KPMG

Financial Risk&Regulation

Harmonizált elvárásokat fogalmazott meg a DORA rendelet a pénzügyi szereplők széles körére

Hírlevél – 2023. szeptember

2023. január 16-án hatályosult és 2025. január 17. napjától alkalmazandó a 2022/2554 EU rendelet[1] (továbbiakban DORA), melynek fókuszában a pénzügyi intézmények kiberkockázatainak kezelése és digitális rezilienciájának egységes elvek mentén történő erősítése áll. A DORA rendelet és szabályozáscsomag implementálásával azonban nemcsak a működési biztonság növelhető, hanem a fogyasztói bizalom, valamint a határon átnyúló szolgáltatások hatékonysága is.

Háttér

A pénzügyi rendszer információs, kommunikációs és technológiai (IKT) rendszereinek összekapcsoltsága és kölcsönös függőségei mára azt eredményezik, hogy egy adott intézményből eredő sérülékenység akár az Európai Unió összes intézményének működésére kiható nehézséget okoz és ezzel a betétesek, befektetők pénzügyi rendszerbe vetett bizalmát is megrendíthetik, ami pedig akár bankpánikhoz is vezethet.[2]

A DORA az ilyen helyzetek megelőzésére egy olyan egységes kiberbiztonsági követelményrendszert kíván bevezetni, amely – az adott intézmény méretével, működésével – **arányos és kockázatalapú megközelítésen alapul**, egyben új digitális működési kockázatkezelési keretrendszert ad meg a pénzügyi szféra szereplőire és egyes IKT szolgáltatókra, amely kifejezetten a digitális reziliencia előmozdítását célozza. Jelentősége abban áll, hogy bár épít korábban már elvárt, kialakított kockázatkezelési tevékenységre (mind uniós pl. NIS és NIS 2 irányelvek[3], mind tagállami elvárásokra, nemzetközi IKT standardokra és ajánlásokra, pl. EBA/ESMA/EIOPA iránymutatásokra, és az ezeket átültető tagállami hatósági ajánlásokra), mégis ez az első olyan átfogó szabályozás, amely az EU szintjén, a pénzügyi ágazati szereplők széles körére egységes, harmonizált elvárásokat fogalmaz meg a témában.

A DORA két megközelítést alkalmaz: egyrészt szabályokat alkot a pénzügyi intézményekre, másrészt szabályozza a pénzügyi intézmények számára harmadik félként technológiai szolgáltatásokat nyújtó vállalatok (IKT-beszállítók) működését is. Figyelembe veszi egy pénzügyi intézmény méretét, tevékenységeit, valamint üzleti profilját, és ezeknek megfelelően határozza meg, milyen informatikai kockázatkezelési elvárásoknak kell megfelelni.

A rendelet alanyi hatálya

A rendelet alanyi hatálya gyakorlatilag a teljes banki és neobanki tevékenység-palettát lefedi, mind a pénzügyi szolgáltatások nyújtóira, mind azok IKT-beszállítóira is kiterjed (függetlenül attól, hogy az az ágazati jogszabályok alapján kiszervezésnek minősül, vagy sem), mivel ezen szolgáltatási körökben észlelhetők különösen a megnövekedett digitalizációból eredő kockázatok. Pl. egy elektronikus pénzkibocsátó a szolgáltatásához

1 AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2022/2554 RENDELETE (2022. december 14.) 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

2 Kiberbiztonság: hogyan kezeli az EU a kiberfenyegetéseket? - Consilium (europa.eu)

3 Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/ 1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv)

videós ügyfélazonosítást alkalmaz, amihez külső szolgáltatót vesz igénybe, akinek a rendszeréhez saját rendszerét csatlakoztatja. Így pl. egy felhőre épülő rendszer sérülékenységei esetén nagyszámú személyes adat, köztük a természetes személyek arcmása, hangfelvétele és személyes azonosító adatai, továbbá hozzájuk köthető banktitok, fizetési titok kerülhet illetéktelenek kezébe, vagy e rendszeren keresztül az elektronikus pénzkibocsátó saját rendszerei is sérülékennyé válhatnak, még több személyes adatot és banktitkot veszélybe sodorva.

A fent felsorolt pénzügyi szolgáltatók érintett beszállítói lehetnek pl. a felhőszolgáltatók, szoftverfejlesztési, support vagy digitális szolgálatást (pl. adatelemzés, adatközpont, automata döntéshozatal, adatkezelés) nyújtók, viszont nem tartoznak az alanyi hatály alá a hardver-szolgáltatók, elektronikus hírközlési-szolgáltatók, így pl. telefon- és internet-szolgáltatók. A fenti szabályok alól mentesülnek továbbá a mikrovállalkozások, bizonyos ágazati jogszabályok szerinti kis méretű intézmények, tagállami mentességet élvező, hatály alól kivett intézmények.

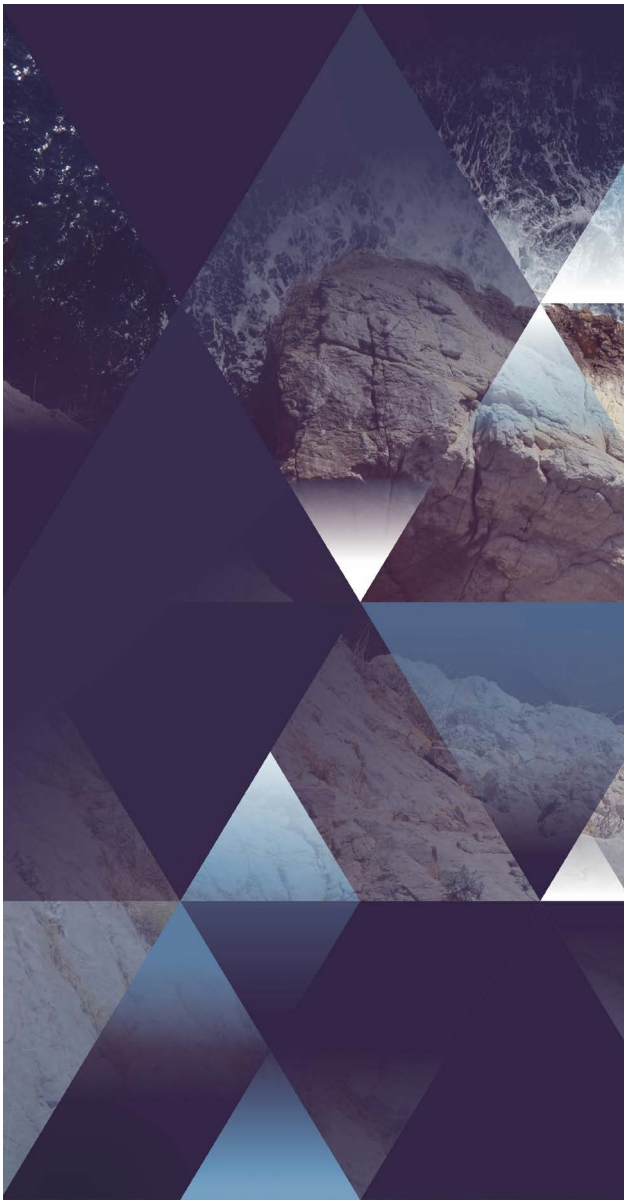
Bár bizonyos pontosító kérdések még tisztázandóak a DORA hatályát illetően (egyes intézmény-típusokat nem nevesít, pl magánnyugdíjpénztárakat), a várakozás az, hogy az alanyi hatály szélesen értelmezendő lesz és vélhetően minél tágabb kört kíván felölelni.

A szabályozott területek

A DORA szabályozás által érintett főbb szabályozási területek: 5 pillér és egy vállalatirányítási blokk köré csoportosíthatóak:

- IKT kockázatkezelés követelményei.
- Digitális működési reziliencia tesztelése.
- Harmadik féltől eredő IKT-kockázatok kezelése, szerződések és felügyeletük (felvigyázási keretrendszer).
- Bejelentések (jelentős IKT események bejelentése és jelentős kiberfenyegetésre vonatkozó önkéntes hatósági értesítés, pénzforgalmi vonatkozású működési vagy biztonsági események hatósági bejelentése).

Információmegosztás (kiberfenyegetésekkel és sérülékenységekkel kapcsolatos információk megosztása).Ezen kívül a vállalatirányítás terén is megfogalmaz a vezető testületekre, vezetők irányítási követelményeire vonatkozó szabályokat.



Korábbi elvárásokra építő szabályrendszer

A DORA egyik legfontosabb követelménye - bár ez nem újdonság -, hogy a hatálya alá tartozó szervezetektől elvárja a megbízható, átfogó és jól dokumentált IKT-kockázatkezelési keretrendszer kidolgozását és beillesztését a vállalkozás kockázatkezelési rendszerébe. Ezen implementált keretrendszerrel - melynek betartását egy, a szervezetben független kontroll funkció ellenőrzi - a pénzügyi szervezeteknek minimalizálniuk kell az IKT-kockázatok hatását.

Új elemként került be a szabályozásba, hogy a kockázatkezelési rendszernek tartalmaznia kell egy **kifejezetten a digitális működési rezilenciára vonatkozó stratégiát is**, konkrét célkitűzésekkel és módszerekkel.

A pénzügyi szervezetek naprakész IKT-rendszereket, -protokollokat és -eszközöket kell fenntartani, melyek arányosak, megbízhatóak, megfelelő kapacitással rendelkeznek, valamint piaci stresszhelyzetben vagy egyéb kedvezőtlen helyzetekben is reziliensek.

A stratégia bevezetését a kockázatok csökkentésére és kezelésére irányuló **védelmi intézkedéseknek** kell követnie. A pénzügyi szervezeteknek olyan folyamatokat és megoldásokat szükséges alkalmazni, melyek garantálják az adattovábbítási eszközök biztonságát, minimalizálják az adatsérülés és -vesztés, a jogosulatlan hozzáférés, valamint az üzleti tevékenységet akadályozni képes technikai hibák kockázatát; megakadályozzák az adatokat érintő incidenseket (rendelkezésre állás, hitelesség és integritás valamint bizalmasság sérülését), továbbá az adatgazdálkodás kockázatainak kezelését, ideértve az emberi kockázatot is.

A pénzügyi szervezeteknek az IKT vonatkozású **események észlelésére, kezelésére és bejelentésére szolgáló folyamatot** kell kialakítaniuk. Egyrészt minden jelentős IKT eseményt és kiberfenyegetést nyilván kell tartaniuk és megadott szempontrendszer szerint osztályozniuk, másrészt megfelelő monitorozási eljárásokat kell kiépíteniük.

A működési reziliencia **tesztelésére ki kell alakítani egy átfogó programot**. Ennek következében az IKT vonatkozású események kezelésére való felkészültség értékelhető, a digitális működési rezilencia gyengeségei és hiányosságai beazonosíthatók lesznek. A teszteket évente, egy független belső vagy külső félnek kell elvégeznie minden fontos funkciót támogató rendszeren.

A DORA kiemelt figyelmet szentel **a (harmadik fél) IKT beszállítók kockázatainak kezelésére**. Egységesíti a szabályokat, valamint az ún. kulcsfontosságú beszállítókra új szabályokat állít fel.

Azt, hogy ki minősül kulcsfontosságú szolgáltatónak, a felügyeleti hatóság állapítja meg, de elsősorban a kritikus vagy fontos funkciót támogató IKT szolgáltatásokat támogató szervezetek eshetnek e körbe. A felügyeleti hatóság ezen szolgáltatók tekintetében egyedi felvigyázási tervet készít a szolgáltató számára, jegyzékbe veszi ezeket, valamint ellenőrzési joggal rendelkezik felettük.

A felügyeleti hatóság annak megállapítása során, hogy mely szolgáltató minősül kulcsfontosságúnak, számos szempontot mérlegel: így például figyelembe veszi a potenciális rendszerszintű hatásokat, amelyek a szolgáltató üzemzavara esetén következnek be, valamint a szolgáltatásnyújtás környezetét, így a felhasználó szervezeteket (ezek számát, jellegét, kapcsolatát, a szolgáltatásaik helyettesíthetőségét), továbbá az érintett tagállamok számát.

A magyar piaci szereplők korábban már az előírások egy részével különböző iránymutatásokban, MNB ajánlásokban találkozhattak, de azok implementálási szintje eleve vegyes képet mutat. Nagyobb és komplexebb működésű, valamint mérettől, komplexitástól függetlenül is az eddig érvényes jogszabályi, felügyeleti elvárásoknak és piaci standardoknak eleve nem teljesen megfelelő vállalatok számára nagyobb erőforrás-igényű projekt indítása válhat szükségessé, hogy elérjék a DORA által elvárt reziliencia-szintet. Fontos kiemelni továbbá, hogy nemcsak a pénzügyi szervezetek saját megfelelése a feladat. A sok IKT-beszállítóval dolgozó pénzügyi szervezetek, pl. bankok, biztosítók számára kiemelten fontos, hogy beszállítóik is elindítsák a megfelelési folyamatot és a saját oldalukon hajtsák végre a szükséges változtatásokat.

DORA szabályozással kapcsolatos szolgáltatásaink

A rendelet 2025. január 17-étől alkalmazandó kötelezően, de a felkészülést javasolt időben elkezdeni. Egyes témaköreit számos, most még csak konzultációs fázisban, vagy még tervezeti fázisban sem lévő RTS és ITS fogja pontosítani, részletezni. Ezek megismeréséig a felkészülés a DORA általános szabályainak, illetve a már létező ESA (és MNB) ajánlásoknak való megfelelés vizsgálatára terjedhet ki, az esetleges hiányok és akciók a részletszabályok ismerete nélkül nagy vonalakban azonosíthatók. Nagy pénzügyi csoportok esetén annak felmérése is megindulhat, hogy a DORA mely elemei igényelnek központi implementációt és melyekben van mozgástér, vagy feladat hazai szinten. Az időben történő felkészülés azért is indokolt, mert több szakterület (pl. működési kockázatkezelés, IT kockázatkezelés, beszerzés, folyamatszabályozás, jog, compliance...) közötti koordinált munkát feltételez. Ezekkel az előkészítő lépésekkel az adott intézmény képessé válhat arra, hogy jó pozícióból tudja megindítani a részletes implementációs projektjét az RTS-ek és ITS-ek kihirdetését követően.

A rendeletnek való megfelelőség fontos pillére a rendszer biztonságtechnikai vizsgálatok elvégzése, amelynek részleteiről az alábbi oldalakon további információt találhatnak: Digital Operational Resilience Act - KPMG Hungary, Kiberbiztonsági tanácsadás - KPMG Magyarország

---

A hírlevél készítésében részt vettek: Glózer-Say Viktória, Kátai Kamilla.

Kontakt:

Rakó Ágnes
Partner
M: +36 70 370 1792
E: agnes.rako@kpmg.hu

Lukács Kornél
Partner
M: +36 70 977 6564
E: kornel.lukacs@kpmg.hu

Szalai Péter
Associate Partner
M: +36 70 370 1739
E: peter.szalai@kpmg.hu

Wieder Gergő
Igazgató
M: +36 70 333 1471
E: gergo.wieder@kpmg.hu

Glózer-Say Viktória
Menedzser
M: +36 70 978 7031
E: viktoria.glozer-say@kpmg.hu

KPMG.hu