Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. – Project: 101190180.

# CYBER RESILIENCE ACT

## CRA & other EU Regulations

September 2025

Digital Innovation Hub Trakia

OSCRAT
Open-Source Cyber Resilience Act Tools

# CRA & other EU Regulations

**CRA**

**Product**

with Digital Elements

**NIS2**

**Organizations**

(Essential & Important entities)

**DORA**

**Financial Sector**

(banks, insurers, ICT providers)

**GDPR**

**Personal Data**

processing organization

# CRA & OTHER EU REGULATIONS

The big picture is that these regulations are not competing with each other — they are complementary. Taken together, they form a comprehensive EU digital resilience framework.

| Regulation | Scope | Main Obligations | Overlap with CRA |
|---|---|---|---|
| **CRA** | **Products** with digital elements (hardware, software, IoT) | Cybersecurity & risk management, secure by design & by default, CE marking, vulnerability handling, incident reporting to ENISA | Risk management, security by design, vulnerability handling, incident reporting |
| **NIS2** | Essential & important **entities** (energy, telecom, digital infra, etc.) | Risk management, incident reporting, supply chain security, governance | Risk management, incident reporting, vulnerability disclosure |
| **DORA** | **Financial** sector (banks, insurers, ICT providers) | ICT risk management, resilience testing, outsourcing oversight, incident reporting | ICT risk management, incident reporting, vulnerability disclosure |
| **GDPR** | All organisations processing personal **data** | Lawful processing, data subject rights, security of processing, breach notification | Security by design, breach/incident reporting |

# INCIDENT REPORTING OBLIGATIONS

The important point is that across all these frameworks the principle is the same: quick notification, structured updates, and a final report to ensure transparency and trust.

| Regulation | Initial Notification | Intermediate / Follow-up | Final Report | Reporting Authority |
|---|---|---|---|---|
| **CRA** | **24h** (for actively exploited vulnerabilities or security incidents) | **72h** details | Incidents: within **1 month** Vulnerabilities: within **14 days** after release of patch/fix | ENISA (EU vulnerability hub) |
| **NIS2** | **24h** early warning | **72h** incident notification | **1 month** final report | National CSIRT / competent authority |
| **DORA** | within 4h of classification as major ICT incident; no later than **24h** after becoming aware | Within **72h** after initial | Within **1 month** after the interim (or last updated) report | National Financial Supervisory Authority - shared with ESAs (EBA/ESMA/EIOPA) |
| **GDPR** | --- | **72h** notification of personal data breach | --- | Data Protection Authority |

# THANK YOU

FOR YOUR ATTENTION

September 2025


**Sashka Boncheva**

**m: +359 888 800 222**

s.boncheva@dihtrakia.org



Digital Innovation Hub
Trakia