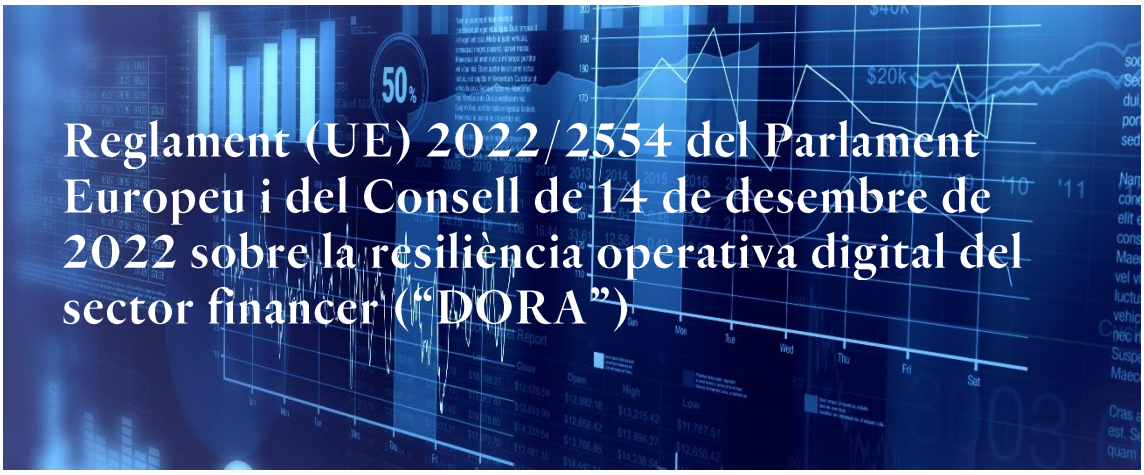
RocaJunyent Informa

Dept. Dret Protecció de Dades, Noves Tecnologies i Ciberseguretat
30 de maig de 2023



El Reglament DORA actualitza i gestiona els requisits de risc de les tecnologies de la informació i la comunicació ("TIC") en tot el sector financer de la UE de manera homogènia, perquè sigui capaç de mantenir la seva resiliència en cas d'una interrupció operativa.

Quan serà aplicable?

El Reglament va entrar en vigor el 16 de gener de 2023 i serà aplicable a partir del 17 de gener de 2025.

Quin és l'àmbit d'aplicació?

DORA tindrà una aplicació molt àmplia i cobrirà les entitats financeres europees autoritzades (com ara institucions de crèdit, firmes d'inversió, entitats de pagament, serveis de report de dades, intermediaris d'assegurances, agències de ràting creditici, etc.), així com a tercers proveïdors de serveis TIC (art. 2 DORA).

Al mateix temps, el Reglament reconeix que existeixen diferències significatives entre les entitats financeres en termes de grandària, perfils empresarials o en relació amb la seva exposició al risc, i estableix un principi de proporcionalitat, de tal manera que imposa obligacions més estrictes a les entitats de major grandària (art. 4 DORA).

Què implica a l'organització de l'entitat?

La plena responsabilitat de l'òrgan de direcció en la gestió del risc TIC de l'entitat financera serà un principi general que es traduirà en un conjunt de requisits específics, com l'assignació d'obligacions i responsabilitats clares per a totes les funcions relacionades amb les TIC, control, formació en TIC, etc. (art. 5 DORA).

Les entitats hauran de disposar d'un marc de governança que garanteixi la gestió efectiva dels riscos TIC, i designar a un responsable dels sistemes (CISO). Trasllada d'aquesta manera l'enfocament dels sistemes de gestió en seguretat de la informació que ja definien normes com la UNE-ISO 27001 per a aquelles empreses que optaven per la certificació.

Com preveu la gestió de riscos?

Les entitats financeres hauran de comptar amb un marc de gestió dels riscos TIC (art.6-16 DORA) complet i sòlid, que cobreixi:

- **Identificació** de les funcions empresarials relacionades amb les TIC i els actius d'informació;
- **Protecció i prevenció** dissenyant i implementant estratègies, procediments, polítiques i eines de seguretat de les TIC;
- **Detecció** de les activitats anòmales relacionades amb les TIC;
- **Resposta i recuperació**, registrant els incidents, garantint la continuïtat de l'activitat, posant en marxa plans de contenció i gestió de crisi i posant a prova periòdicament la seva política de continuïtat de negoci i el seu pla de recuperació;
- **Reduir els temps de recuperació**, restaurant els sistemes TIC després d'un incident amb un temps mínim d'inactivitat i una pertorbació limitada;
- **Aprenentatge i evolució** (tant en quant a les capacitats i recursos com del personal).

En què consisteixen les proves de resiliència operativa?

Aquestes proves consisteixen a comprovar l'estat de preparació dels sistemes de les entitats financeres davant incidents relacionats amb les TIC. Les entitats estaran obligades (art.24-27 DORA) a realitzar aquestes proves amb els sistemes i aplicacions

TIC essencials almenys una vegada a l'any. Es contemplen dos tipus de proves diferents segons la grandària i importància de l'entitat, bàsiques i avançades.

Caldrà notificar els incidents?

Les entitats hauran de registrar els incidents i classificar-los segons els criteris d'importància establerts a DORA (art.17-23 DORA) i només hauran de notificar mitjançant informe a les autoritats competents els incidents relacionats amb les TIC que es considerin greus. Les entitats financeres hauran de presentar informes inicials (primer dia), intermedis (primera setmana) i finals (primer mes) i informar els seus usuaris i clients quan l'incident tingui o pugui tenir un impacte en els seus interessos financers.

Aquestes obligacions de report hauran d'estar coordinades amb altres obligacions de report previstes per altres normes. El reglament preveu la possibilitat que els supervisors europeus desenvolupin un sistema d'estandardització i centralització dels incidents, a través de la creació d'un Hub, si bé els criteris estan encara per definir.

Què implica DORA per als proveïdors TIC?

Els proveïdors TIC (art.28.44 DORA) són companyies que ofereixen serveis digitals i de dades, com serveis en el núvol, software i anàlisi i centres de dades.

DORA parteix del principi general que els riscos relacionats amb els proveïdors han d'estar integrats en el marc de gestió de riscos TIC de cada entitat financera, per la qual cosa aquestes hauran de dur a terme una supervisió constant dels seus acords amb ells. A més:

- DORA faculta a les autoritats competents per a supervisar a aquests proveïdors. Així, es podran designar proveïdors "essencials", en funció de les entitats financeres que depenguin dels seus serveis, que seran supervisats per alguna de les autoritats competents (ABE, AESPJ i AEVM). Aquestes podran sol·licitar informació i realitzar recerques generals i inspeccions in situ. En cas d'incompliment, les autoritats poden imposar multes coercitives als proveïdors.

- Les empreses que desitgin contractar proveïdors TIC establerts en un tercer país i que hagin estat designats com a essencials, només podran fer-ho si aquests han establert una filial a la UE en els últims 12 mesos anteriors a la designació (art.31.12).