PRUDENCIÁLIS MODELLEZÉSI ÉS IT FELÜGYELETI IGAZGATÓSÁG

Gyakori kérdések és válaszok felhőszolgáltatások igénybevételével kapcsolatban (GYIK)

Konzultáció

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

Igen, van lehetőség a Felügyelettel konzultálni, melyet az Intézmény az MNB kijelölt intézményi felügyelőjén 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[1] kitöltésével lehet kapcsolatba lépni.

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.

Szabályozás

3. 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 (Felhőajánlás) , az informatikai rendszer védelméről szóló (jelenleg) 7/2017. (VII. 5.) MNB ajánlás[2] (Informatikai rendszer védelméről szóló ajánlás), az EBA[3] iránymutatása a kiszervezésről (jelenleg: EBA/GL/2019/02), az EIOPA[4] iránymutatásai a felhőszolgáltatókhoz történő kiszervezésről (jelenleg: EIOPA-BoS-20-002), illetve az ESMA[5] 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.

Fogalmak

---

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

[2] 2021. január 1-től a Magyar Nemzeti Bank 8/2020. (VI.22.) számú ajánlása az informatikai rendszer védelméről alkalmazandó

[3] Európai Bankhatóság

[4] Európai Biztosítás- és Foglalkoztatóinyugdíj-hatóság

[5] Európai Értékpapír-piaci Hatóság

4. 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. Ha kizárólag közösséget alkotó jogi személyek használják az adott felhőszolgáltatást, mint például a vállalatcsoporton belüli felhőszolgáltatás esetében, az közösségi felhő. Amennyiben egy vállalatcsoport közösen használ egy publikus felhőszolgáltatást, az publikus felhőnek minősül.

5. Mit jelent a magánfelhő?

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.

6. 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.

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

Nem, ez közösségi felhőnek minősül. Részletesen lásd a 4. kérdésben.

A felhő ajánlás hatálya

8. 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 is megvalósul, akkor az is a felhő ajánlás hatálya alá tartozik.

Megfelelés

9. 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.

10. 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 kontrollok megfelelősége és a jogszabályi kötelezettségek teljesítése a legfontosabb szempont.

11. 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).

12. 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.

13. 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.

14. 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 Felhőajánlás és az Informatikai rendszer védelméről szóló ajánlás követelményeit kimutathatóan teljesítenie kell.

15. 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 szolgáltatáscsomagját igénybe venni. Fontos 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 Felhőajánlás, melyen túl szükséges figyelembe venni a kiszervezésre vonatkozó ágazati jogszabályokat, valamint az európai felügyeleti hatóságok felhő irányelveiben foglaltakat is.

16. 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.

Információbiztonság

17. 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.

18. Minden esetben szükséges a Felhőszolgáltatótól független mentést biztosítani?

A felhőszolgáltatótól független mentést[6] 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 Felhőajánlás 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.

Felelősség

19. 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.

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

Adatvédelem

20. 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[7] 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 adatok EGT-n kívüli helyszínre történő továbbítása a fentiek miatt külön elemzést és ellenőrzést igényel, melyeket szerződéses vagy technológiai garanciákkal is ki kell kényszeríteni.

Felhőszolgáltatások ellenőrzése

21. 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.

22. 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.

[7] Európai Gazdasági Térség