COVINGTON

EMEA Tech Regulation: Key Takeaways

NIS2 and the Cyber Resilience Act

What You Need to Know

- In recent years, there has been an uptick in cyber attacks on organizations in Europe and across the world. This has included large ransomware incidents and sophisticated state-sponsored attacks on a range of critical infrastructure and services. In response to this ongoing threat, EU legislators have introduced rules that aim to minimize the likelihood of these attacks from occurring and their economic and social impact.
- **NIS2** will replace the EU's existing (and first) cybersecurity law, the NIS Directive. NIS2 will require organizations across different sectors to ensure that networks and systems they use to deliver services and conduct their activities attain a higher level of cybersecurity. NIS2 is likely to be signed off at EU level in early 2023, after which Member States will have 21 months to transpose it into national law. The obligations will likely begin to apply in 2024 or 2025.
- The **Cyber Resilience Act (CRA)** sets out cybersecurity requirements for a range of hardware and software products placed on the EU market, including smart speakers, games, operating systems, etc. The CRA will likely be agreed by the EU institutions in 2024, with obligations beginning to apply in 2025 or 2026.

For more information, please reach out to Mark Young, Paul Maynard, Anna Sophia Oberschelp de Meneses, or another member of our team.

Mark Young
London
+44 20 7067 2101
myoung@cov.com

Paul Maynard
London
+44 20 7067 2381
pmaynard@cov.com

Anna Sophia Oberschelp de Meneses
Brussels
+32 2 549 5249
aoberschelpdemeneses@cov.com

Why Does It Matter?

- **NIS2** will require companies to put governance structures in place to manage cybersecurity, comply with breach reporting obligations, and monitor supply chains for cybersecurity risk.
  - "Essential entities," including the energy, transport, health, digital infrastructure, and cloud sectors, will be subject to greater scrutiny and upfront regulation. Regulators will be able to perform audits and carry out inspections. Fines are up to €10m or 2% of annual turnover (whichever is higher).
  - "Important entities," including manufacturers of medical devices, chemicals, electronic equipment and social networks, will only be subject to investigation or enforcement where there is evidence of non-compliance. Fines are up to €7m or 1.5% of annual turnover.
- Under the **CRA**, manufacturers of in-scope products will be required to conduct mandatory security assessment requirements, implement vulnerability-handling procedures, and provide necessary information to users. The CRA will apply to products placed on the market in the EU, irrespective of where the products are manufactured. Products designated as critical will be subject to more onerous obligations. The CRA also proposed high fines for non-compliance, up to €15 million or 2.5% of annual turnover.

Why Covington?

Our Cybersecurity practice has unsurpassed experience addressing the most significant cybersecurity matters confronted by commercial enterprises. We are known for our cross-disciplinary approach and providing pragmatic advice on cutting edge issues and compliance with new regulations. We have helped multiple organizations implement cybersecurity and information governance programs and respond to cyber attacks.