A fizetési rendszert működtető pénzügyi vállalkozás, a hitelintézettel egyenértékű prudenciális szabályozásnak megfelelő pénzügyi vállalkozás, valamint az olyan pénzügyi vállalkozás, amelyre az összevont alapú felügyelet kiterjed

INFORMATIKAI ENGEDÉLYEZÉSE

A működéshez szükséges tárgyi feltételek és biztonsági követelmények folyamatos biztosítása érdekében az IKT-rendszer megfelelőségét alátámasztó dokumentumok, melyekkel a pénzügyi vállalkozás igazolja, hogy megtervezte, beszerezte és bevezette azon IKT-biztonsági stratégiákat, szabályzatokat, eljárásokat, protokollokat és eszközöket, amelyek célja biztosítani az IKT-rendszerek rezilienciáját, folytonosságát és rendelkezésre, továbbá fenntartani az adatok rendelkezésre állására, hitelességére, integritására és bizalmas kezelésére vonatkozó magas szintű normákat.

Ennek érdekében szükséges az *„Európai Parlament és a Tanács a pénzügyi ágazat digitális működési rezilienciájáról, valamint az 1060/2009/EK, a 648/2012/EU, a 600/2014/EU, a 909/2014/EU és az (EU) 2016/1011 rendelet módosításáról szóló 2022. december 14-i 2022/2554 (EU) rendelete”* **(DORA),** valamint annak 15. cikkében foglalt felhatalmazáson alapuló

„az (EU) 2022/2554 európai parlamenti és tanácsi rendeletnek az IKT-kockázatkezelési eszközöket, módszereket, folyamatokat és szabályzatokat, valamint az egyszerűsített IKT-kockázatkezelési keretrendszert meghatározó szabályozástechnikai standardok tekintetében történő kiegészítéséről szóló (EU) 2024/1774 rendelet” **(RMF RTS)** alapján az IKT-rendszerek biztonságával kapcsolatos irányítási, szervezeti és szabályozási rendszer, valamint a működésbiztonság bemutatása az alábbi dokumentumokkal:

a.) a Digitális működési rezilienciára vonatkozó stratégia és éves informatikai beruházási és költség tervek a DORA 6. cikk (8) és a 6. cikk (2) g) pontja szerint;
b.) Szervezeti és működési szabályzat a DORA 4. cikk (1)-(2) és a DORA 5. cikk (2) c) pontja szerint;
c.) az „(EU) 2022/2554 európai parlamenti és tanácsi rendeletnek a harmadik fél IKT-szolgáltatók által nyújtott, kritikus vagy fontos funkciókat támogató IKT-szolgáltatások igénybevételéről szóló szerződéses megállapodásokra vonatkozó szabályzat tartalmi elemeit meghatározó szabályozástechnikai standardok tekintetében történő kiegészítéséről szóló(EU)2024/1773 rendelet” alapján a harmadik fél IKT-szolgáltató tevékenységét szabályozó szerződések vagy megállapodások, továbbá az ilyen szolgáltatások igénybe vételét biztosító belső eljárásrendek; a kockázatok kezelését és a szolgáltatásfolytonosságot, valamint az elszámoltathatóságot biztosító technológiai és szervezési megoldások ismertetése, továbbá a harmadik fél IKT-szolgáltatók szerződései és nyilvántartása DORA 8. cikk (5) bekezdés szerint;
d.) az IKT-vonatkozású funkciók egyértelmű kijelölését biztosító dokumentumok (adatgazda és rendszergazda kijelölések és az informatikai biztonsági felelős kijelölése és a harmadik fél IKT-szolgáltatók-felvigyázásáért felelős személy megbízása) a DORA 5. cikk (2) c) pontja és a (3) cikke alapján;
e.) az IKT-kockázatkezelési keretrendszerére ellenőrök általi, rendszeres, a pénzügyi szervezetek ellenőrzési tervével összhangban elkészített belső ellenőrzési terv és az IKT-ellenőrzést végző belső ellenőröknek megfelelő szakértelmét igazoló dokumentumok a DORA 6. cikk (6) bekezdése alapján;

f.) Üzleti hatáselemzés (BIA) DORA 11. cikk (5) bekezdés szerint;
g.) adatvagyonleltár a DORA 8. cikke szerint;
h.) Az IKT-kockázatkezelési keretrendszer részeként kialakított stratégiák, szabályzatok, eljárások, IKT-protokollok DORA 6. cikk és az RMF RTS 1-26 cikkek szerint.
i.) az IKT-rendszerek létrehozását célzó projektmenedzsmentre vonatkozó szabályozás és az alkalmazott biztonsági elvek leírása a DORA 5. cikke és az RMF RTS 15. cikke szerint;

j.) a kérelmező IKT-eszközeit használó vagy hozzáférő munkavállalók és a harmadik fél IKT-szolgáltató személyzetére vonatkozó követelmények a DORA 5. cikkében és az RMF RTS 19 és 20. cikkben foglalt követelményeknek megfelelően;

k.) a DORA 7. cikk alapján és az RMF RTS szerint kialakított informatikai rendszerek ismertetése az alábbi tartalommal:

i.) az IKT-rendszerek architektúrája és a hálózat elemei,

ii.) a nyújtott üzleti tevékenységeket támogató üzleti informatikai rendszerek,

iii.) a szervezetet és az ügyvitelt támogató informatikai rendszerek (például a számviteli, a törvényes beszámolási rendszerek, a munkaerő-gazdálkodás, az ügyfélkapcsolatok kezelése, az e-mail szerverek és a belső fájlszerverek),

iv.) az engedélyezett külső kapcsolatok típusa (például kapcsolat a partnerekkel, szolgáltatókkal, a csoport más jogalanyaival és távmunkavégzésben dolgozó munkavállalóikkal, ideértve e kapcsolatok jogosságának indoklását),

v.) az i-iv. pontokban felsorolt összes szolgáltatás esetében a bevezetett logikai biztonsági intézkedések és mechanizmusok, ideértve azt, hogy az intézmény az ilyen hozzáférés felett milyen ellenőrzéssel rendelkezik, továbbá az egyes ellenőrzések jellegét és gyakoriságát – például technikai vagy szervezeti, megelőző vagy feltáró, valós időben végzett monitoring vagy rendszeres vizsgálat, a biztonsági berendezések konfigurálása, a kulcsok és az ügyfélazonosító igazolványok létrehozása, a rendszer monitoring, hitelesítés, a kommunikáció titkossága, a behatolások érzékelése; vírusirtó rendszerek és naplók stb. (az

vi.) az informatikai rendszerekhez való belső hozzáférést irányító logikai biztonsági intézkedések és mechanizmusok;

l.) az IKT-kockázatok részletes felmérése, amely kiterjed a harmadik fél szolgáltatókra és valamennyi, a működési környezettől való függőségből eredő kockázatra, továbbá a csalás kockázatára. A bevezetett vagy tervezett kockázatcsökkentő intézkedések részletes bemutatása a DORA 6. cikke és az RMF RTS 1., 3. és 27. cikke szerint;

m.) az IKT-rendszerek vagyonelemeinek nyilvántartási szabályai és az elemek aktuális nyilvántartásai a DORA 8. cikke és az RMF RTS 4-5. cikkei szerint;

n.) az IKT-rendszerek működtetése során alkalmazott megelőző védelmi és biztonsági elvek és megoldások leírása a DORA 9. cikkében foglalt elvárásnak megfelelően az alábbi tárgykörökben és részletezettséggel:

i.) alkalmazott titkosítási és kriptográfiai megoldások (RMF RTS 7. cikk),

ii.) az IKT-rendszerek üzemeltetési eljárásai és azok szabályozása (RMF RTS 8. cikk),

iii.) a kapacitás- és teljesítménymenedzsment eljárások és megoldások ismertetése (RMF RTS 9. cikk),

iv.) a sérülékenységek-, és a javító programok, frissítések kezelésére alkalmazott intézkedések bemutatása (RMF RTS 10. cikk),

v.) az adatok és IKT-rendszerek biztonsági besorolása és a besorolás alapján alkalmazott védelmi intézkedések, valamint az adatok megosztásának, továbbításának és tárolásának szabályai, az adatok tárolási szerkezete és az adatkapcsolatokra alkalmazott biztonsági megoldások ismertetése (RMF RTS 11. cikk),

vi.) a behatolás és az adatokkal való visszaélés elleni biztosítékok részeként alkalmazott naplózási eljárások, protokollok és eszközök ismertetése (RMF RTS 12. cikk),

vii.) a hálózat biztonságos működésének biztosítására vonatkozó eljárások és az adattovábbítás során alkalmazott biztonsági intézkedések és a folyamatok biztonsága érdekében alkalmazott technikai megoldások leírása (RMF RTS 13-14. cikk),

viii.) a kérelmező telephelyének és adatközpontjának fizikai biztonságát szolgáló intézkedések és mechanizmusok, például a belépést ellenőrző rendszer és a környezeti biztonság elemei (RMF RTS 18. cikk),

ix.) a jogosultságok és hozzáférések biztonságos kezelésére és nyilvántartására alkalmazott rendszerek (RMF RTS 20-21. cikk),

x.) az IKT-rendszereket és az azokban kezelt információs vagyonelemeket érintő biztonsági események, incidensek észlelésére, monitorozására, kezelésére és nyomon követésére szolgáló eszközök leírása ((RMF RTS 22. cikk);

o.) a rendellenes tevékenységek észlelésére az eseményekre történő reagálásra alkalmazott rendszerek és eljárások, a DORA 10. cikke és az RMF RTS 12. és 23. cikke szerint;

p.) a szükséges és alkalmazott szolgáltatásfolytonossági, kommunikációs és válságkezelési intézkedések felmérése, szabályozása, a kapcsolódó reagálási és helyreállítási tervek és tesztelési dokumentumok ismertetése, valamint szolgáltatásfolytonossági elvárásokat biztosító műszaki megoldások ismertetése a DORA 11. cikke és az RMF RTS 26. cikke alapján;

q.) a biztonsági mentési szabályzatok és eljárások, visszaállítási és helyreállítási eljárások és módszerek, valamint az eljárások végrehajtását biztosító műszaki megoldások leírása a DORA 12. cikke és az RMF RTS 24-25. cikknek megfelelően;

r.) az (EU) 2022/2554 európai parlamenti és tanácsi rendeletnek az IKT-vonatkozású események és kiberfenyegetések osztályozására vonatkozó kritériumokat, a lényegességi küszöbértékeket és a jelentős eseményekkel kapcsolatos bejelentések részleteit meghatározó szabályozástechnikai standardok tekintetében történő kiegészítéséről szóló, a Bizottság *(EU) 2024/1772* felhatalmazáson alapuló rendelete (2024. március 13.) végrehajtását biztosító szabályozás, folyamatok és rendszereszközök dokumentumai;

s.) az (EU) 2022/2554 európai parlamenti és tanácsi rendeletnek az információ-nyilvántartáshoz kapcsolódó táblák tekintetében történő alkalmazására vonatkozó végrehajtás-technikai standardok megállapításáról szóló, a Bizottság *(EU) 2024/2956* végrehajtási rendelete (2024. november 29.) alapján létrehozott IKT-szolgáltatók nyilvántartása.

A követelményeket a kevesebb mint 10 főt foglalkoztató és 2 millió EUR-t meg nem haladó éves árbevételű és/vagy éves mérlegfőösszegű vállalkozások esetében a DORA és az RMF RTS mikrovállalkozásokra vonatkozó előírásaira tekintettel kell alkalmazni.

2025. január