The New EU General Data Protection Regulation (GDPR)

The clock has started on the biggest change to the European data protection regime in 20 years. After four years of negotiation, the new EU General Data Protection Regulation (GDPR) has now been formally adopted by the European Parliament. It will take effect twenty days from its post-vote publication in the Official Journal (May 2018) giving Data Controllers two years to prepare.

The Regulation will directly replace member states' own data protection legislation (the Data Protection Act 1998 (DPA) in the UK). It will apply to any entity offering goods or services (regardless of payment being taken) and any entity monitoring the behaviours of citizens residing within the EU. Companies are now directly responsible for DP compliance wherever they are based (and not just their EU based offices) as long as they are processing EU citizens' personal data.

Principles

The Data Protection Principles, as set out in the DPA, remain but they have been condensed into six as opposed to eight principles. Article 5 of the Regulation states that personal data shall be:

1. Processed fairly, lawfully and in a transparent manner in relation to the data subject.

2. Collected for specified, explicit and legitimate purposes and not further processed for other purposes incompatible with those purposes.

3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

4. Accurate and, where necessary, kept up to date.

5. Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

6. Processed in a way 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.

Consent

Like the DPA, the Regulation will require Data Controllers to have a legitimate reason for processing personal data. If they rely on the consent of the Data Subject, they must be able to demonstrate that it was freely given, specific, informed and unambiguous for each purpose for which the data is being processed. Consent can be given by a written, including electronic, or oral statement. This could include the Data Subject ticking a box when visiting a website, choosing technical settings for social network accounts or by any other statement or conduct which clearly indicates his/her acceptance of the proposed processing of personal data. Silence, pre-ticked boxes or inactivity will no longer constitute consent.

Children

The Preamble to the Regulation states:

> *"Children deserve specific protection of their personal data, as they may be less aware of risks, consequences, safeguards and their rights in relation to the processing of personal data. This concerns especially the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of child data when using services offered directly to a child."*

Article 8 requires that where the personal data of a child under 16 is being processed to provide "information society services" (e.g. online businesses, social networking sites etc.) consent must be obtained from the holder of parental responsibility for the child. Member states are allowed though to lower this threshold where appropriate but not below the age of 13.

Data Subjects' Rights

The list of rights that a Data Subject can exercise has been widened by Section 2 of the Regulation. The subject access right, rectification and being able to object to direct marketing remain. The right to have personal data processed for restricted purposes and the right to transfer data/have it transferred to another Data Controller (data portability) are new rights.

In addition Article 17 introduces a "Right To Be Forgotten" which means that Data Subjects will be able to request that their personal data is erased by the Data Controller and no longer processed. This will be where the data is no longer necessary in relation to the

purposes for which it is processed, where Data Subjects have withdrawn their consent, where they object to the processing of their data or where the processing does not comply with the Regulation. However, the further retention of such data will be lawful in some cases e.g. amongst others, where it is necessary for compliance with a legal obligation or for reasons of public interest in the area of public health or for the exercise or defence of legal claims.

To strengthen the "Right To Be Forgotten" in the online environment, the Regulation requires that a Data Controller who has made the personal data public should inform other Data Controllers which are processing the data to erase any links to, or copies or replications of that data.

Data Protection by Design

Data Controllers will be expected to include data protection controls at the design stage of new projects involving the processing of personal data. Where they wish to process personal data that poses potentially high risks they will have to, prior to the processing, carry out a Data Protection Impact Assessment. Supervisory Authorities (the member state's DP regulators e.g. the Information Commissioner's Office (ICO) in the UK) will be able to produce lists as to what sort of processing would warrant such an assessment.

Notification

The current system of Notification under the DPA will be replaced by a requirement for Data Controllers to keep an internal record in relation to all personal data they process (Article 30). The record must include, amongst other things, details of the purpose of processing of personal data, recipients, transfers to third countries, time limits for erasure as well as a general description of the technical and organisational measures in place protecting the data.

Data Breaches

Currently in the UK there is no legal obligation, under the Data Protection Act 1998 (DPA) to report personal data breaches to anyone. However the Information Commissioner's Office (ICO) guidance recommends that serious breaches should be brought to its attention. Last year telecoms company Talk Talk was the subject of a cyber attack in which almost 157,000 customers' personal details were hacked. The company was criticised for its slow response especially the time it took to inform the ICO and customers.

The Regulation contains a new obligation on Data Controllers to repot data breaches. Article 4 of the Regulation defines a personal data breach as:

> *"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed"*

Article 33 of the Regulation requires that, as soon as the Data Controller becomes aware that a personal data breach has occurred, it should without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the ICO, unless the controller is able to demonstrate that the breach is unlikely to result in a risk for the rights and freedoms of individuals. Where this cannot be achieved within 72 hours, an explanation of the reasons for the delay should accompany the notification to the ICO and information may be provided in phases without undue further delay.

Furthermore Data Subjects should be notified without undue delay if the personal data breach is likely to result in a high risk to their rights and freedoms, in order to allow them to take the necessary precautions. This notification should describe the nature of the personal data breach as well as recommendations for the individual concerned to mitigate potential adverse effects. This should be done as soon as reasonably feasible, and in close cooperation with the ICO and respecting guidance provided by it or other relevant authorities (e.g. law enforcement authorities).

Fines

Currently the ICO can issue a Monetary Penalty Notice of up to £500,000 for serious breaches of the DPA. The Regulation introduces much higher fines.

For some breaches of the Regulation (e.g. failing to comply with Data Subjects' rights or the conditions for processing) Data Controllers can receive a fine of up to 4% of global annual turnover for the preceding year (for undertakings) or 20 million Euros. For other breaches (e.g. failing to keep records or complying with security obligations) the fine can be up to 10 million Euros or 2% of global annual turnover (for undertakings).

Compensation

The Regulation also contains a right to civil damages just like under S.13 of the DPA. Article 82 of the Regulation states:

> *"Any person who has suffered material or immaterial damage as a result of an infringement of the Regulation shall have the right to receive compensation from the controller or processor for the damage suffered."*

This may see more in Data Subjects taking legal action against Data Controllers for data breaches. There may even be more class actions like the one against the London Borough of Islington in 2013 when 14 individuals settled for £43,000 in compensation after their personal data was disclosed without their authority. This action followed an ICO investigation, which resulted in the council being fined £70,000 under the DPA.

Data Protection Officer

Section 4 of the Regulation introduces a statutory role of Data Protection Officer (DPO). Most organisations handling personal data, both Data Controllers and Data Processors, will require a DPO who will have a key role in ensuring compliance with the Regulation. A group of undertakings may appoint a single DPO provided that he/she is easily accessible. Public bodies may also have a single DPO for several such authorities or bodies, taking account of their organisational structure and size.

The DPO, who can be a staff member or contractor, shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfill the tasks referred to in Article 39. These are:

- to inform and advise the controller or the processor and the employees who are processing personal data of their obligations pursuant to this Regulation;
- to monitor compliance with this Regulation, including the assignment of responsibilities, awareness- raising and training of staff involved in the processing operations, and the related audits;
- to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;
- to cooperate with the supervisory authority (the ICO);

- to act as the contact point for the supervisory authority on issues related to the processing of personal data

The Regulation is accompanied by the EU Policing and Criminal Justice Data Protection Directive which contains new rules for Data Protection when applied to crime and justice, but which can be implemented by each Member State through its own laws with greater flexibility.

There is a lot to learn and do in the next two years. All Data Protection practitioners and lawyers need to read the Regulation and consider its impact on their organisation and clients. Training and awareness at all levels needs to start now.

Ibrahim Hasan is a solicitor and director of Act Now Training (www.actnow.org.uk).