Breach reporting duties: UK and EU

Telecoms | Data | Payments

Cross-cutting data protection and sector security regimes | June 2026

UK

CROSS-CUTTING: DATA PROTECTION (ALL DATA CONTROLLERS)

UK GDPR Articles 33 and 34

Notify the ICO within 72 hours of awareness, unless unlikely to result in a risk to individuals.
Tell affected individuals where the risk is high.
One regulator, one online reporting service.

SECTOR SECURITY AND INCIDENT REPORTING

Telecoms

Personal data breaches: PECR reg 5A, every breach to the ICO, 72 hours, no risk threshold.
Security compromises: CA 2003 s.105K (TSA 2021), to Ofcom as soon as reasonably practicable.

Essential and digital services

NIS Regulations 2018, regulations 11 and 12.
Significant impact (substantial impact for digital service providers): 72 hours to the competent authority; the ICO for digital service providers.

Financial services

FCA SUP 15.18 (Policy Statement PS26/2).
Operational incident meeting a threshold: report within 24 hours of that determination.
In force 18 March 2027.

EU

EU GDPR Articles 33 and 34

Notify the supervisory authority within 72 hours. Lead supervisory authority for cross-border breaches; every affected DPA for non-EEA controllers.
EDPB common template: consultation to 5 August 2026.

Telecoms

Personal data breaches: ePrivacy Directive and Regulation 611/2013, to the national authority within 24 hours.
Security incidents: moved into NIS2 (EECC Articles 40 and 41 repealed, 18 October 2024).

Essential and important entities

NIS2 (Directive (EU) 2022/2555), Article 23.
Significant incident: early warning within 24 hours, then notification within 72 hours, then final report within one month.

Financial services

DORA (Regulation (EU) 2022/2554), Article 19.
Major ICT-related incident: staged initial, intermediate and final reports to the national competent authority.

One incident can engage several regimes. No notification substitutes for another.

BRATBY LAW
bratby.law | rob@bratby.law | +44 77 3831 2629