RSA

GDPR GUIDANCE

In conjunction with
Cyber Protection from RSA

THE PHILOSOPHY OF GDPR

The EU General Data Protection Regulation (GDPR 2016/679) came into effect on 25th May 2018.

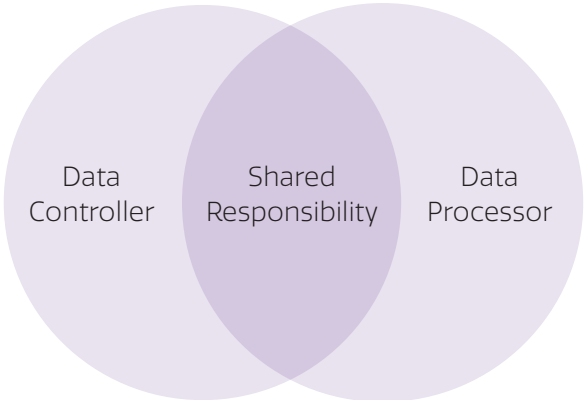
It protects fundamental legal rights for individuals in the European Union in respect of their personal data, no matter which company holds it, or in which country it is held.

GDPR is part of a global legislative drive to put individuals in control of their data, encourage organisations to protect it, and hold them liable if they don't.

It also enhances the power of regulators; in extreme cases they can levy fines of up to 4% of an organisation's annual global turnover.

Who does it apply to?

- Organisations operating within the EU and carrying out data processing
- Organisations outside the EU that offer goods or services to individuals in the EU.
- Data Controllers and Data Processors. A Controller determines the purposes and means of processing personal data. A Processor is responsible for processing personal data on behalf of a controller



What does it apply to?

Personal data, meaning any information relating to an identifiable person who can be directly or indirectly identified.

Therefore personal identifiers such as name, identification number, location data or online identifier can all constitute personal data. GDPR also applies to both automated personal data and manual filing systems.

Personal data that has been pseudonymised can fall within the scope of GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

GDPR applies to personal data referred to as 'special categories of personal data'. The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual.

It's not just about privacy

While 'privacy by design' should be at the heart of a company's Information Security Management System, security is equally important.

Steps to achieve cyber security

Information risk management regime

- Establish an effective governance structure and determine your risk appetite
- Maintain the board's engagement with cyber risk
- Produce supporting information risk management policies.

Areas of consideration for cyber security

- Network security
- Malware prevention
- Monitoring
- Incident management
- User education and awareness
- Home and mobile working
- Secure configuration
- Removable media controls
- Managing user privileges

It's not just about GDPR

In the UK, GDPR has to be read in conjunction with the Data Protection Act 2018 which came into force in May 2018. Not only did this enact GDPR into UK law, it contains details of how it is to be implemented and enhances certain aspects of it.

At the same time, the Network and Information Systems Directive also came into force. This requires Operators of Essential Services to take appropriate measures to manage the risks to the security of network and information systems which support the delivery of essential services.

When you consider that May also saw the final implementation date for the new payment card industry data security standards requirements, it is no wonder companies are struggling to keep up with the new demands.

Structure of GDPR

GDPR consists of two sections. Recitals and Articles. The recitals describe how the regulation works and what it aims to achieve, the articles (of which there are 99) describe the regulations that organisations have to comply with.

Article 5 sets out the general principles that organisations need to comply with and states that 'personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by GDPR in order to safeguard the rights and freedoms of individuals; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.'

Article 32 contains the core information security requirements and begins 'taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing, as well as the risk of the varying likelihood and severity, for the rights and freedoms of natural persons, the controller and processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.'

In other words, organisations must undertake risk assessments from the data subjects' perspective and ensure they maintain the confidentiality, integrity and availability of personal data.

THE SIX PRIVACY PRINCIPLES OF GDPR

1

Lawfulness, fairness and transparency

2

Integrity and confidentiality

3

Storage limitations

4

Purpose limitations

5

Data minimisation

6

Accuracy

GDPR at a Glance

Governance and accountability – Organisations have to implement a formal data protection programme to demonstrate they take data protection seriously and they comply with GDPR.

Rights for data subjects – New and enhanced rights for data subjects including a right to erasure, a right to data portability, a right to challenge some forms of non-essential processing, and a right not to be subject to an automated decision in some circumstances.

Privacy by design – Organisations must take privacy into account when designing new processes or new products and services, they must ensure, by default, that minimal personal data is collected, used and retained.

Privacy risk impact assessment – These are required before processing personal data for operations which are likely to present higher privacy risks.

Appointment of a data protection officer (DPO) – Appointment of a DPO with expert knowledge is mandatory for public authorities. It is also compulsory for organisations heavily involved in the regular and systematic monitoring of data on a large scale, or in processing large amounts of personal data in special categories. These may include insurers, banks and healthcare companies.

Notification of personal data breach – Breaches must be notified to supervisory authorities within 72 hours. If the breach is likely to pose a high risk to the affected individuals' rights and freedom, there is also a duty to notify those individuals of the breach.

Enforcement – Regulators may impose fines up to €20 million or 4% of an organisation's annual global turnover. Regulators also have broad investigative and corrective powers, including the power to undertake on-site data protection audits and issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation – It will be much easier for data subjects who have suffered 'material or non-material damage' to claim compensation against controllers and processors. The inclusion of 'non-material' damage means that individuals can claim compensation for emotional distress even if they can't prove financial loss.

Consumer protection bodies – These can also bring claims on behalf of data subjects, while not a class action right, this nevertheless increases the risk of group privacy claims against organisations.

Cyber Protection from RSA

RSA can provide dedicated insurance to assist in managing the risks. Most importantly, we partner with world-class organisations to provide an end to end solution should the worst happen. For further details please contact us.

RSA contacts

Please contact us directly on
cyberliability@uk.rsagroup.com
or speak to your broker to find out
more about our Cyber Protection offering.

UKC05146