GDPR (EU General data Protection Regulation)

OVERVIEW

The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and aims to increase data privacy to EU citizens, and restructures how many organisations will approach data protection and comes into effect on 25 May 2018.

WHO IT INVOLVES

The GDPR applies to both 'controllers' and 'processors', but different elements of the GDPR can apply to each.

A controller: determines the purposes and means of the processing of personal data

A processor: responsible for processing personal data on behalf of a controller

Where a controller uses a processor there must be a written contract (with specific terms to be included, specified by the GDPR), and they should only use a processor that has 'sufficient guarantees' in place. Sufficient guarantees constitute terms of expert knowledge, reliability and resources to implement measures which meet the requirements of the GDPR. A processor can only act under the instructions of a controller and must also comply directly with GDPR requirements.

APPLICATION

The GDPR applies to personal data, which means any information relating to an identified or identifiable natural person ('data subject'), which can include name, an identification number, location data, and physiological, genetic, mental, economic, cultural or social identity of that natural person.

The GDPR also encompasses special categories of personal data, establishing a higher threshold of protection. This personal data is typically of a sensitive nature and includes race or ethnic origin, political opinions, beliefs, genetic, biometric and health data.

REQUIREMENTS

The GDPR stipulates that data processing of personal data should be lawful, fair and in a transparent manner, for specific and legitimate purposes, processed accurately and kept up to date and in a secure manner, and not keeping the data for longer than is necessary.

It further requires that in order to process personal data, there must be a legal basis under Article 6, defined as follows:

CONSENT –must be clear and concise and kept under constant review. Individuals must also be able to opt-in without having a default consent option, and it must be easy to withdraw consent.

CONTRACT – a contractual obligation, although this must be a necessity and the reasoning behind the necessity must be justifiable.

LEGAL OBLIGATION – data can be processed to comply with common law or statutory obligations, although again this must be a necessity and the reasoning must be justifiable.

VITAL INTERESTS – protection of life with data processing being a necessity. If there is an alternate way of saving life than the Vital Interests basis will not apply; it therefore has very limited scope.

PUBLIC TASKS – data can be processed if it is 'in the exercise of official authority', or to perform a task that is in the public interest. No specific statutory power is needed, but the reason behind the data processing must have a clear, legal basis and, once again, it must be necessary. If there is an alternative way of completing the public task than this basis will not apply.

LEGITIMATE INTERESTS – this is a three-stage test:

1. Purpose: identify a legitimate interest;
2. Necessity: show that data processing is necessary to achieve said legitimate purpose; and
3. Balance: balance the interest against the individual's interests, rights and freedoms. Interests can be personal, commercial or for a wider societal interest.

If an alternative method of achieving the legitimate interest exists, this basis will not apply. Additionally, a record of legitimate interests assessments should be kept. Legitimate interests must also be declared in a privacy notice.

There are two further categories covered under the GDPR; special categories of personal data, and criminal offences data.

Special Categories Data

In order to process special categories of data (defined above), there must be a legal basis under Article 6, as well as satisfying a separate condition for processing special; data under Article 9. This reasoning can include safeguarding rights, provision of health or social care, and social protection law.

Criminal Offences Data

In order to process personal data relating to criminal convictions and offences there must be a legal basis under both Article 6 and Article 10, the latter requiring official authority when processing data in relation to, or keeping a comprehensive register of criminal convictions.

RIGHTS

The GDPR also outlines and extends individual's data protection rights.

BREACH NOTIFICATION – if a breach is likely to "result in a risk for the rights and freedoms of individuals", a notification must be issued within 72 hours of being aware of the breach.

RIGHT TO ACCESS – data subjects have the right to obtain confirmation whether their own personal data is being processed, where, and for what purpose. The controller must provide a copy of this information, for free and in electronic form, to the data subject.

RIGHT TO RECTIFICATION – the data subject has the right to obtain rectification of inaccurate information from the data controller without delay.

RIGHT TO ERASURE (TO BE FORGOTTON) – the data subject has the right to have the controller erase their personal data, and potentially halt third party processing of said data. Reasons could include that that data is no longer relevant, or the subject has withdrawn consent.
Note: Controllers can balance subject's rights with the "public interest in the availability of the data."

RIGHT TO OBJECT – individuals can object to data processing in relation to public or legitimate interests, direct marketing, or scientific, historical or statistical purposes.

DATA PORTABILITY – a data subject has the right to receive personal data which concerns them in a "commonly used and machine-readable format."

PRIVACY BY DESIGN – an individual has the right to have their data protected from the onset; meaning that there must be "appropriate technical organisation measures" implemented, only absolutely necessary data is held, and that there is limited access to said data.

DATA PROTECTION OFFICERS (DPO) – an internal record keeping requirement displaces the previous system of submitting notifications externally. A DPO appointment will only be mandatory for controllers and processors requiring regular monitoring of a large scale of data subject, special categories of data, or data relating to criminal convictions and offences.

HOW TO COMPLY

In order to show compliance to the GDPR, as well as observing the above rights and requirements, a company should also choose to implement appropriate technical

and organisational measures to ensure and to be able to demonstrate that data processing is in accordance with the regulation, with the same being reviewed and updated where necessary.

Data Protection policies could include:

- Staff training;
- Internal audits, reviews or HR policies;
- Appointing a DPO (where appropriate);
- Maintaining and up-keeping relevant and related documentation on controlling and processing activities;
- Data minimisation;
- Pseudonymisation;
- Transparency;
- Allowing individuals to monitor processing;
- Using data protection impact assessments (DPIA), which must be carried out when using new technologies and the processing is likely to result in high risks to the rights and freedoms of the individual. The GDPR specifies what the DPIA should contain;
- Creating and improving security features on an ongoing basis; and
- Adhering to approved codes of conduct and/or certification schemes.

IMPLICATIONS

Data Protection Fee

Currently the data protection registration fee (required for every data controller who consequently processes personal data) sits at £35 for most organisations, although this is under review with Parliament and new fees are thought to coincide with the GDPR implementation on 25 May 2018. It is thought that fees will be £40 to £2,900, depending on a number of factors including the number of staff and annual turnover.

Penalties

There are two tiers of administrative fines which can be imposed for a breach of the GDPR, depending on the specific infringement:

- up to 4% of their annual global turnover, or €20 million – whichever is greater; or
- up to 2% of their annual global turnover, or €10 million – whichever is greater.

These could be levied on an organisation instead of, or as well as, other appropriate measures, with regard given to:

- the nature, gravity and duration of the infringement;
- the intention or negligence of the infringement;
- mitigating actions that were taken, if any;

- degree of responsibility, and whether there were technical/organisation measures in place;
- other previous infringements;
- types of personal data;
- the manner the authorities were notified about the infringement;
- controller/processor's compliance;
- adherence to approved codes of conduct or certified schemes; and
- any other aggregating or mitigating factors.

If only a minor infringement has occurred, or if the fine is likely to impose a disproportionate burden onto a natural person, a reprimand may be issued instead.

The supervising authority has the following corrective powers to:

- issue warning to the controller/processor that current operations are likely to infringe provisions of the GDPR;
- issue reprimands accordingly;
- order the controller/processor to comply with a data subject's request pursuant to the GDPR;
- order communication of a personal data breach to the data subject;
- impose a temporary or definitive limitation or ban;
- order the erasure of rectification of data; and
- suspend data flow to a third country or international operation.

Liability

The GDPR also gives individuals the right to a judicial remedy (often compensation) if they feel their rights under the GDPR have been infringed.

Other Penalties and Criminal Sanctions

The GDPR has allowed Member States to set their own rules on other penalties for infringements, particularly to infringements which are not necessarily subject to administrative fines. Penalties should be effective, proportionate and dissuasive, and the Member State should take all measures necessary to ensure implementation of the chosen penalties.