KOVÁCS RÉTI SZEGHEŐ
ÜGYVÉDI IRODA

Uniós kiberbiztonsági jogalkotás végrehajtási szabályait fogadta el az Országgyűlés

Fontos kötelezettségeket állapít meg a szabályozás a pénzügyi szektor résztvevői számára. A felkészülést minél előbb meg kell kezdenie az érintett vállalkozásoknak.

Áprilisban a Magyar Országgyűlés törvényt fogadott el az uniós DORA (*Digital Operational Resilience Act for the financial sector*, azaz a pénzügyi szektor digitális működési ellenállóképességéről szóló rendelet) végrehajtásáról.

A DORA egységes követelményeket ír elő a pénzügyi szolgáltatók üzleti folyamatait támogató hálózatok és információs rendszerek biztonságával kapcsolatban. A követelmények elsősorban vonatkoznak az információs és kommunikációs technológiák kockázatainak a kezelésére, kiberfenyegetések besorolására, értékelésére és elhárítására, amelyre a vállalkozásoknak belső eljárásrendet is ki kell alakítaniuk. Mindezen túlmenően, a digitális működési ellenállóképesség vizsgálatára teszteket kell alkalmazniuk, és intézkedéseket kell tenniük a kockázatok megfelelő kezelésére.

Összesen 20 féle pénzügyi szolgáltató esik a DORA hatálya alá. Ide tartoznak például hitelintézetek, fizetési szolgáltatók, számlainformációs szolgáltatók, elektronikus pénzintézetek, befektetési vállalkozások, kripto-eszköz szolgáltatók, alapkezelők, biztosítások, viszontbiztosítók, biztosításközvetítők, meghatározott nyugdíjpénztárak és hitelminősítő ügynökségek.

A fenti pénzügyi szolgáltatói körnél, a hazai végrehajtási törvény egy szélesebb személyi hatályt állapít meg. A végrehajtási törvény vonatkozik minden pénzügyi vállalkozásra, minden tőzsdei vállalatra, valamint minden biztosítóra és viszontbiztosítóra, mérettől függetlenül.

A legtöbb pénzügyi vállalkozásnak csak a DORA 16. cikkében előírt egyszerűsített kockázatkezelési keretszabályoknak kell megfelelniük (ez az ún. mini DORA). Többek között a fizetési rendszereket működtető pénzügyi vállalkozások, valamint azon pénzügyi vállalkozások, amelyek ugyanolyan felügyelet alá tartoznak, mint egy hitelintézet, teljes egészében meg kell ugyanakkor feleljenek a DORA 6. cikkében előírt kockázatkezelési keretszabályoknak. A hazai végrehajtási törvény sajátossága, hogy vonatkozik a Magyar Fejlesztési Bankot és a Magyar Export-Import Bankot kiveszi a törvény hatálya alól.

A végrehajtási törvény a Magyar Nemzeti Bankot jelöli ki felügyeleti hatóságnak, a DORA és a végrehajtási törvény alapján fennálló kötelezettségek ellenőrzésére.

A DORA rendelet 19. cikke alapján a végrehajtási törvény előírja, hogy az összes DORA hatálya alá tartozó pénzügyi szolgáltatónak, a jelentős információbiztonsági incidenseket egyidejűleg be kell jelentenie a Nemzeti Kiberbiztonsági Incidenskezelő Központnak (*Computer Security Incident Response Team*, CSIRT) is a NIS2 irányelv alapján. A végrehajtási törvény ugyancsak előírja, hogy a

pénzügyi szolgáltatók jelentős kiberfenyegetés esetén kötelező jelentéstétel mellett a CSIRT-et is értesíteniük kell.

A teljesség érdekében itt utalunk arra, hogy a NIS2 irányelv keretszabályozást határoz meg a kibervédelmi kockázatkezelési és jelentési kötelezettségekkel érintett ágazatokban tevékenykedő vállalkozások számára. Ilyen ágazatok például az energia-, közlekedés-, egészségügy és digitális infrastruktúra területei. Emellett a NIS2 harmonizálja a kibervédelmi követelményeket és a kibervédelmi intézkedések végrehajtását minden tagállamban. E cél érdekében az irányelv a minimum harmonizáció eszközét használva állapít meg egységes minimum szabályokat, valamint hatékony együttműködési mechanizmusokat hoz létre a tagállamok hatóságai között. A NIS2 kiterjeszti a kibervédelmi kötelezettségek alá tartozó ágazatok és tevékenységek listáját, és intézkedéseket tesz az implementáció biztosítása érdekében. A korábbi NIS irányelvhez képest a NIS2 új szabályai hivatalosan létrehozzák az Európai Kibervédelmi Válság Koordinációs Szervezetek Hálózatát (*European Cyber Crises Liaison Organisation Network*, EU-CyCLONe), amely koordinált választ hivatott adni a kiterjedt kibervédelmi incidensekre és válsághelyzetekre.

A NIS2 irányelv főbb pontjai közé tartozik, hogy többek között bővíti a kibervédelmi kötelezettségekkel érintett kört, jelentési kötelezettségek körét meghatározza, további kockázatkezelési és kibervédelmi intézkedéseket ír elő, szigorúbb felügyeleti szabályokat határoz meg és erősíti a vezetői felelősséget, regisztrációs kötelezettségeket határoz meg, és erősíti a hatóságok közti európai együttműködést. A NIS2 irányelvet ez év októberéig kell átültetniük a tagállamoknak nemzeti jogukba.

A DORA-t érintő végrehajtási törvény 2025. január 17-én lép hatályba, azaz a DORA alkalmazásának időpontjával egy időben, ugyanakkor a felkészülést már most érdemes elkezdenie az érintett vállalkozásoknak.