KOVÁCS RÉTI SZEGHEŐ
ÜGYVÉDI IRODA

Ezúttal DORA állítja kihívások elé a pénzügyi szervezeteket

Az új uniós digitális pénzügyi csomag részeként, ez év elején lépett hatályba az Európai Parlament és a Tanács 2022/2554 rendelete a pénzügyi ágazat digitális működési rezilienciájáról, azaz a „Digital Operational Resilience Act" (vagyis : DORA).

Az egyre növekvő digitalizáció miatt, a kiberveszélyeknek és a digitális rendszerek időnkénti működési zavarainak egyik legjobban kitett szektor a pénzügyi rendszer. A zavarokra, és a folyamatosan változó, erősödő kiberbiztonsági kockázatokra történő hatékony válaszadás érdekében, a DORA javaslata hangsúlyozza, hogy olyan tartós digitális rendszereket és eszközöket kell létrehozni és karbantartani, amelyek képesek ellenállni a potenciális fenyegetéseknek és minimalizálni digitális rendszerekben rejlő kockázatok negatív hatását.

A rendelet célja tehát, hogy segítsen védelmet nyújtani a kiberfenyegetésekkel, a működési kockázatokkal és más olyan lehetséges zavarokkal szemben, amelyek károsíthatják a pénzügyi stabilitást. Ez nagyon szépen hangzik, **de mit is jelent ez a gyakorlatban?**

Mi az a bizonyos elvárt digitális működési reziliencia?

A DORA fogalommeghatározása szerint, a „digitális működési reziliencia" a pénzügyi szervezet képessége arra, hogy kiépítse, biztosítsa és felülvizsgálja működési integritását és megbízhatóságát azáltal, hogy harmadik fél informatikai szolgáltatók által nyújtott szolgáltatások igénybevételével közvetlenül vagy közvetetten biztosítja azon hálózati és információs rendszerek biztonságának kezeléséhez szükséges informatikai vonatkozású képességek teljes körét, amelyeket a pénzügyi szervezet használ, és amelyek a pénzügyi szolgáltatások folyamatos nyújtását és minőségét támogatják, többek között zavarok fennállásakor is.

Kiket érint a DORA és mi a konkrét feladatuk?

A DORA különféle pénzügyi piaci szereplőit érinti, beleértve a befektetési vállalkozásokat, biztosítókat és viszontbiztosítókat, biztosításközvetítőket, foglalkoztatói nyugellátást szolgáltató intézményeket, de kapcsolódó informatikai vállalkozásokat is.

A pénzügyi szervezeteknek a jövőben rendelkezniük kell egy olyan **belső irányítási és kontrollkerettel, azaz egy kockázatelemzési és kapcsolódó cselekvési tervvel és szervezeti mechanizmussal,** amely biztosítja az informatikai kockázat eredményes és prudens kezelését, a digitális működési reziliencia magas szintjének elérése érdekében. A pénzügyi szervezet vezető testületének kell meghatároznia, jóváhagynia és ellenőriznie az informatikai kockázatkezelési keretrendszerrel összefüggő valamennyi intézkedést, és viselnie a felelősséget azok végrehajtásáért.

Mikortól kell alkalmazni a DORA-t?

Szerencsére rendelkezésre áll még több, mint egy év a felkészüléshez, ugyanis a DORA-t **2025. január 17-től** kell majd alkalmazni. Ugyanakkor, mivel számos, nem pusztán informatikai vonatkozású belső szabályzatot, folyamatot kell megalkotni a megfelelés érdekében, így a felkészülést célszerű mihamarabb megkezdeni.