EU REPORTING RULES AT A GLANCE

Regime	Who and what does it cover?	Principal reporting trigger	Principal deadline
GDPR	Controllers experiencing a personal data breach.	A personal data breach, unless it is unlikely to result in a risk to individuals' rights and freedoms.	• Notify the supervisory authority without undue delay and, where feasible, within 72 hours of awareness. • Inform affected individuals without undue delay where the breach is likely to result in a high risk, subject to statutory exceptions. • Processors must notify their controller without undue delay.
ePrivacy Directive (as implemented)	Providers of publicly available electronic communications services.	Any personal data breach connected with those services; no risk threshold applies to authority notification.	• Notify the competent national authority without undue delay and, where feasible, within 24 hours of detection. • Where information is incomplete, provide a further notification as soon as possible and within three days of the initial notification (and justify any delay in providing remaining information). • Inform affected subscribers or individuals without undue delay where the breach is likely to adversely affect their personal data or privacy, subject to statutory exceptions.
NIS2 *(See our earlier alert.)*	Essential and important entities in covered sectors.	A significant incident affecting service provision, including one that causes or is capable of causing severe operational disruption, financial loss or considerable harm to others.	• Submit an early warning without undue delay, within 24 hours of awareness, and an incident notification without undue delay, within 72 hours. (For trust service providers, the incident notification deadline is 24 hours.) • Submit a final report generally within one month after the incident notification; ongoing incidents require a progress report followed by a final report.
DORA *(See our earlier alert.)*	In-scope financial entities.	An ICT-related incident classified as **major** under DORA's criteria.	• Notify as early as possible, within four hours of classification and normally no later than 24 hours after awareness. • If classified as major after that 24-hour period, notify within four hours of classification. • Submit an intermediate report within 72 hours after the initial notification, with further updates as required, and a final report within one month after the intermediate report or latest updated intermediate report.

Regime	Who and what does it cover?	Principal reporting trigger	Principal deadline
EU AI Act (high-risk AI systems) *(See our earlier alert.)*	Providers of high-risk AI systems, with related duties for deployers.	A serious incident involving specified harms to people, critical infrastructure, fundamental rights, property or the environment.	• Generally report immediately after establishing a causal link or its reasonable likelihood, and no later than 15 days after the provider or, where applicable, deployer becomes aware. • Report widespread infringements and serious disruption of critical infrastructure immediately, within two days. • Death-related incidents require reporting immediately once a causal relationship is established or suspected, within 10 days. • The relevant high-risk rules apply from December 2, 2027, or August 2, 2028, depending on classification. • Systemic-risk model incidents must be reported without undue delay.
EU AI Act (general-purpose AI models with systemic risk) *(See our earlier alert.)*	Providers of general-purpose AI models classified as having systemic risk.	Serious incidents relating to the model.	Report relevant information about serious incidents and possible corrective measures to the AI Office and, as appropriate, national competent authorities without undue delay.
Cyber Resilience Act	Manufacturers of in-scope products with digital elements made available in the EU.	An actively exploited vulnerability in the product or a severe incident affecting its security. Personal data need not be involved.	• Submit an early warning without undue delay, within 24 hours of awareness, and a fuller notification without undue delay, within 72 hours. • For vulnerabilities, submit a final report within 14 days after a corrective or mitigating measure becomes available. • For severe incidents, submit a final report within one month after the incident notification. Inform affected users—and, where appropriate, all users—of the event and necessary mitigation or corrective measures without undue delay.