MICROSEC

Microsec zrt.

NIS2, DORA és Adatrendelet segédlet

V1.3

Tartalom

1 Bevezetés

Az Európai Unió több új az IT területet szabályozó rendeletet, direktívát fogadott el, amelyek a termékek és szolgáltatások különböző vizsgálatát, osztályozását vagy besorolását írják elő, továbbá a beszállítók/harmadik feles szolgáltatók ellenőrzése is előírt feladattá vált.

Ezek jogi szabályok a következők:

- **Adatrendelet (Data Act)** – a 2023/2854/EU[1] rendelet az összekapcsolt termékekről és szolgáltatásokról
- **NIS2 irányelv –** a 2022/2555/EU[2] direktíva és nemzeti szabályozása, amelynek célja a magasabb IT biztonság
- **DORA rendelet** – a 2022/2554/EU[3] rendelet a pénzügyi ágazat ellenálló képességéről (tk. a NIS2 bankspecifikus előírásai)

A Microsec zrt. abból a célból állította össze jelen dokumentumot, hogy ügyfelei számára megkönnyítse a fenti jogszabályoknak megfelelést.

Jelen dokumentumban információkat tartalmaz:

- a jogszabályokról,
- a besorolási elvekről,
- az előzetesen elvégzett besorolásról, és
- ahol értelmezett, arról, hogy hogyan lehet a követelmények megvalósulását a legkönnyebben ellenőrizni.

Amennyiben az Ön szervezete alanya valamelyik fenti előírásnak, tekintse meg az arra vonatkozó fejezeteket.

[1] https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:32023R2854

[2] https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:32022L2555

[3] https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:32022R2554

2 Az Adatrendelet (Data Act)

Az Európai Parlament és a Tanács (EU) 2023/2854 rendelete a méltányos adathozzáférésre és -felhasználásra vonatkozó harmonizált szabályokról, valamint az (EU) 2017/2394 rendelet és az (EU) 2020/1828 irányelv módosításáról (**továbbiakban Adatrendelet**) 4 fő célt tűz ki, melyek a következők:

1. **Adathozzáférés biztosítása a felhasználóknak**

   A legfőbb cél az, hogy a felhasználók – legyenek azok magánszemélyek vagy vállalkozások – visszakapják az ellenőrzést az általuk generált adatok felett.

   - A rendelet arra kötelezi az adatbirtokosokat (pl. az összekapcsolt termékek, mint az okoseszközök és ipari gépek gyártóit), hogy az adatokhoz való hozzáférést biztosítsák a felhasználóknak.
   - A felhasználók ingyenesen és könnyen hozzáférhetnek a termékeik használatával keletkezett adatokhoz, és eljuttathatják azokat egy általuk választott harmadik félnek (pl. egy javítószolgáltatónak vagy egy új szolgáltatónak).

2. **A B2B adatmegosztás ösztönzése**

   A rendelet továbbá megteremti a jogi kereteket ahhoz, hogy a vállalkozások (különösen a kkv-k) hozzáférhessenek a nagyobb szereplők által birtokolt adatokhoz, ösztönözve ezzel az innovációt és a versenyt.

   - Az adatbirtokosoknak az adatokat méltányos, ésszerű és megkülönböztetésmentes (FRAND) feltételek mellett kell megosztaniuk a harmadik felekkel, ha ezt a felhasználó kéri.
   - Különös figyelmet fordít a rendelet arra, hogy megtiltsa az adatok megosztására és felhasználására vonatkozó olyan tisztességtelen szerződéses feltételeket, amelyeket egyoldalúan szabtak meg a felek között, védve ezzel a kkv-kat.

3. **Az adatpiac élénkítése és a verseny növelése**

   Cél, hogy az adatok megosztása révén új, innovatív adat vezérelt szolgáltatások (pl. prediktív karbantartás, javítószolgáltatások) jöhessenek létre, ami általánosan növeli az EU gazdasági teljesítményét.

4. **Váltás a szolgáltatók között (cloud switching) megkönnyítése**

   A rendelet megkönnyíti a felhő- és adatfeldolgozási szolgáltatók közötti váltást, ezáltal megelőzve az ügyfelek beékelődését (vendor lock-in) és növelve a versenyt ezen a piacon.

2.1 Az Adatrendelet szerinti besorolás alapelvei

Mivel az Adatrendelet azon termékekre és szolgáltatásokra vonatkozik, amelyek vagy „összekapcsolt termékek” vagy „kapcsolódó szolgáltatások”, ahhoz, hogy megállapítsuk, hogy valamelyik termékünk, szolgáltatásunk esetében ez hatályos-e ránk, el kell végeznünk a termékek szolgáltatások besorolását.

Ezt minden egyes termékre és szolgáltatásra vonatkozóan a következő táblázatban található kérdéslista megválaszolásával végezhetjük el.

Amennyiben a válaszaink megegyeznek az Összekapcsolt termék vagy a Kapcsolódó szolgáltatás oszlop tartalmával, akkor azonosítottunk olyan terméket, szolgáltatást, amire vonatkozik az Adatrendelet.

	Összekapcsolt termék	**Kapcsolódó szolgáltatás**
A termék tárgy-e?	Igen	Nem
A termék felhasználásra vagy környezetre vonatkozóan adatot gyűjt-e?	Igen	-
Fizikai hozzáférésen vagy eszközön keresztül képes-e termék adatokat közölni?	Igen	-
A termék elsődleges funkciója-e a felhasználótól eltérő személy által végzett tárolás, továbbítás, kezelés?	Nem	-
A kapcsolódó szolgáltatás hiánya meggátolja egy vagy több termék funkció működését.	Igen	Igen

2.2 A Microsec zrt. által elvégzett Adatrendelet szerinti termékbesorolás

A Microsec zrt. **nem rendelkezik összekapcsolt termékkel**.

A Microsec zrt. **kapcsolódó szolgáltatást nyújt az e-Szignó Scan&Sign termékhez**, melyek esetében a szkenner termékhez olyan kapcsolódó szolgáltatást nyújt, amivel hiteles konverzió végezhető el.

3 NIS2 direktíva

A NIS2 egy uniós irányelv, amely megerősíti a kiberbiztonsági követelményeket a kritikus szektorokban működő, mintegy 18 ágazatban. Célja, hogy egységesen magas szintű kiberbiztonsági érettséget érjen el az EU-ban a hálózatok és információrendszerek védelmének növelésével, szigorúbb kockázatkezelési előírásokat és incidensbejelentési kötelezettségeket vezetve be.

Ennek a magyar jogba iktatását végezte el a **2024. évi LXIX. törvény[4] Magyarország kiberbiztonságáról** (továbbiakban Kiberbiztonsági törvény) és egészítette ki részletszabályokkal a **7/2024. MK rendelet[5] a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről** (továbbiakban MK rendelet).

A minősített bizalmi szolgáltatásokat a Kiberbiztonsági törvény 1. §. (4) g) alapvető szervezetnek tekinti, így az **e-Szignó Hitelesítés szolgáltató kiberbiztonsági audit elvégzésére kötelezett, melyet weboldalán közzé tesz.**

3.1 Az információs rendszerek MK rendelet szerinti biztonsági osztályba sorolása

Az elektronikus információs rendszereink biztonsági osztályba sorolását az MK rendelet 1. mellékletének 2. pontja alapján kell végezni.

[4] https://net.jogtar.hu/jogszabaly?docid=a2400069.tv

[5] https://net.jogtar.hu/jogszabaly?docid=a2400007.mkf

3.2 A Microsec zrt. által elvégzett az MK rendelet szerinti termék- és szolgáltatás biztonsági osztályba sorolása

Alap biztonsági osztályba került besorolásra:

- Minden fejlesztett és forgalmazott szoftvertermék
  - e-Szignó Desktop
  - e-Szignó Mobile
  - e-Szignó SDK
  - e-Szignó Server
  - e-Szignó Autosigner Client| Service
  - e-Szignó Preserver
  - e-Szignó Microsigner
  - e-Szignó Web On-Premise
  - e-Szignó Scan & Sign
  - e-Szignó Scan & Sign
  - e-Szignó Certmanager
- Nem bizalmi szolgáltatások
  - Microsigner közvetítő szolgáltatás
  - Eszosz

Jelentős biztonsági osztályba került besorolásra

- Bizalmi szolgáltatások
- V2X szolgáltatások

3.3 További segédlet az ellátási lánc kockázatmenedzsmentjéhez, ellenőrzéséhez

A NIS2 a teljes ellátási lánc védelmére törekszik, így ennek kapcsán ki kell terjeszteni a kockázatmenedzsmentet az alvállalkozókra/beszállítókra is, továbbá meg kell valósítani azok megfelelő ellenőrzését is.

A Microsec zrt. ellenőrzését az ellátási menedzsment kapcsán javasolt a szolgáltató tanúsításai alapján megtenni.

Az elérhető megfelelőségértékelések/tanúsítások:

- **eIDAS megfelelőségértékelés**

  Évente kell végrehajtani.

  A sikeres audit tanúsítvány bizonyítja (mert ezek előfeltételei), hogy:

  - A szolgáltató rendelkezik NIS2 audittal.

    Az eIDAS (21. cikk (2) 2 szerint ez előfeltétele a szolgáltató eIDAS megfelelőség értékelésének.

  - A szolgáltató évente 4x sérülékenység vizsgálatot és 1x penetrációs vizsgálatot hajt végre.

    A bizottsági végrehajtási rendeletek ezt kötelezővé teszik.

  Az eIDAS megfelelőség értékelés elérhető az alábbi oldalon:

  https://e-szigno.hu/eidas-megfeleles

- **NIS2 audit**

  Kétévente kell végrehajtani.

  A sikeres audit tanúsítvány bizonyítja, hogy a szolgáltató megfelel a NIS2 előírásainak.

  A NIS2 audit igazolás elérhető az alábbi oldalon:

  https://www.microsec.hu/hu/minosegbiztonsag-es-audit

- **ISO 9001 és ISO 27001 tanúsítások**

  Évente kerülnek megerősítésre.

  Az ISO 9001 és ISO 27001 tanúsítások elérhetők az alábbi oldalon:

  https://www.microsec.hu/hu/minosegbiztonsag-es-audit

4 DORA rendelet

A DORA rendelet (Digital Operational Resilience Act) egy olyan EU-s pénzügyi szabályozás, amely a pénzügyi szektor működési biztonságára összpontosít.

Szabályokat és előírásokat határoz meg a pénzintézetek számára információs és kommunikációs technológiával kapcsolatos események észlelésére, védelmére, helyreállítására és javítására a pénzintézeteken belül. Ennek a szabályozásnak része, hogy a harmadik feles IKT szolgáltatók (tehát olyan szolgáltatók, akik a pénzügyi szervezet részére szolgáltatnak) tevékenységet is nyomon kövesse a pénzintézet, biztos lehessen ezen szolgáltatók biztonságában is.

A harmadik feles szolgáltatókra a DORA rendeletből a 30. cikk rendelkezései vonatkoznak.

4.1 A DORA rendelet besorolási szintjeinek ismertetése

A harmadik feles IKT szolgáltatók tevékenységének nyomon követéséhez a pénzügyi szervezetnek be kell sorolnia azokat. Három besorolási szint létezik, és ezek különböző követelményeket várnak el:

4.1.1 Alap

Sajnos a DORA nem adott nevet a kategóriának, de a következőkben Alap szintként hivatkozunk rá.

Ez esetben harmadik féllel kötött szerződésnek a Rendelet 30. cikk (2) paragrafusában leírtakat kell tartalmaznia, és annak kell meg is felelni.

Ezek nagyon röviden:

- Szolgáltatás teljes körű leírása (dokumentáció),
- Alvállalkozó igénybevételének szabályai,
- Szolgáltatás földrajzi helyének megjelölése,
- Adatvédelmi rendelkezések,
- Adatvisszaszolgáltatási rendelkezések,
- Hatósági együttműködési kötelezettség,
- Szerződés megszüntetési rendelkezések,
- Részvételi kötelezettség a pénzügyi szervezet biztonságtudatossági képzésein.

4.1.2 Kritikus vagy fontos funkciót támogató IKT szolgáltatás

A rendelet definíciója szerint a *„kritikus vagy fontos funkció”: olyan funkció, amelynek zavara lényegesen rontaná a pénzügyi szervezet pénzügyi teljesítményét, vagy szolgáltatásai és tevékenységei megbízhatóságát vagy folytonosságát, vagy az említett funkció kiesése, hibás vagy meghiúsult működése lényegesen rontaná a pénzügyi szervezet képességét az engedélyében foglalt feltételek és kötelezettségek, valamint a pénzügyi szolgáltatásokra vonatkozó jogszabályokban előírt egyéb kötelezettségei folyamatos teljesítésére.*

A kritikus vagy fontos funkciót támogató IKT szolgáltatás esetben harmadik féllel kötött szerződésnek tartalmaznia mindent, ami Alap szintnél szükséges, valamint két további lényeges dolgot:

- A harmadik feles IKT szolgáltató vezessen be a DORA-nak megfelelő vészhelyzeti terveket, és olyan IKT biztonsági intézkedéseket, mint a sérülékenység vizsgálat, penetrációs vizsgálat és a kódelemzés.
- Vegyen rész a veszély alapú (TLPT) behatolás tesztelésben.

4.1.3 Kritikus harmadik fél IKT-szolgáltató

Ezt a besorolást az erre feljogosított hatóság osztja ki. Jelenleg nincs ilyen.

4.2 A DORA besorolási módszertan kidolgozása és a besorolás

A 2024/1773/CID 3. cikk (2) bekezdése alapján a pénzügyi szervezet által kidolgozott módszertanon kell alapulnia a harmadik feles IKT szolgáltatások besorolásának. Ennek alapján a következőképpen érdemes eljárni, figyelembe véve a kockázatkezelés alapelveit.

4.2.1 Alap kategóriába javasolt sorolni

Az itt felsorolt esetek mindegyikére jellemző, hogy a termék/szolgáltatás kiváltása piaci termékkel rövid idő alatt biztosítható:

- Minden olyan szolgáltatást, amely használata során nem integrált, és aminek van alternatív lehetséges forrása.
- Nyílt, szabványos felülettel integrált szolgáltatásokat
- Ezek esetében a szabványos felület lehetővé teszi, hogy egy ugyanezen interfészt támogató alternatív szolgáltatóhoz a szolgáltatás átvihető legyen.
- Nem egyedi fejlesztésű szoftvereket.

Az Alap szintre besorolásban továbbá segíthet a Bizottság (EU) 2017/565 felhatalmazáson alapuló rendelet 30. cikk (1) és (2) is, amely a következőt mondja:

> *(1) A 2014/65/EU irányelv 16. cikke (5) bekezdése első albekezdésének alkalmazásában az operatív funkció akkor tekintendő kritikusnak vagy fontosnak, ha a teljesítésében bekövetkezett hiányosság vagy hiba lényegesen gyengítené a befektetési vállalkozás folyamatos megfelelését az engedélyezéséhez szükséges feltételeknek és kötelezettségeknek vagy a 2014/65/EU irányelvből eredő egyéb kötelezettségeinek, illetve gyengítené pénzügyi teljesítményét és befektetési szolgáltatásainak és tevékenységeinek megalapozottságát vagy folyamatosságát.*
>
> *(2) A többi funkció státusának sérelme nélkül a következő funkciók nem tekinthetők kritikusnak vagy fontosnak az (1) bekezdés alkalmazásában:*
>
> *a) a vállalkozásnak nyújtott tanácsadói szolgáltatások és egyéb, a vállalkozás befektetési tevékenységének részét nem képező szolgáltatások, beleértve a vállalkozásnak nyújtott jogi tanácsadást, a vállalkozás alkalmazottainak képzését, a számlázási szolgáltatásokat és a vállalkozás helyiségeinek és alkalmazottainak biztonságát is;*
>
> *b) szabványosított szolgáltatások megvásárlása, beleértve a piaci információs szolgáltatásokat és árfolyamok szolgáltatását.*

Ez alapján számos szolgáltatás minősíthető Alap szintre.

4.2.2 Kritikus vagy fontos funkciót támogató IKT szolgáltatás kategóriába javasolt sorolni

Az itt felsorolt esetek mindegyikére jellemző, hogy a termék/szolgáltatás kiváltása piaci termékkel rövid idő alatt gyorsan nem megoldható:

- Minden olyan szolgáltatást, amely használata során nem nyílt, szabványos felülettel integrált, és kiváltása hosszabb ideig tartana.
- Egyedi szoftverfejlesztés szolgáltatás keretében fejlesztett szoftver

4.2.3 Miért nem javasolt bármit besorolni indokolatlanul magasabb szintre?

Az indokolatlanuk kritikus vagy fontossá minősítés ellen az szól, hogy az Alap szinthez képest a következő követelményeket (amelyekhez erőforrást is kell rendelni) rója a pénzügyi szervezetre:

- A 28. cikk (8) szerint a kritikus vagy fontos funkciókat támogató szolgáltatások esetében kilépési stratégiákat is ki kell dolgoznia és be kell vezetnie a pénzügyi szervezetnek, és ezt TESZTELNI is kell.

Ez gyakorlatban azt jelentheti, hogy egy kritikus és fontos funkciót támogató IKT rendszer esetében egy másik szolgáltatótól is szükséges lehet beszerezni és tesztelni is egy ekvivalens szolgáltatást, hogy az arra történő átállás feltételei teljesülhessenek.

- A 29. cikk szerint a kritikus vagy fontos funkciókat támogató IKT-szolgáltatások esetén szükséges az IKT-koncentrációs kockázat értékelése, és az eredményének megfelelő kontroll intézkedések végrehajtása.

4.3 A Microsec zrt. által elvégzett és ügyfelei számára javasolt DORA szerinti termékbesorolás

A Microsec zrt., hogy üzletfelei számára megkönnyítse a DORA megfelelést, elvégezte saját maga is termékei/szolgáltatása DORA szerinti besorolását, melyet javasol használni.

A besorolást az alábbi táblázat tartalmazza.

Kategória	Csoport	Termékek
Alap	Nem integráltalan használt szolgáltatások	Aláíró tanúsítványok Tárolt kulcsos távoli aláíró szolgáltatás (e-Szignó Web vagy e-Szignó Mobile felülettel) Bélyegző tanúsítványok SSL tanúsítványok PSD2 tanúsítványok Időbélyegzés Archiválás OCCR
Alap	Nyílt, szabványos felülettel integrált szolgáltatások	Tárolt kulcsos távoli aláíró szolgáltatás, CSC interfészen
Alap	Nem egyedi fejlesztésű szoftverek	e-Szignó Desktop e-Szignó SDK e-Szignó Server e-Szignó Preserver e-Szignó Autosigner Client|Service Microsigner Microsigner SDK e-Szignó Web on-premise MicroCA/MicroAC Suite e-Szignó Scan & Sign
Kritikus vagy fontos funkciót támogató IKT szolgáltatás	Nem nyílt, szabványos felülettel integrált szolgáltatás (A kiváltása hosszabb ideig tartana.)	Tárolt kulcsos távoli aláíró szolgáltatás, a pénzügyi szervezetnél telepített e-Szignó Web alkalmazással (aláíró felülettel)

4.4 További segédlet a DORA szerinti előzetes kockázatértékeléshez és az átvilágításhoz

A pénzügyi szervezett számára a 2024/1773/CID 5. cikke szerinti szükséges előzetes kockázatértékelés, valamint a 6. cikk szerinti átvilágítás a harmadik feles IKT szolgáltatókkal kapcsolatosan.

Ezen feladatok megkönnyítéséhez összegyűjtöttük az alábbi táblázatba a Microsec bizalmi szolgáltatásával kapcsolatosan az előre megválaszolható kérdésekre a válaszokat.

Röviden összefoglalva: a bizalmi szolgáltatások esetében javasoljuk a pénzügyi szervezetek felé, hogy a kockázatértékeléshez és az átvilágításhoz használják fel tanúsításainkat, mint harmadik féltől származó vizsgálat eredményét.

Jogszabályi szakasz	**Vizsgálandó rész**	**Válasz**	**Igazolás**
5. cikk (2) a)	[A kockázatértékelésnek figyelembe kell vennie IKT-szolgáltatásokból eredő kockázatokat, többek között] működési kockázatok;	Lásd 6. cikk (1) b) és 5. cikk (2) b)	-
5. cikk (2) b)	[A kockázatértékelésnek figyelembe kell vennie IKT-szolgáltatásokból eredő kockázatokat, többek között] jogi kockázatok;	A Szolgáltató bizalmi szolgáltatóként kötelezett, hogy a 24/2016 BM. rendelet 5. §-a szerint és célokra rendelkezzen felelősségbiztosítással, valamint a Szolgáltató megszűnésével kapcsolatos kockázatokra a 19-22. § szerint pénzügyi garanciával.	Mivel a tanúsítások lefedik ezek vizsgálatát, a Szolgáltató ezen követelménynek történő megfelelőségének ellenőrzésére az évenkénti tanúsítási dokumentumainak ellenőrzése javasolt. Lásd 6. cikk (1) a) 2-nél.
5. cikk (2) c)	[A kockázatértékelésnek figyelembe kell vennie IKT-szolgáltatásokból eredő kockázatokat, többek között] IKT-kockázatok;	Lásd 6. cikk (1) b)	-

Jogszabályi szakasz	Vizsgálandó rész	Válasz	Igazolás
5. cikk (2) d)	[A kockázatértékelésnek figyelembe kell vennie IKT-szolgáltatásokból eredő kockázatokat, többek között] reputációs kockázatok;	Lásd 6. cikk (1) a) 1	-
5. cikk (2) e)	[A kockázatértékelésnek figyelembe kell vennie IKT-szolgáltatásokból eredő kockázatokat, többek között] a bizalmas vagy személyes adatok védelméhez kapcsolódó kockázatok;	A Szolgáltató bizalmi szolgáltatóként az adatokat a Dáptv. 88. § (1) előírásai szerint kezeli, őrzi meg, és törli.	Mivel a tanúsítások lefedik ezek vizsgálatát, a Szolgáltató ezen követelménynek történő megfelelőségének ellenőrzésére az évenkénti tanúsítási dokumentumainak ellenőrzése javasolt. Lásd 6. cikk (1) a) 2-nél.
5. cikk (2) f)	[A kockázatértékelésnek figyelembe kell vennie IKT-szolgáltatásokból eredő kockázatokat, többek között] az adatok rendelkezésre állásával kapcsolatos kockázatok;	Lásd 5. cikk (2) e)	-
5. cikk (2) g)	[A kockázatértékelésnek figyelembe kell vennie IKT-szolgáltatásokból eredő kockázatokat, többek között] az adatkezelés és az adattárolás helyéhez kapcsolódó kockázatok;	A Szolgáltató adatkezelésének országai: Magyarország, Spanyolország	Az Adakezelési tájékoztató tartalmazza ezt: https://www.microsec.hu/api/?func=cms.media&file=/pdf/microsec-adatkezelesi-tajekoztato-v1.14.pdf
5. cikk (2) h)	[A kockázatértékelésnek figyelembe kell vennie IKT-szolgáltatásokból eredő kockázatokat, többek között] a harmadik fél IKT-szolgáltató helyéből eredő kockázatok;	A Szolgáltató telephelyének országa: Magyarország.	A cégnyilvántartásból ellenőrizhető: https://www.e-cegjegyzek.hu/

Jogszabályi szakasz	Vizsgálandó rész	Válasz	Igazolás
6. cikk (1) a) 1	Rendelkezik-e üzleti hírnévvel?	Igen, a Szolgáltató 40 éves és több mint 20 éve nyújt bizalmi szolgáltatásokat.	https://www.microsec.hu/hu/cegtortenet
6. cikk (1) a) 2	[Rendelkezik-e] megfelelő képességekkel, szakértelemmel és kellő pénzügyi, humán és technikai erőforrásokkal, információbiztonsági előírásokkal, megfelelő szervezeti felépítéssel, kockázatkezeléssel és belső kontrollokkal	A Szolgáltatóra az eIDAS és a Dáptv. továbbá a vonatkozó szabványok kifejezetten előírásokat támasztanak ezekre vonatkozóan, ezek alapján évente megfelelőség értékelésre kerül A Szolgáltató továbbá ISO 9001 és ISO 27001 tanúsításokkal is rendelkezik. Ezen felül a Szolgáltató tovább alanya a NIS2 tanúsításnak, amely hamarosan lehetségessé válik	A Szolgáltató ezen követelménynek történő megfelelőségének ellenőrzésére az évenkénti tanúsítási dokumentumainak ellenőrzése javasolt, mely folyamatosan elérhető az alábbi linkeken: **eIDAS szerinti megfelelőség értékelés** https://e-szigno.hu/eidas-megfeleles **ISO 9001 és ISO 27001 tanúsítások** https://www.microsec.hu/hu/minosegbiztonsag-es-audit **NIS2 tanúsítás** https://www.microsec.hu/hu/minosegbiztonsag-es-audit

Jogszabályi szakasz	Vizsgálandó rész	Válasz	Igazolás
6. cikk (1) a) 3	[Rendelkezik-e] IKT-szolgáltatások megbízható és professzionális nyújtásához szükséges engedélyekkel vagy regisztrációval	A Szolgáltató bizalmi szolgáltatóként nyilvántartásba vett az NMHH-nál. A Szolgáltató NIS2/kiberbiztonsági törvény alanyként nyilvántartásba vett az SZTFH-nál.	A Szolgáltató ezen követelménynek történő megfelelőségének ellenőrzésére a nyilvántartások ellenőrzése javasolt: **NMHH** https://esign.nmhh.hu/bszny/ **SZTFH** Jelenleg nem ismert kereshető nyilvántartás.
6. cikk (1) b)	képes-e arra, hogy nyomon kövesse a releváns technológiai fejleményeket, azonosítsa az IKT-biztonsággal kapcsolatos legfontosabb gyakorlatokat, és adott esetben alkalmazza azokat annak érdekében, hogy a digitális működési rezilienciára vonatkozóan hatékony és megbízható keretet biztosítson;	A Szolgáltató bizalmi szolgáltatóként kötelezett arra, hogy a technológia fejleményeket kövesse. A bizalmi szolgáltatásokra előírt az üzletmenet folytonossági tervek létezése és tesztelése, valamint a penetrációs és sérülékenység tesztelés.	Mivel a tanúsítások lefedik ezek vizsgálatát, a Szolgáltató ezen követelménynek történő megfelelőségének ellenőrzésére az évenkénti tanúsítási dokumentumainak ellenőrzése javasolt. Lásd 6. cikk (1) a) 2-nél.

5 Dokumentum verzió kezelés

Verzió	Dátum	Módosítás
V1.0	2024-11-26	Első verzió
V1.1	2024-12-03	A besorolásból még hiányzó termékek hozzáadása
V1.2	2025-05-21	Frissítés
V1.3	2025-10-30	NIS2 és Adatrendelet kiegészítések