General Data Protection Regulation (GDPR)

To enter in to EU law on 25th May 2017

Glossary and references

Updated: 20th October 2017

Glossary

BCR / Binding Corporate Rules: a set of internal rules (e.g. a Code of Conduct) adopted by multinational companies which define their global policy towards international transfers of personal data to entities located in countries which do not provide an adequate level of protection.

Breach / Data Breach: The accidental or malicious theft, sharing, unauthorised processing, or loss / deletion of personal data. All data breaches must be recorded; those posing a risk to data subjects' rights and freedoms (e.g. leaking of sensitive personal data, or that may lead to identity theft or fraud) must be reported to the data controller's supervisory authority within 72 hours of detection.

Consent: A specific, informed, and unambiguous indication of the data subject's wishes in relation to providing personal data to a Controller.

Controller / Data Controller: An organisation that collects personal data and decides how and for what purpose it will be processed. The Controller is ultimately responsible for ensuring that processing is carried out in compliance with the GDPR. If a Controller also processes any personal data that it collects, it is both a Controller and Processsor.

Cyber incident: Any event that leads to, or may lead to, a data breach, e.g. hackers gaining access to a Processor's systems.

DPIA: Data Protection Impact Assessment. An analysis to be carried out prior to processing that describes the nature of the processing (including necessity and proportionality) and any associated risks to data subjects' rights and freedoms.

DSAR: Data Subject Access Request. One of the rights of a data subject under GDPR, this entitles a subject to request a machine-readable record of all data a Controller and / or Processor holds on them.

DPO: Data Protection Officer. A required post for organisations that handle sensitive personal data, and/or where processing special categories of personal data.

EDPB: European Data Protection Board. A pan-EU body that ensures consistency of how GDPR is interpreted.

ISO27001: A framework for information security management that may prove useful in conducting a Privacy Impact Assessment.

Minimization / Data Minimization: The practice of only collecting personal data that is specifically required to carry out processing (e.g. not collecting date of birth if it does not serve a specific and necessary purpose to the Controller).

Penalty: Fines that may be levied for non-compliance with GDPR. Two tiers exist: €10m or 2% of global annual turnover; and €20m or 4% of global annual turnover. In both tiers, the largest sum will be sought (e.g. a lower-tier fine applied to a company with €5m global annual turnover would be €10m; if that same company had a global annual turnover of €800m, the fine would be €16m).

Personal Data: Any data or information which, alone or in aggregate, can unambiguously identify an individual data subject, e.g. email address, IP address, name, job title, physical address, telephone number.

PIA: Privacy Impact Assessment. Another term for DPIA.

Processor / Data Processor: An organisation that processes personal data on behalf of a Controller. Processors must also adhere to GDPR and are responsible for any data breaches or unlawful processing of personal data that might occur in relation to their handling of data provided by a Controller.

Special categories: A subset of personal data that is associated with high risk to data subjects' rights and freedoms. Includes race and ethnic origin; biometric and genetic data; information relating to health, sex life and sexuality; political opinions, religious and philosophical beliefs; trade union membership.

Subject / Data Subject: A natural person (e.g. living citizen) residing within the EU. Note: Data relating to deceased individuals is out of scope of the GDPR.

Supervisory Authority: The organisation within a specific territory or region that enforces compliance with GDPR, conducts audits of ControlelIrs / Processors, and levies fines for non-compliance where required – e.g. the Information Commissioner's Office (ICO) in the UK.

Useful links

Full text of GDPR: http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

Article 29 Working Party guidelines on DPIAs and establishing whether processing is likely to result in 'high risk' to data subjects' rights and freedoms: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137

DSAR 'nightmare scenario' (useful in assessing how your organization might need to update systems and processes to answer a full DSAR): https://www.linkedin.com/pulse/nightmare-letter-subject-access-request-under-gdpr-karbaliotis/

ICO guidance on preparing GDPR-compliant privacy notices: https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/privacy-notices-under-the-eu-general-data-protection-regulation/

ECJ guidance on Binding Corporate Rules: http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/index_en.htm