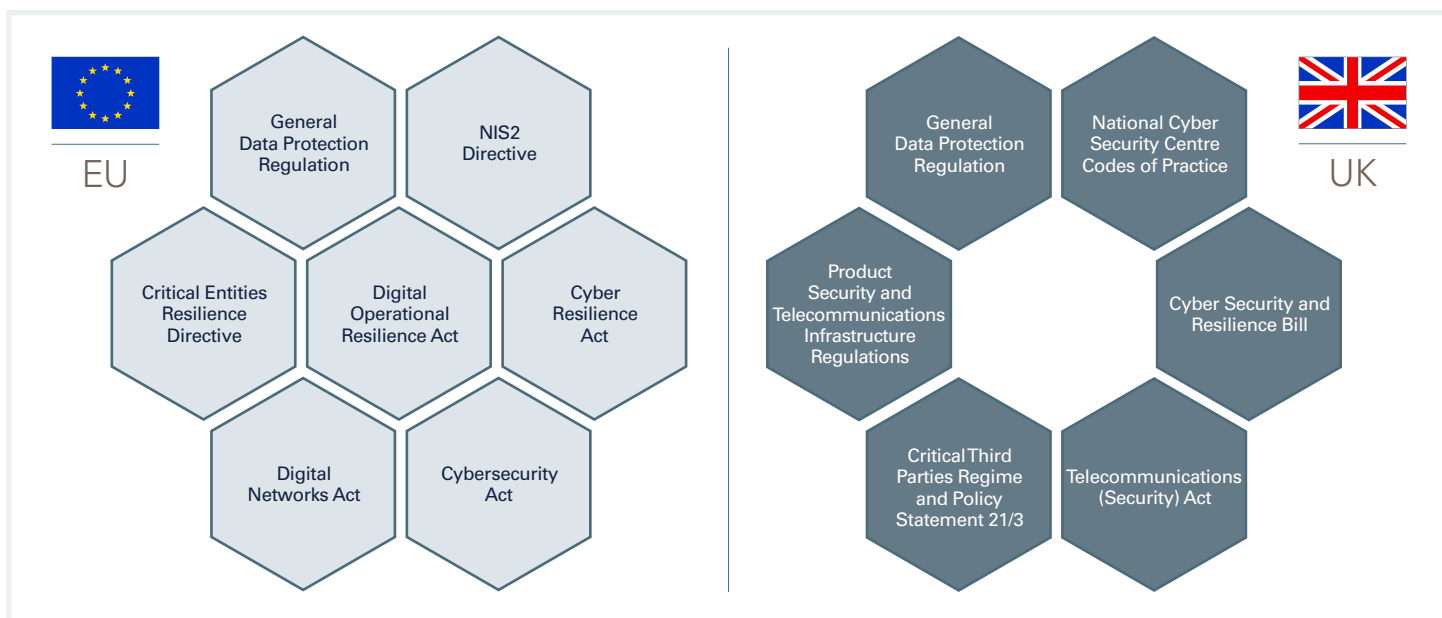


Overview

European Cybersecurity Regulation

In an era of increasing digital threats and rapid regulatory evolution, companies operating in Europe must not only navigate a fragmented and dynamic cybersecurity landscape but also adopt proactive strategies that align compliance with business objectives. Skadden's Cybersecurity and Data Privacy Practice offers clients seamless, strategic and pragmatic guidance across the EU's and U.K.'s intricate regulatory frameworks, leveraging our extensive experience, technical know-how and strong regulator relationships to support clients in regulatory response investigations and respond effectively to incidents while implementing robust governance, compliance and risk mitigation programs.

Navigating Complex Regulations. The EU and U.K. have strengthened their cybersecurity legal frameworks to address the growing risks posed by digital threats, cybercrime and vulnerabilities in critical infrastructure and digital products, leading to a flurry of new laws and compounding the existing patchwork of sector- and country-specific rules. Skadden assists clients — including companies worldwide doing business in Europe or handling data of European citizens — in navigating this multifaceted landscape and in working with cyber regulators. We help companies understand which rules apply to which parts of their business and how they can strategically scope their compliance programs to minimize disruptions.



Understanding the Emerging Landscape. Skadden advises boards and senior management on their legal obligations and personal liability risks under this new raft of laws, helping them to navigate budget constraints with the reality of regulatory requirements.

Incident Response and Crisis Management. To prepare clients to meet the strict notification deadlines imposed by the emerging cybersecurity frameworks — often requiring organizations to alert regulators within 24 hours or less of a cyber incident — Skadden assists clients in developing and stress-testing response plans through tabletop exercises, before an inevitable incident occurs. We also coordinate rapid-response teams to support and coach clients through all aspects of a cyber incident, leveraging privilege protections, where available.

Overview

European Cybersecurity Regulation (continued)



Why Skadden

- **Cross-border cybersecurity leadership:** Skadden’s team adeptly navigates the complex EU and U.K. cybersecurity landscape, providing seamless, practical guidance for multinational clients.
- **Board-level strategic advice:** Our team translates evolving legal requirements into actionable strategies for boards and senior management, helping organizations manage compliance and personal liability risks.
- **Comprehensive lifecycle support:** We deliver end-to-end assistance, from compliance and policy development to incident response and regulator engagement, ensuring clients are prepared for both routine and crisis situations.
- **Network of partners and experts:** Skadden maintains a trusted network of leading forensic investigators, crisis communication specialists, technical experts and other key professionals, enabling us to assemble and coordinate rapid-response teams that support clients through the technical, legal and reputational aspects of cyber incidents.

Relevant Experience

- **Regulatory compliance mapping:** Skadden identifies relevant EU and U.K. cybersecurity laws and sector-specific regulations, assesses their applicability and advises on practical steps to achieve compliance across multiple jurisdictions.
- **Board and senior management training:** We proactively train boards and executive teams on their legal obligations, personal liability risks and best practices for cyber governance under new and emerging laws.
- **Incident response planning and execution:** Our team develops, reviews and stress-tests incident response plans to ensure organizations can meet tight regulatory notification deadlines and effectively manage cyber crises.
- **Breach coaching:** We regularly coach clients through cyber incidents, engaging vendors, managing communications, engaging with the police and regulators and enabling clients to focus attention on maintaining business function to the fullest extent possible,
- **Regulator engagement:** Skadden represents clients in communications with cyber regulators, including responding to inquiries, managing investigations and negotiating favorable outcomes.
- **Policy and program development:** We craft and test internal cybersecurity policies, procedures and training programs, ensuring alignment with evolving legal requirements and industry standards.