és hol biztosított. A független mentés megvalósítható az Intézmény által vagy az elsődleges felhőszolgáltatótól független szolgáltató igénybevételével is – ebben az esetben a mentés tárolására igénybe vett felhőszolgáltatás is a Felhő ajánlás hatálya alá tartozik. Szoftverszolgáltatás, vagy ahhoz hasonló, felhőszolgáltató-specifikus szolgáltatás esetében is szükséges – a kockázatokkal arányosan – független mentés készítése, mely lehetővé teszi a szolgáltatás helyreállítását, az üzletmenet-folytonossági tervekkel és az exit stratégiával összhangban. Ennek a megvalósíthatóságát a szolgáltatás előzetes elemzése során, a szolgáltatás lényegességi értékelésével arányban kell értékelni.

7. Felelősség

7.1. Milyen teendője van az Intézménynek a felhőszolgáltató által ellátott feladatokkal kapcsolatban?

A felhőszolgáltatók a szolgáltatási modell függvényében szerződésben vállalják egyes szolgáltatási elemek biztosítását. Az Intézménynek a szerződéskötést megelőzően fel kell mérnie az ilyen, a felhőszolgáltatás körébe tartozó feladatok kockázatait, értékelnie kell a felhőszolgáltató kontrollintézkedéseit, és dokumentáltan döntést kell hoznia arról, hogy a kínált formában nyújtott szolgáltatást mi alapján, milyen feltételek teljesülése esetén tekinti elfogadható kockázatúnak. Értelemszerűen abban az esetben, ha a kockázatok nem kezelhetők megfelelően, a szerződéskötéstől indokolt tartózkodni.
A felhőszolgáltatás igénybevételének időszakában rendszeresen felül kell vizsgálnia, hogy a felhőszolgáltató megfelelően látja-e el a feladatait, és a felhőben működő szolgáltatás Intézményre gyakorolt működési kockázatai indokolnak-e javító intézkedéseket vagy a szerződés módosítását, megszüntetését. Jelentős incidens esetén ezt az elemzést soron kívül el kell végezni.
Más szolgáltatási területek esetén (pl. felhasználói adminisztráció) a felhőszolgáltató csak a feltételeket biztosítja ahhoz, hogy a szolgáltatás biztonságosan nyújtható legyen, de a tényleges beállításokat, adminisztrációt az Intézménynek kell elvégeznie.
A feladatok megoszlását szerződésben szükséges rögzíteni. Az ügyfeleknek nyújtott szolgáltatás működéséért, továbbá az ügyfelek adatainak és eszközeinek védelméért a végső felelősség vagy elszámoltathatóság – felhőszolgáltatás igénybevétele esetén is – az Intézményt terheli.

8. Adatvédelem

8.1. Bevonható-e a felhőszolgáltatásba Európai Gazdasági Térségen kívüli szolgáltató?

Biztosítani kell az ágazati jogszabályokon és a vonatkozó ajánlásokon, iránymutatásokon túl az adatvédelmi, információbiztonsági jogszabályoknak (például Általános adatvédelmi rendelet (GDPR)) való megfelelést, és az EGT-n[9] vagy EU-val ekvivalensként elfogadott adatvédelmű országokon kívüli országok esetén be kell tudni mutatni az illetékes hatóság felé, hogy milyen további adatvédelmi kockázatok merülnek fel a kiszervezésből adódóan, és hogy ezeket milyen intézkedésekkel kezelik. A felhőszolgáltatásban érintett

[8] olyan mentés, melyet nem az elsődleges felhőszolgáltató végez és tárol

[9] Európai Gazdasági Térség

adatok EGT-n kívüli helyszínre történő továbbítása a fentiek miatt külön elemzést és ellenőrzést igényel, melyeket szerződéses és technológiai garanciákkal is ki kell kényszeríteni.

9. Felhőszolgáltatások ellenőrzése

9.1. Melyek a független harmadik felek által a felhőszolgáltatásra vonatkozóan készített audit jelentések és tanúsítványok elfogadásának feltételei?

Az Intézménytől jogilag független harmadik felek által készített jelentések, tanúsítványok a kontrollok meglétén túl a kontrollok megfelelő működésére vonatkozóan is nyújtsanak bizonyosságot; a hatókör a nyújtott szolgáltatásra terjedjen ki teljes egészében (időszak, feldolgozási helyszínek, kontrollok, szolgáltatások, rendszerek stb.). Az ellenőrzést végzők rendelkezzenek olyan, a felhőszolgáltatások kapcsán releváns szakismerettel, amely az Intézmény elvárásainak megfelel. Az Intézmény tekinthessen bele a releváns ellenőrzési megállapításokba és bizonyítékokba, és legyen képes a megállapításokat és javaslatokat a saját kockázatkezelési keretrendszerére vonatkozóan értelmezni. Az esetlegesen feltárt kockázatok, hiányosságok kezelése történjen meg nyomon követhető módon. Több ügyfél közösen is ellenőrizheti csoportos auditok formájában a szolgáltatót. A felhőszolgáltatókat a Felügyelet nem felügyeli és nem minősíti, szükség esetén azonban élhet a kiszervezés esetére történő vizsgálati jogával. Amennyiben a felhőszolgáltatás igénybevétele kiszervezésként valósul meg, akkor a kiszervezés ellenőrzésére vonatkozó ágazati jogszabályi követelményeket is be kell tartani.

9.2. A Felügyelet milyen mértékben fogadja el a független audit jelentéseket vagy tanúsítványokat a felhőszolgáltatások kapcsán?

Az MNB a külső audit jelentéseket mérlegelése alapján figyelembe veheti, azok hatóköre, alaposság, megbízhatósága, függetlensége függvényében. Az Intézmény ellenőrzési folyamatainak kell rendelkezniük arról, hogy a független auditjelentéseket és tanúsítványokat milyen formában és feltételekkel fogadja el, és tudnia kell igazolni, hogy az Intézmény ellenőrzése által elfogadott jelentések megfelelnek ezeknek a feltételeknek, továbbá a jogszabályi és szabályozói elvárásoknak.

10. Felhőszolgáltatásnak minősülés, jelentési és adatszolgáltatási kötelezettség

10.1. Felhőszolgáltatásnak minősül-e, amennyiben egy kiszervezett szolgáltatás esetében a virtualizációs réteget, az operációsrendszert és az alkalmazást az intézmény üzemelteti, a storage-ot viszont a szolgáltató, és az ügyféladatok közötti elválasztás storage szinten megtörténik (ügyfelenként különböző volume-ok), de a storage azonos?

Ezen felosztás nem minősül sztenderd felhőmodellnek[10], majdnem tiszta hardver hostingnak tekinthető (ami nem felhőszolgáltatás). Ha a storage, volume kezelés felett nincs kontrollja az intézménynek, és az erőforrásokat nem tudja önkiszolgáló módon, dinamikusan kezelni, akkor a szolgáltatást kiszervezésként kell kezelni.
A felhőszolgáltatás ismérveinek[11] teljesülése esetén azonban felhőszolgáltatásnak kell a szolgáltatást tekinteni és ennek megfelelően kell a kiszervezésre vonatkozó követelmények, illetve a Felhő ajánlás szerint

[10] Infrastruktúra szolgáltatás (IaaS) esetén a mögöttes felhő infrastruktúrát nem az ügyfél menedzseli, de a storage felett van/lehet kontrollja.

[11] Lásd a Felhő ajánlás 1. pontját:

ellenőrizni, valamint meg kell győződni arról, hogy a szolgáltató megfelelően kezeli a storage-ot, konfigurációt, elválasztást.

10.2. Szükséges-e a videókonferenciát támogató alkalmazások (Zoom, MS Teams) bejelentése? Ha mondjuk az intézmény szolgáltatójával/partnereivel történik (csak) a kapcsolattartás (azaz nem ügyféllel), akkor ezt le kell-e jelenteni az MNB-nek (pl. negyedéves adatszolgáltatás keretében)?

Az intézmények kötelesek az igénybe vett felhőszolgáltatásokat teljeskörűen bejelenteni, melynek célja annak biztosítása, hogy az intézmények csak kellőképpen transzparens és kontrollált módon vegyenek igénybe felhőszolgáltatásokat, kizárva a felhőszolgáltatások ún. „shadow IT-ként" történő, nem biztonságos használatát. Fontos, hogy a Felhő ajánlás előírja az igénybe vett felhőszolgáltatások vonatkozásában kockázatelemzés elvégzését, melynek eredménye alapján, a kockázatoknak megfelelően szükséges a Felhő ajánlás által elvárt további intézkedéseket alkalmazni. A videókonferenciát támogató alkalmazások biztonságával kapcsolatos elvárások kapcsán lásd A távmunka és távoli hozzáférés informatikai biztonsági követelményeiről szóló 12/2020. (XI.6.) MNB ajánlás[12] „VII.4. Fax, telefon-, konferencia-, videókonferencia-hívások és egyéb kommunikációs csatornák biztonsága" fejezetét. Az alkalmazott szoftvereszközök jogtisztaságát biztosító elvárások tekintetében lásd Az informatikai rendszer védelméről szóló (jelenleg) 8/2020. (VI.22.) MNB ajánlás „5.3. Az alkalmazott szoftver eszközök jogtisztaságát bizonyító szerződések" pontját.

10.3. Pénzügyi vállalkozásokat tömörítő cégcsoport esetében szükséges bejelenteni a közösen használt belső hálózatot, és egyéb on premise szolgáltatásokat (pl. fájlszerver, AD, levelezés), mint felhőszolgáltatás?

Abban az esetben szükséges ezen szolgáltatásokat felhőszolgáltatásként bejelenteni, amennyiben a közösen használt szolgáltatásokat felhőszolgáltatás igénybe vételével valósítják meg. Ebben az esetben az MNB valamennyi, a felügyelete alá tartozó csoporttagtól elvárja a bejelentést. Amennyiben a közösen használt szolgáltatásokat nem felhőszolgáltatás igénybe vételével valósítják meg, de kiszervezésnek minősül, akkor csoporton belüli kiszervezésként szükséges bejelenteni.

10.4. A negyedéves adatszolgáltatási kötelezettség kapcsán pontosan miket kell az intézménynek benyújtania?

---

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 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).

[12] https://www.mnb.hu/letoltes/12-2020-tavmunka-ajanlas.pdf

A Magyar Nemzeti Bank elnökének hatályos, a pénz- és hitelpiaci szervezetek által a jegybanki információs rendszerhez elsődlegesen a Magyar Nemzeti Bank felügyeleti feladatai ellátása érdekében teljesítendő adatszolgáltatási kötelezettségekről szóló MNB rendelete[13] 4. § (1) bekezdésében foglaltak szerint: „A hitelintézet és a hitelintézeti típusú EGT-fióktelep – a (2) bekezdésben foglalt kivétellel – a 2. mellékletben foglaltaknak megfelelő tartalommal, formában, gyakorisággal és határidőre felügyeleti jelentést teljesít az MNB részére."
A jelenleg elvárt adattartalom:

- felhőszolgáltató neve;
- felhőszolgáltató székhelye;
- felhőszolgáltató adószáma;
- felhőszolgáltató anyavállalatának neve;
- felhőszolgáltató anyavállalatának székhelye;
- felhőszolgáltató anyavállalatának adószáma;
- felhőszolgáltatás igénybevételével érintett tevékenységek és adatok, adatkörök;
- nyújtott szolgáltatás helyszínéül szolgáló ország vagy országok (ideértve az adatok kezelési, feldolgozási és tárolási helyét);
- szolgáltatás kezdetének dátuma;
- szerződés hatályos változatának dátuma;
- következő szerződésmegújítási határidő (adott esetben);
- szerződés kapcsán irányadó jog.

A fenti adatokat minden egyes felhőszolgáltatásra – ismétlő soros rendszerben – ki kell tölteni, a szektorra vonatkozó adatszolgáltatás munkalapokon (Hitelintézetek: 9I; Pénzügyi vállalkozások: 29IT; Pénzforgalmi intézmények: 86I; Biztosítók: 42Q23; Befektetési vállalkozások: 37G, Alapkezelők: 50U; Pénztárak: 71OPI,71EPI, 71MPI,76NPI). Valamennyi adatszolgáltatáshoz tartozik kitöltési útmutató, amelyben a felhőszolgáltatásra egységesen (Pl.: 9I-re) a következők szerepelnek:
A 9I11 sor szerinti „felhőszolgáltatás" fogalmát, valamint a 9I11 sor alábontó soraiban kért információk magyarázatát a közösségi és publikus felhőszolgáltatások igénybevételéről szóló 4/2019. (IV. 1.) MNB ajánlás tartalmazza. Amennyiben az intézmény több felhőszolgáltatást vesz igénybe, akkor a válaszokat több blokk kitöltésével kell megadni.

11. Felhőszolgáltatás dokumentálása

11.1. Felhőszolgáltatással kapcsolatban milyen dokumentációkkal kell rendelkeznünk? (Felügyeleti vizsgálat során ezeket kéri az MNB)

A Magyar Nemzeti Bank 4/2019. (IV.1.) számú ajánlása (továbbiakban: Felhő ajánlás) a közösségi és publikus felhőszolgáltatások igénybevételéről 62. pontja összefoglalja a legfontosabb dokumentációs követelményeket, melyek jelenleg a következők:
„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;

[13] jelenleg 55/2021. (XI. 23.) MNB rendelet: https://www.mnb.hu/statisztika/informaciok-adatszolgaltatoknak/rendeletek-allasfoglalasok/55-2021-xi-23-mnb-rendelet

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."

További dokumentációs követelményeket ír elő a Felhő ajánlás 16. és 29. pontja a kiszervezésnek minősüléssel kapcsolatos felmérés és döntéshozatal, valamint a nyilvántartás kapcsán.

11.2. Amennyiben egy cégcsoport már régebben (2017 előtt) igénybe vett közösségi felhőszolgáltatást, szükséges-e utólag elkészíteni minden, a Felhő ajánlásban előírt dokumentumot? Továbbá tesztelés, pilotolás kapcsán milyen dokumentációs, bejelentési kötelezettsége van az intézménynek?

A Felhő ajánlásban előírt dokumentumok közül a kizárólag a felhőszolgáltatás igénybe vételére vonatkozó döntéshez szükséges dokumentumot, az előny-hátrány elemzést nem szükséges utólag elkészíteni. Ezt leszámítva szükséges és indokolt a Felhő ajánlásban előírt dokumentumokat utólag elkészíteni. A Felhő ajánlás 62. pontja összefoglalja a legfontosabb dokumentációs követelményeket, melyek jelenleg a következők:

„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."

Egyes előírásokat, melyek értelmezhetők a bevezetést követően is (pl. kockázatelemzés, kontrollok értékelése, szerződés megfelelőségének vizsgálata és kialakítása, lásd fent), azokat a kockázatelemzés során szükséges elvégezni.

Az intézmények iparági EU-s felügyeleti hatóságai szintén elvárják az irányelveikben előírtaknak való megfelelés biztosítását a már korábban igénybe vett felhőszolgáltatások esetén – az EBA 2021. december 31-ig, az EIOPA és ESMA 2022. december 31-ig –, ugyanakkor itt sem indokolt azon dokumentumok elkészítése, melyek kizárólag a felhőszolgáltatás igénybe vételére vonatkozó döntéshez szükségesek, indokoltak.

Tesztelés kapcsán nincs dokumentációs, bejelentési kötelezettsége az intézménynek, és pilotolás kapcsán sem, amennyiben nem használ érzékeny adatokat (üzleti titok, pénzügyi ágazati titok körébe tartozó adatok, személyes adatok), illetve nem támogat éles üzemi folyamatokat. Érzékeny adatok felhasználása vagy éles üzemi folyamatok esetén a Felhő ajánlásban előírtakat maradéktalanul alkalmazni kell. A teszteléssel kapcsolatos részletes követelményeket lásd Az informatikai rendszer védelméről szóló (jelenleg) 8/2020. (VI.22.) MNB ajánlás 4.4.8. pontjában. [14]

[14] 4.4.8. Az intézmény gondoskodik a megváltoztatott informatikai rendszerek, rendszerelemek, paraméterek éles üzembe állítását megelőző, dokumentált, elvárható gondosságú teszteléséről. A tesztelés során az intézmény gondoskodik a funkcionális és a nem funkcionális tesztek elvégzéséről, beleértve az informatikai biztonsági teszteket is.

Az MNB mindamellett a hatályos jogszabályoknak és ajánlásoknak való megfelelést értékeli a vizsgálatok során.

11.3. Közösségi felhőszolgáltatást igénybe vevő pénzügyi vállalkozásokat tömörítő cégcsoport esetében milyen egyszerűsítési lehetőségek vannak az egyes csoporttagok által elvárt kockázatelemzés tekintetében (pl. elegendő, hogy a szolgáltató specifikus kockázatelemzést felhasználhassa mindegyik cégcsoport tagja, kiegészítve a saját kockázataival)?

Az Intézmény támaszkodhat a cégcsoport szintű kockázatelemzésre, amennyiben annak hatóköre és minősége erre alkalmassá teszi azt, azonban ki kell egészítenie a saját kockázataival, azok értékelésével és ennek során a helyi jogszabályi elvárásokat is figyelembe kell vennie.

11.4. Milyen szintű kockázatként és milyen bekövetkezési gyakorisággal szükséges értékelni egy felhőszolgáltató esetén azon eseményt, hogy a szolgáltató „hirtelen” döntés alapján felfüggeszti a szolgáltatás nyújtását egy régióra, országra?

A kockázatelemzés az Intézmény hatásköre, melynek során fel kell mérnie a saját kockázattűrő képességét, valamint azt, hogy mik a szolgáltatás átköltöztetésének lehetőségei és időigénye.
A kockázatelemzésnek ki kell terjednie a felhőszolgáltatóval kapcsolatos geopolitikai kockázatokra is. Amennyiben a geopolitikai kockázatok elfogadhatatlan mértékűre nőhetnek, az ellehetetleníti a felhőszolgáltatás kockázatarányos megvalósítását, illetve veszélyeztheti a szolgáltatás rendezett kivezetését azáltal, hogy nem biztosított a szolgáltatás átköltöztetési lehetősége vagy a végrehajtásához szükséges idő.

11.5. Mi az MNB minimális, szerződésre vonatkozó tartalmi elvárása? Kollaborációs szolgáltatásokat nyújtó felhőszolgáltatások esetében milyen szerződéses kiegészítések/megoldások alkalmazhatók, mire kell különös figyelmet szentelni?

A pénzügyi intézményekre vonatkozó szerződéscsomagok jellemzően tartalmazzák a kötelező tartalmi elemeket, ugyanakkor az Intézmény felelőssége, hogy a szerződéskötést megelőzően az ágazati jogszabályoknak és az MNB ajánlásainak való megfelelést igazolja. További részleteket lásd a Felhő ajánlás 25. pontjában.

12. Felhőszolgáltatás ellenőrzése

12.1. Milyen evidenciákkal, konkrét hozzáférésekkel kell rendelkeznie az intézménynek, hogy meggyőződhessen például a szolgáltató által végzett titkosítás és 0-24 órában garantált biztonsági naplóelemzés megfelelőségéről?

A megfelelés ellenőrzése történhet a szolgáltatást biztosító eszközök menedzsment felületén keresztül, biztonsági naplóelemzés esetén pedig a központi biztonsági naplógyűjtő és -elemző (SIEM) rendszerből készített, az Intézmény szempontjából releváns naplóállományok SIEM rendszerbe történő beérkezését alátámasztó dokumentumokkal (például képernyőképekkel), továbbá biztonsági naplóelemzési riportokkal vagy azokból készített, az intézmény számára szűkített kivonattal. Emellett az Intézmény támaszkodhat saját vagy harmadik felektől származó megfelelőségi és ellenőrzési jelentésekre, tanúsítványokra. Amennyiben az Intézmény saját maga által generált titkosító kulcsokat használ, akkor további bizonyosságot szerezhet a kontrollok megfelelő működéséről (pl. BYO key, HSM modul). Ezen kérdéshez lásd még a Felhő ajánlás III.2.3. Bizonyosságszerzés pontját.

12.2. Felhő szolgáltatás esetében milyen penetrációs tesztelési periódust javasol a Felügyelet?

Figyelembe kell venni a szerződést, azon belül pedig kockázatarányos megközelítést javaslunk. Ezzel kapcsolatban az MNB Gyakori kérdések és válaszok sérülékenységvizsgálatok és betörési (penetrációs) tesztek végzésével kapcsolatban (GYIK) című dokumentuma[15] ad iránymutatást melynek 10. pontja szerint: „Az informatikai rendszer védelméről szóló (jelenleg) 8/2020. (VI.22.) MNB ajánlás 13.1.4. f) pontja szerint: „az Internet felől elérhető alkalmazások penetrációs tesztje a kockázatként meghatározott hibák javítása után, az üzembe állítást megelőzően, illetve bármely a biztonságot érintő változtatás alkalmával, majd legkésőbb évente ismételve megtörténik". (…) Az Internet felől nem elérhető, de kritikus adatokat feldolgozó rendszerek esetén is ajánlott a penetrációs teszt elvégzése (lásd a 8/2020. (IV. 22.) MNB ajánlás 4.4.8. pontja)."

12.3. A Felhő ajánlás III.3. Szerződéses követelmények című fejezetének 25. e) pontja szerint „amennyiben az Intézményre releváns, a szolgáltató által nyújtott szolgáltatás tanúsításának kikötése a (…) 42/2015. (III. 12.) Korm. rendelet szerint". Ezen előírás teljesül-e, amennyiben a szolgáltatóval kötött szerződés tartalmazza, hogy a szolgáltatónak alá kell vetni magát a szolgáltatás tanúsításának a 42/2015. (III. 12.) Korm. rendelet szerint, amennyiben a szolgáltatás a tanúsító szervezet által vizsgálat alá kerül?

Az általános audithoz való hozzájárulás rögzítése tartalmazza a zártsági audit lefolytatásának lehetőségét is.

13. Felhőszolgáltatásokkal kapcsolatos informatikai tevékenységek

13.1. Felhőszolgáltatás igénybe vételkor az Informatikai fejlesztésnek és üzemeltetésnek milyen konkrét tervezési és napi üzemeltetési feladatai vannak (üzembiztonság, DR képesség stb.)?

A feladatok az igénybe vett szolgáltatási modelltől függenek, például nem mindegy, hogy egy rendszerben az intézmény csak a jogosultságokat, jelszóparamétereket konfigurálja és minden mást a szolgáltató üzemeltet, vagy a szolgáltató csak a platformot adja és üzemelteti, a többit pedig az intézmény kezeli. A saját kezelésben maradó eszközök, rendszerek, funkciók üzemeltetését, DR képességét az Intézménynek kell biztosítania. A szerződéskötés során egyértelműen rögzíteni kell a felelősségi határokat, továbbá a felhőszolgáltatóval tisztázni szükséges a DR eljárásokat, azok költségvonzatát és az értesítési láncot.

13.2. A 8/2020 MNB ajánlásban megfogalmazott DLP, SSL megbontásra vonatkozó (kötelező?) követelményeket milyen formában várja el az MNB, hogy megvalósításra kerüljön pl. egy SaaS szolgáltatást igénybe vevő intézmény esetében?

Az adatszivárgás elleni védelemre vonatkozó követelményeket egy SaaS szolgáltatás esetén is vizsgálni és a kockázatokkal arányosan érvényesíteni kell az adatok teljes életciklusára (tárolás, megosztás, felhasználás stb.) vonatkozóan, minden lehetséges adatszivárgási csatornán. Előzetesen fel kell mérni, hogy milyen adatbiztonsági kontrollok érhetők el (szolgáltatói DLP, titkosítás, anonimizálás stb.), és ezt figyelembe kell

---

15 https://mnb.hu/letoltes/serulekenysegvizsgalatok-es-penetracios-tesztek-gyik-v1-0.pdf

További részletes útmutatásokat lásd az MNB Informatikai Felügyeleti Főosztályának weboldalán: https://www.mnb.hu/felugyelet/szabalyozas/informatikai-felugyelet

venni, értékelni kell a felhőszolgáltatás kockázatainak elemzése, a felhőszolgáltatás kiválasztása vagy elvetése során. A titkosított csatornák kockázatokkal arányos bontása és vizsgálata (például netbanki csatornák kivételként való kezelése mellett) vagy ennek hiányában kompenzáló kontrollok alkalmazása (például adatszivárgásra alkalmas vagy biztonsági kockázatot hordozó kategóriák és nem kategorizált oldalak tiltása WEB tartalomszűrési csatornán) felhőalapú és nem felhőalapú implementáció esetén egyaránt szükséges.

14. Felhőszolgáltatás felügyeleti vonatkozásai

14.1. Mi az MNB álláspontja banktitok felhő szolgáltatásban való kezeléséről?

Az MNB a kockázatarányos kontrollok kialakítását és működtetését várja el, ezek megléte esetén a banktitok is kezelhető felhőszolgáltatásban. Ezzel kapcsolatban lásd még a Felhő ajánlás adatvédelemre vonatkozó előírásait:

- III.1.1. Jogszabályi megfelelés biztosítása című fejezet 9. pontja;
- III.2.1. Az adatok és az adatkezelés helye című fejezet.
- IV.1. Adatbiztonság, adat- és titokvédelem című fejezet;
- 1. melléklet, 2. Adatvédelmi, információbiztonsági jogszabályok című fejezet;

14.2. Rendszerintegrátorként, banki beszállítóként van-e lehetőség konzultációra az MNB-vel, ha igen akkor mi a pontos menete?

Az MNB alapvetően a felügyelt intézmények számára tart konzultációt, azonban a rendelkezésre álló kapacitás függvényében nyitott az egyeztetésre más cégekkel is. Konzultációs igényüket a felügyelt intézmények az intézmény felügyelőjének jelezhetik, vagy konkrét kérdés esetén javasoljuk, hogy az Informatikai felügyelet honlapján[16] keresztül vagy az iff@mnb.hu e-mail címen vegyék fel a kapcsolatot az MNB Informatikai felügyeleti főosztályával.

14.3. Mikor kerül kiadásra a 4/2019 ajánlás új verziója és milyen számmal?

A DORA rendelet megjelenéséig nem tartjuk indokoltnak az ajánlás tartalmi felülvizsgálatát.

[16] https://www.mnb.hu/felugyelet/szabalyozas/informatikai-felugyelet

Tartalom