Requirements in the European Union

Who needs to report?	What needs to be reported?	By when?	By whom?
General Data Protection Regulation (GDPR) (Articles 33 and 34 of Regulation (EU) 2016/679)			
Data controllers	Personal data breaches unless unlikely to result in a **risk** to the rights and freedoms of individuals	Within 72 hours of becoming aware	Relevant data protection supervisory authority
	Personal data breaches that are likely to result in a **high risk** to the rights and freedoms of individuals	Without undue delay	Data subjects (with limited exceptions)
European Electronic Communications Code (EECC) (Articles 40-41 of Directive (EU) 2018/1972)			
Providers of public electronic communications networks and services	Security incidents that have had a significant impact on the operation of networks or services	Without undue delay	National competent authority
	If there is a **particular and significant threat** of a security incident		Users potentially affected by such a threat
NIS2 Directive (Article 23 of Directive (EU) 2022/2555)			
Essential and important entities	Any incidents that have a significant impact on the provision of services	Without undue delay	Computer Security Incident Response Team (CSIRT) or, where applicable, the relevant competent authority
	An **early warning notification** of the incident	Without undue delay and in any event within 24 hours of becoming aware	
	An incident notification updating the information referred to in the early warning	Without undue delay and in any event within 72 hours of becoming aware	
	Upon the request of a CSIRT or the competent authority, an **intermediate report** on relevant status updates	On request	
	A final report	Not later than one month after the submission of the incident notification above	
	If the incident is ongoing at the time of the submission of the final report above, a **progress report** at that time and a final report	Within one month of the handling of the incident	
Essential and important entities	Significant incidents likely to adversely affect provision of those services (where appropriate) and in the event of any significant cyber threat, potential response measures and, where appropriate, the nature of the threat	Without undue delay	Recipients of services
Cyber Resilience Act (CRA) (Articles 13, 14 and 24 of Regulation 2024/2847)			
Manufacturers of products with digital elements	**From 11 September 2026** **Any** actively exploited vulnerabilities in the product with digital elements An **early warning notification** of an actively exploited vulnerability	Without undue delay and in any event within 24 hours	To the CSIRT designated as coordinator and to the European Union Agency for Cybersecurity (ENISA) via the single reporting platform established under Article 16
	A **vulnerability notification** (unless information already provided)	Without undue delay and in any event within 72 hours of becoming aware	
	A **final report** (unless information already provided)	No later than 14 days after a corrective or mitigating measure is available	
	From 11 September 2026 Any **severe incident** having an impact on the security of the product with digital elements An early warning notification of a severe incident	Without undue delay and in any event within 24 hours	The CSIRT and ENISA via the single reporting platform established under Article 16
	An **incident notification** (unless information already provided)	Without undue delay and in any event within 72 hours of becoming aware	
	A **final report** (unless information already provided)	Within one month after the submission of the incident notification above	
	An **intermediate report**	On request	
	From 11 December 2027 The existence of a vulnerability in a component	On identification	The person or entity manufacturing or maintaining the component
	From 11 December 2027 An exploited vulnerability or severe incident having an impact on the security of the product with digital elements	After becoming aware	Impacted users and, where appropriate, all users
Open-source software stewards – **from 11 September 2026**	Any actively exploited vulnerability contained in the product with digital elements to the extent the open-source software steward is involved in its development, and any severe incident having an impact on the security of the product with digital elements to the extent that severe incidents having an impact on products with digital elements affect network and network information systems provided by the open-source software stewards for the development of such products	On becoming aware	The CSIRT and ENISA
	An exploited vulnerability or severe incident having an impact on the security of the product with digital elements to the extent that severe incidents having an impact on products with digital elements affect network and network information systems provided by the open-source software stewards for the development of such products	After becoming aware	Impacted users and, where appropriate, all users
Digital Operational Resilience Act (DORA) (Articles 19 of Regulation (EU) 2025/301, supplementing Articles 17-19 of Regulation (EU) 2022/2554). Requirements as to timing are contained in Article 5 of Commission Delegated Regulation (EU) 2025/301			
Financial entities	Major ICT-related incidents	As early as possible and within four hours from the moment of classification of the incident as major, but no later than 24 hours from the moment of becoming aware	The relevant competent financial supervisory authority
	An **intermediate report** after the initial notification, as soon as the status of the original incident has changed significantly or the handling of the major ICT-related incident has changed based on new information available Followed, as appropriate, by **updated notifications** every time a relevant status update is available, as well as upon a specific request of the competent authority	Intermediate reports within 72 hours from the submission of the initial notification, even where the status or the handling of the incident have not changed	
	An **updated intermediate report**, in any case when regular activities have been recovered	Without undue delay	
	A **final report** when the root cause analysis has been completed, regardless of whether mitigation measures have already been implemented, and when the actual impact figures are available to replace estimates	No later than one month from the submission of the intermediate report or the last updated intermediate report	
	Major ICT-related incident having an impact on the financial interests of clients/significant cyber threat		Clients/potentially affected clients
Critical Entities Resilience Directive (CER) (Article 15 of Directive 2022/2557)			
Critical entities	Incidents that significantly disrupt or have potential to significantly disrupt the provision of essential services	Without undue delay	Competent authority
	An **initial notification** (unless operationally unable to do so)	Within 24 hours of becoming aware	
	A **detailed report** (where relevant)	Within one month	