

ÁLLÁSFOGLALÁS AZ MNB KÖZÖSSÉGI ÉS PUBLIKUS FELHŐSZOLGÁLTATÁSOK IGÉNYBEVÉTELÉRŐL SZÓLÓ 4/2019. (IV.1.) AJÁNLÁSÁVAL KAPCSOLATBAN

1. TÉNYÁLLÁS

A Megkeresésben a Biztosító az MNB-nek a közösségi és publikus felhőszolgáltatások igénybevételéről szóló 4/2019. (IV. 1.) számú ajánlása (**4/2019. MNB ajánlás**) alább ismertetett pontjainak értelmezésével kapcsolatban kérte az MNB álláspontját.

2. JOGKÉRDÉSEK

- i. A 4/2019. MNB ajánlás III.6. 33. g) pontja szerint az MNB elvárja, hogy a Biztosító a felhőszolgáltató megfelelő felügyelete és ellenőrzése körében hivatalosan átadott, a vonatkozó hazai és uniós jogszabályoknak megfelelő adatközpont helyszíneket vegyen igénybe.

A Biztosító a Megkeresésben arra vonatkozóan kérte az MNB állásfoglalását, hogy a megfelelő adatközpont kiválasztásakor pontosan mely hazai és uniós jogszabályok tekintendők irányadónak, továbbá mely tanúsítványokat tekint az MNB elfogadhatónak. A Biztosító a 4/2019. MNB ajánlás fenti pontjával kapcsolatosan nem ismertette álláspontját.

- ii. A 4/2019. MNB ajánlás III.6. 33. h) pontja rögzíti a Biztosító azon kötelezettségét, hogy a felhőszolgáltató megfelelő felügyelete és ellenőrzése körében legyen felkészülve a hibás teljesítés esetére, ennek körében pedig az üzletmenet-folytonosság biztosítása érdekében gondoskodjon alternatív felhőszolgáltatók, illetve más megoldások felméréséről.

A Biztosító által feltett kérdés arra irányult, hogy a hibás teljesítés esetén, illetve a kivezetési stratégia körében milyen technikai megoldások alkalmazhatóak. A Biztosító álláspontja, hogy egy alternatív felhőszolgáltató igénybevétele egyenértékű az on-premise telepített szolgáltatáshoz való visszatéréssel.

- iii. A 4/2019. MNB ajánlás IV.1.2. 48. e) pontja előírja, hogy a kockázatelemzés alapján kritikus funkcionalitás vagy rendszer esetén az intézmény gondoskodjon az adatmentések felhőszolgáltatótól független tárolásáról is; a függetlenül tárolt mentések rendszerességét a kockázatok és jogszabályi elvárások figyelembevételével határozza meg.

A Biztosító kérdése az adatmentések felhőszolgáltatótól független tárolásának lehetséges technikai megoldásaira irányult, álláspontja szerint az egyaránt megvalósulhat on-premise szolgáltatással, valamint alternatív felhőszolgáltatónál való adattárolással is. Ennek indoka, hogy a Biztosító véleménye szerint a független adattárolás célja az *„üzletfolytonossági vagy vészhelyzet helyreállítást igénylő esetben a szolgáltatások folytonosságához a szükséges adatállomány biztosítása”*.

- iv. A 4/2019. MNB ajánlás IV.3.2. 56. g) pontja értelmében az üzemeltetés biztonsága érdekében a Biztosító bizonyosságot szerez a szolgáltató informatikai üzemeltetési folyamatainak kontrollált működéséről, illetve megosztott hatáskör esetén a saját hatáskörébe tartozó elemekre vonatkozóan kialakítja ezeket – többek között – az SLA-k elvárásai, kezelése, monitorozása és jelentése hatókörben.

A Megkeresésben feltett kérdés arra irányult, hogy mekkora mozgástérrel rendelkezik a Biztosító az SLA elvárások és monitorozási követelmények meghatározásában, a Biztosító álláspontja szerint ugyanis az MNB-nek nincs „részletes elvárása” az SLA-k tekintetében. A Biztosító nyilatkozata szerint az SLA-követelményeket *„a Biztosítónak kell meghatároznia a saját üzleti elvárásainak figyelembevételével úgy, hogy a követelmények biztosítsák az elvárt működési szint megfelelőségét, annak monitorozhatóságát. Az SLA értékek számszerűsítettek, átláthatók és ellenőrizhetők legyenek mind a Biztosító, mind a szolgáltatást végző szolgáltató, mind a felügyelő hatóság számára.”*

- v. A Biztosító továbbá – hivatkozva a 4/2019. MNB ajánlás lényeges tevékenységek értékelésekor követendő szempontokat tartalmazó rendelkezéseire – az általa megjelölt konkrét tevékenységek minősítésével kapcsolatban kérte az MNB álláspontját. A konkrét példákon túl, kérdése arra irányult, hogy helyes-e azon álláspontja miszerint „*a biztosító az ajánlásban adott és saját érvei mentén meghatározhatja azon tevékenységeinek körét, amik megítélése szerint nem minősülnek lényeges tevékenységnek, amit megfelelő indoklás mellett a T. MNB sem kifogásol.*”

3. AZ MNB ÁLLÁSPONTJA

Amint az az MNB honlapján megtalálható, „*Állásfoglalás kéressel kapcsolatos eljárások és elvek*” című tájékoztatóban¹ (Tájékoztató) is szerepel, a jogszabályok által meghatározott körön kívül az MNB-nek nincs hatásköre – többek között – szerződések, termékek, üzleti megoldások, folyamatok jogi megfelelőségének előzetes, általános vizsgálatára.

Állásfoglalás kiadására jellemzően jogszabályi rendelkezések értelmezése, illetve keretjellegű normatív rendelkezések tartalommal való feltöltése vonatkozásában kerül sor. Az állásfoglalás kiadása nem hatósági ügy, arra nem vonatkoznak a hatósági eljárásokban irányadó határidők, és bármely tevékenységnek, üzleti döntésnek, jogügyletnek (illetve ezek elhatárolásának, megkezdésének, végrehajtásának) az MNB állásfoglalásától való függővé tétele kizárólag az állásfoglalást kérő személy felelőssége. A jelen állásfoglalásban foglaltak nem értelmezhetőek a Megkeresésben írtakkal érintett üzleti koncepció, megoldás jogszabályi megfelelőségével kapcsolatos felügyeleti álláspontként, az MNB célja a jelen – nem kötelező erejű – állásfoglalás kiadásával összefüggésben az, hogy a Biztosító annak ismeretében alakíthassa ki saját jogi álláspontját.

3.1. AZ ADATKÖZPONTOKKAL KAPCSOLATOS ELVÁRÁSOK

Az MNB az adatközpont megfelelőségének hitelt érdemlő igazolására kizárólagos szabványt nem határoz meg. Az egyes adatközpontok megfelelőségét a Biztosítónak kell vizsgálnia a kiválasztás során, az MNB-nek nincs hatásköre állásfoglalás kiadására a piaci szereplők által nyújtott – a felügyelt intézmények által (is) igénybe vehető – adatközpontok megfelelőségének általánosságban való értékelésére vonatkozóan.

A Biztosító például, de nem kizárólagosan az alábbi szabványok szerinti tanúsításokat, keretrendszereket is figyelembe veheti az adatközpont és az általa nyújtott szolgáltatások megfelelőségének igazolása érdekében:

- The Series of Standards EN 50600 Information technology – data centre facilities and infrastructures
- ANSI/BICSI 002-2019, Data Center Design and Implementation Best Practices
- The Telecommunications Industry Association (TIA) ANSI/TIA-942
- Uptime Institute standard for datacenter design
- ISO/IEC 27000 series
- NIST's Special Publications (SP 800-123, SP 800-12, SP 800-53, SP 800-30, SP 800-37, SP 800-39)
- Payment Card Industry Data Security Standard (PCI DSS)
- SOC 2; ISAE 3402
- Common Criteria
- COBIT; ITIL; TOGAF; SABSA; COSO
- FIPS 140-2

Az MNB továbbá felhívja a Biztosító figyelmét, hogy a 4/2019. MNB ajánlás 1. számú melléklete tartalmazza az ajánlás tárgyához kapcsolódó egyes jogszabályok, ajánlások és iránymutatások felsorolását, amelyek a kiválasztás során iránymutatásul szolgálhatnak és amelyekre a 4/2019. MNB ajánlás III.6. 33. g) pontja utal.

3.2. HIBÁS TELJESÍTÉS ESETÉRE VALÓ FELKÉSZÜLÉS LEHETSÉGES MÓDJAI

A 4/2019. MNB ajánlás a III.2.2.20. és 21. pontjában a felhőszolgáltatás kockázatelemzése körében előírja a *kivezetés kockázatainak előzetes felmérését*, kockázatcsökkentő intézkedésként pedig kivezetési stratégia elkészítését. A 21. pont lényegében a kivezetési stratégia céljaival és az azokhoz kapcsolódó általános intézkedésekkel foglalkozik, előírva a Biztosítónak, hogy a kivezetési stratégia részeként

¹ <http://www.mnb.hu/felugyelet/szabalyozas/allasfoglalasok/allasfoglalas-keressel-kapcsolatos-eljarasok-es-elvek>

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

Tekintve, hogy a hibás teljesítésre való felkészülésre alapvetően a felhőszolgáltatásból való kilépés, így a szolgáltatáskivezetési (exit) stratégia és akcióterv részeként kerül sor, a kivezetéssel kapcsolatos elvárások és az ott megfogalmazott célok szem előtt tartásával kell a Biztosítónak döntenie a lehetséges megoldásokról. A fentieket is alapul véve a kivezetési stratégia célja, hogy a Biztosító anélkül tudjon kilépni a felhőalapú kiszervezési megállapodásból, hogy a kilépés, illetve az átállás indokolatlanul akadályozná vagy rontaná az ügyfeleknek nyújtott szolgáltatásai folytonosságát vagy minőségét, illetve hátrányosan érintené a jogszabályi követelményeknek való megfelelését.

Az MNB ajánlás III.7.1. 35. b) pontja a *kivezetés előkészítése* körében rögzíti, hogy „az Intézmény a kivezetés előkészítése során a kivezetés megvalósításához biztosítja a szükséges személyi, tárgyi, technikai, jogi és szerződéses feltételek meglétét, így a szolgáltatás kivezetéséhez, **helyi üzemeltetéshez, esetleg más szolgáltatóhoz történő továbbításához** szükséges szaktudást, projektcsapatot.”

Támpontot nyújthat a felhőszolgáltatókhoz történő kiszervezés lebonyolítása során az Európai Biztosítás- és Foglalkoztatáspolitikai Bizottság (EIOPA) által 2019. július 1. napján publikált „*Consultation paper on the proposal for Guidelines on outsourcing to cloud service providers*”² (**Consultation Paper**) elnevezésű, kifejezetten a felhőszolgáltatókhoz történő kiszervezéssel foglalkozó, arra vonatkozó iránymutatások tervezetét tartalmazó dokumentum³. A kivezetési stratégiával foglalkozó 15. iránymutatás⁴ alapján a Biztosítónak lehetősége van a kivezetés során a kiszervezett tevékenység másik szolgáltató(k)nak történő átadására, valamint a tevékenység saját, közvetlen irányítás alá történő bevonására is. A Biztosítónak a fenti megoldások alkalmazásakor figyelembe kell vennie az érintett adatok helyét és az üzletmenet fenntartásának biztosíthatóságát az átállási szakasz során. A vonatkozó rendelkezések alapján az MNB álláspontja, hogy hibás teljesítés esetén – amennyiben az adott szolgáltatás más felhőszolgáltatónál is elérhető – alternatív felhőszolgáltató is igénybe vehető az üzletmenet-folytonosság biztosítására, továbbá az alternatív felhőszolgáltató igénybevétele a kivezetési stratégia szempontjából az on-premise, helyben telepített megoldással egyenértékű megoldás lehet a kivezetés végrehajtása során.

3.3. ADATMENTÉSEK FELHŐSZOLGÁLTATÓTÓL FÜGGETLEN TÁROLÁSÁNAK LEHETSÉGES MÓDJAI

A 4/2019. MNB Ajánlás a IV.) a felhőszolgáltatás-biztonsági alapelvek című fejezet alatt a IV.1.1. pontban a tárolt adatok biztonságáról rendelkezik a 47. pontban, rögzítve azt az általános követelményt, hogy a Biztosító és a felhőszolgáltató a tárolt adatok kapcsán, az azokat felhasználó üzleti folyamat biztonsága érdekében gondoskodik a felhőben tárolt adatok rendelkezésre állásáról, illetve az adatok védelméről az illetéktelen megismerés és módosítás ellen. Az ezt követő konkrét, a fent megjelölt cél megvalósítását elősegítő rendelkezések között szerepel, hogy a Biztosító gondoskodik az adatmentések felhőszolgáltatótól független tárolásáról is a kockázatelemzés alapján kritikus funkcionalitás vagy rendszer esetén.

A fentiek alapján a Biztosító által foganatosított független adatmentések elsősorban az adatok folyamatos rendelkezésre állását szolgálják. Az 4/2019. MNB ajánlás, illetve egyéb vonatkozó jogszabály a független adatmentés megvalósítására, annak módjára nem tartalmaz kifejezett rendelkezést, megkötést. Az MNB álláspontja ennek megfelelően, hogy a felhőszolgáltatótól független tárolás egyaránt megvalósulhat on-premise, illetve alternatív felhőszolgáltatónál való adattárolással.

3.4. A SZOLGÁLTATÁSISZINT-MEGÁLLAPODÁSBAN (SLA) RÖGZÍTENDŐ TARTALMI ELEMEL

² <https://eiopa.europa.eu/Publications/Consultations/2019-07-01%20ConsultationDraftGuidelinesOutsourcingCloudServiceProviders.pdf>

³ A nyilvános konzultációra bocsátott iránymutatásokat várhatóan 2020. július 1-jétől kell alkalmazni, amely időpontig azok tartalma módosulhat. Az MNB célszerűnek tartja, hogy ezen módosításokat, változásokat a Biztosító kísérvé figyelemmel.

⁴ Guideline 15.- b) identify alternative solutions, where appropriate and feasible, and develop transition plans to enable the undertaking to remove and transfer existing activities and data from the cloud service provider **to alternative service providers or back to the undertaking**. (...).

A Biztosítónak akár a kiszervezési szerződés részeként, akár külön megállapodásban rögzítenie kell a szolgáltatási szintre vonatkozó elvárásokat, rendelkezéseket. Ezek tartalmát a Biztosító üzleti igényeinek megfelelően alakíthatja ki, amelynek kialakításakor támpontot nyújt a 4/2019. MNB ajánlás az alábbiak szerint:

„III.3. Szerződéses követelmények

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

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

na) a mérendő indikátorok, és az elvárt mértékei;

nb) a mérések módja és eszközei;

nc) a szolgáltatás elérhetősége és minimális funkcionalitása;

nd) a méréseket végző fél, az SLA jelentések elkészítésének felelőssége, jelentések gyakorisága;

ne) az SLA-k megsértésének kárral arányos következményei és az eskalációs eljárások rögzítése;”

A fentiekkel lényegében egyező követelményeket támaszt a Consultation Paper a 10. iránymutatás 35. j)⁵ pontjában (*the agreed service levels which should include quantitative and qualitative performance targets, that are directly measured by the undertaking in order to independently monitor the services received and, eventually, adopt corrective action if agreed service levels are not met*).

A 4/2019. MNB ajánlás – az I. pontjában foglaltak alapján – az ágazati és egyéb vonatkozó további jogszabályokban és ajánlásokban foglaltakkal együtt, azokon felül értelmezendő. Így a Biztosítónak továbbra is figyelembe kell vennie az informatikai rendszer védeleméről szóló 7/2017. (VII. 5.) MNB ajánlás (7/2017. MNB ajánlás) 4.2.4. pontjában foglaltakat, amelyek előírják, hogy „a szolgáltatási szerződések (a továbbiakban: SLA) esetén az intézmény szerződéses feltételekkel biztosítja, hogy a szolgáltatás az intézmény részéről mérhető, számonkérhető és szankcionálható legyen (SLA követelmények érvényesítése).”

A SLA vonatkozásában tehát kötelező konkrét tartalmi elem szerepeltetése nem elvárt, az MNB a megállapodás kidolgozásakor követendő elveket és szempontokat határozott meg, amelyeken túl az 4/2019. MNB ajánlás IV.3.2. 56. g) pontja alapján az SLA-ban rögzítettek folyamatos ellenőrzése, figyelemmel kísérése is elvárt a Biztosítótól.

3.5. LÉNYEGES TEVÉKENYSÉGEK ÉRTÉKELÉSE

Amint az fentebb kifejtésre került, az MNB állásfoglalásának tárgyát alapvetően jogi normák által nem szabályozott kérdések, többféleképpen értelmezhető, adott esetben egymásnak ellentmondó jogi szabályozás képezheti, az állásfoglalás kiadásának célja pedig, hogy az állásfoglalást kérő személy az MNB – nem kötelező erejű – állásfoglalása ismeretében kialakíthassa saját jogi álláspontját. Az MNB-nek ugyanakkor nincs hatásköre egyéb szabályzatok, szerződések, termékek, üzleti folyamatok előzetes általános vizsgálatára. Ebből következik, hogy a Biztosító által a lényeges tevékenységek értékeléséhez kapcsolódóan példaként felhozott konkrét tevékenységek megítélése, illetve minősítése nem szolgálhat állásfoglalás kiadásának alapjául.

A Megkeresésben előadott, jelen pontban tárgyalt kérdés kapcsán az MNB felhívja a Biztosító figyelmét, hogy a 4/2019. MNB ajánlás 13-15. pontján túl a Biztosítónak a vonatkozó jogszabályokat, így többek között a Bit. kiszervezésre vonatkozó rendelkezéseit, valamint a Bizottság (EU) 2015/35 felhatalmazáson alapuló (2014. október 10.), a biztosítási és viszontbiztosítási üzleti tevékenység megkezdéséről és gyakorlásáról szól 2009/138/EK európai parlamenti és tanácsi irányelv (Szolvencia II) kiegészítéséről szóló rendelet 274. cikkét is figyelembe kell vennie a tevékenységek minősítése során.

⁵ Guideline 10. – Contractual requirements

35. In addition to the set of requirement defined by Article 274 of the Delegated Regulation, the written agreement between and undertaking and the cloud service provider for arrangements should set out at least:

j) the agreed service levels which should include quantitative and qualitative performance targets, that are directly measured by the undertaking in order to independently monitor the services received and, eventually, adopt corrective action if agreed service levels are not met;

A Consultation Paper a 7. iránymutatásban a 25-27. pontban foglalkozik a kiszervezett tevékenység minősítésével. Ennek lényege, hogy a 2015/35 Rendelet alapján kritikus vagy fontos – a Bit. szóhasználatában kiemelten fontos – működési feladatkör vagy tevékenység felhőszolgáltatóhoz történő kiszervezése minden esetben lényeges tevékenységnek minősül („*The undertaking should consider always as material all the outsourcing of critical or important operational functions to cloud service providers.*”). Annak megítélése szempontjából, hogy mely tevékenységek minősülnek kritikus vagy fontos működési feladatkörnek vagy tevékenységnek az MNB „*Melyek azok az elvek, szempontok, amelyek alapul vételével a biztosító az általa működtetett és a törvényben ilyenként fel nem sorolt feladatköröket és tevékenységeket kiemelten fontosnak minősítheti*”⁶ címet viselő állásfoglalása nyújthat segítséget.

Amennyiben az értékelés alapján a felhőszolgáltatóhoz kiszervezett tevékenység nem minősül kritikus vagy fontos feladatkörnek, illetve tevékenységnek, úgy a Consultation Paper 27. a)-h)⁷ pontjaiban meghatározottakat kell a Biztosítónak figyelembe vennie és értékelnie – a kockázatelemzéssel (4/2019. MNB ajánlás III.2. 17-18. pont) is összhangban – a tevékenység lényegességének értékelése során.

A fentiekre tekintettel, az ismertetett elvek és szempontok alapján a Biztosító saját érvei mentén meghatározhatja azon tevékenységek körét, amelyek megítélése szerint nem minősülnek lényeges (materiális) tevékenységnek. Ez azonban értelemszerűen nem zárja ki, hogy az MNB a minősítés jogszabályoknak, illetve egyéb szabályozó eszközöknek való megfeleléséget utóbb vizsgálja, és – a Biztosító indokolását is szem előtt tartva – egyedileg mérlegelve döntsön annak megfeleléséről.

Felhívom figyelmét arra, hogy az MNB – a honlapján megtalálható részletes Tájékoztatóval összhangban – kizárólag konkrét jogkérdésben foglal állást, a felügyelt intézmények tevékenységét, alkalmazott gyakorlatai jogszabályi megfeleléséget folyamatos felügyelés keretében, helyszíni vagy helyszínen kívüli vizsgálatok során ellenőrzi. Az MNB véleményét kizárólag a Biztosító által rendelkezésre bocsátott információk alapján alakította ki, a jelen állásfoglalásban foglalt egyedi jogértelmezés kizárólag a Biztosító által előadott tényállásra vonatkozik. Az MNB véleménye nem tekinthető kötelező erejű állásfoglalásnak, más hatóságra, illetve a bíróságra nézve nincs kötelező tartalma. A jelen állásfoglalás kizárólag a Biztosító tájékoztatása céljából készült, a benne foglaltak egyéb célok érdekében, továbbá harmadik személyekkel szemben nem használhatóak fel, illetve jogvita eldöntésére nem alkalmazhatóak.

⁶ [http://alk.mnb.hu/data/cms2421472/tmp8B9C.tmp\(9137819\).pdf](http://alk.mnb.hu/data/cms2421472/tmp8B9C.tmp(9137819).pdf)

⁷ 27. Moreover, in order to determine the materiality of cloud outsourcing, undertakings should take into account, together with the outcome of the risk assessment, at least the following factors:

- a. the potential impact of outages, disruptive events or failure of the cloud service provider to provide the services at the agreed service levels on the undertaking:
 - i. continuous compliance with the conditions of their authorization, and other obligations under the Solvency II Directive;
 - ii. short and long-term financial and solvency resilience and viability;
 - iii. business continuity and operational resilience;
 - iv. operational risk, including conduct, information and communication technology (ICT), cyber and legal risks;
 - v. reputational and strategic risks;
 - vi. recovery and resolution planning, resolvability and operational continuity in an early intervention, recovery or resolution situation, where applicable.
- b. the potential impact of the cloud outsourcing arrangement on the ability of the undertaking to:
 - i. identify, monitor and manage all risks;
 - ii. comply with all legal and regulatory requirements;
 - iii. conduct appropriate audits regarding the function affected by the cloud outsourcing arrangement, in line with Article 38 of the Solvency II Directive;
- c. the undertaking's aggregated exposure to the same cloud service provider and the potential cumulative impact of outsourcing arrangements in the same undertaking's business area;
- d. the size and complexity of any undertaking's business areas affected by the cloud outsourcing arrangement;
- e. the cost of the cloud outsourcing as a proportion of total operating and ICT costs of the undertaking;
- f. the potential business interconnections between the undertakings and the cloud service provider. For instance, if the undertaking is providing (re)insurance coverage to the cloud provider;
- g. the ability, if necessary or desirable, to transfer the proposed cloud outsourcing arrangement to another cloud service provider or reintegrate the services ('substitutability'); and
- h. the protection of personal and non-personal data and the potential impact of a confidentiality breach or failure to ensure data availability and integrity on the undertaking, policyholders or other relevant subjects including but not limited