# General Data Protection Regulation

## The Key changes at a glance

In April 2016, the European Union paved the way for a single European Digital Market by adopting major data protection reforms. A New Regulation (`The General Data Protection Regulation')* would have replaced the current UK Data Protection Act 1998, coming into force on 25 May 2018.

Following the Brexit decision by the UK public, European Union laws and regulations have become more uncertain. However, the European Communities Act 1972 remains in force in the UK which continues to give EU regulations direct effect. The ICO have stated that we are in need of "clear laws with safeguards" and are form of UK data protection law is necessary. Given the progress of the digital market and the business need to transfer data across borders, it is likely that any reform of UK data protection law will take much of the same tone as the New Regulation.

* Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

Whilst the underlying principles of the current EU data protection regime are retained, clarified and expanded, the reforms also introduce new and complex concepts in relation to the processing of personal data.

Inevitably changes to data handling processes and customer documentation will be needed to comply with the new standards, and business will have an express obligation to document and demonstrate compliance and its response to any personal data security breach.

Forward planning the transition to the new regime and re-assessing its risk profile, is of key importance to businesses seeking to maintain customer confidence and avoid the massively increased financial penalties proposed.

We outline below some of the key changes and some practical tips to help business prepare for implementation.

| Topic | Provision | Key Changes | How to Prepare |
|---|---|---|---|
| **Scope and Cross Border Processing** | Harmonisation | The Regulation will have direct effect within EU Member States. Subject to limited areas in which Member States may derogate from the default position, the rules will be the same across the EU. | This is a positive change aimed towards making compliance across multiple EU Member States easier. However there may still be differences within the EU, such as additional supervisory powers and penalties under derogations.<br>Consider existing supervisory enforcement and supervisory regimes of Member States in which you have a presence as possible indicators of variance between Member States. |
| | Territorial Scope | Extends to processing personal data by controllers and processors established inside the EU, and also outside the EU where the processing is about EU 'residents' in connection with either:<br>A. offering goods or services; or<br>B. monitoring behaviour. | Non-EU organisations should assess whether their activities will bring them within the scope of the Regulation. If so, they will need to nominate a representative in the EU to act on their behalf. |
| | Supervisory Authority | ICO deals with complaints or infringements where the subject matter:<br>relates to a solely UK established controller or processor, or (ii) substantially affects only UK data subjects. | Continue to engage with ICO on policy issues and track for developing guidance. |
| | Lead Authority ("One-Stop Shop") for cross border processing | Cross border personal data processing (i.e. processing undertaken in or affecting data subjects in more than one Member State) is supervised by the 'Lead Supervisory Authority' i.e. the Supervisory Authority of the Member State where the controller or processor has its sole or main establishment. | Continue to engage with ICO on policy issues and track for developing guidance. |
| **Justification and Transparency** | Changes to Consent | More prescriptive rules will apply where relying on consent as a justification for processing, including: it must be as easy for data subjects to withdraw consent as it is to give it;<br>– making consent a contract requirement will not be effective where the processing is not necessary to perform the contract;<br>– consent to process the data must be distinguishable where placed within wider consent declarations; and<br>– reliance on consent will trigger the right to be forgotten and data portability. | Review consent cases and identify contexts where consent has been required under contract, assess whether another justification can be met.<br>Review consent wording in standard documentation. Generally consider whether consent remains a practicable basis having regard to wider implications involved, and the ability for data subject to withdraw consent at any time. |
| **Data Handling Standards** | Privacy Impact Assessment | Controller is required, particularly for new technologies, to assess whether processing has a high risk of prejudicing data subject rights (e.g. systematic or large scale sensitive personal data processing or profiling/evaluation).<br>High risk processing requires prior consultation with the Supervisory Authority, who can potentially use its corrective powers (e.g. ban or limit the processing). | Evaluate whether existing or proposed new processing is high risk and if so assess whether risks can be reduced or avoided, for example by pseudonymisation.<br>Devise and adopt Privacy Impact Assessment processes and documentation which incorporates for example, senior management sign-off for high risk processing activities. |
| | Privacy by Design | Data protection principles must be incorporated both technologically and through operating policies, into product/ | Privacy needs to be embedded in your organisation's culture and built into the policies |

| Topic | Provision | Key Changes | How to Prepare |
|---|---|---|---|
| | | project design process.<br>Data privacy risks must be properly assessed and dealt with before launching any new products, and maintained throughout. | and processes that you adopt.<br>Ensure that there is an understanding of your obligations at all levels of your organisation through training and awareness-raising.<br>Identify applicable privacy codes of practice based on the location of your main establishment in the EU and take steps to comply with these. |
| | Obligations of Data Processors | Data controllers will remain responsible for the acts of data processors, however, data processors will themselves be subject to certain obligations under the Regulation (including data security) and corresponding penalties for non-compliance. Data processing contracts must include additional mandatory provisions, for example, the data controller must have the right to audit the processor. | Review processing agreements to ensure that the provisions are adequate to address the obligations imposed by the Regulation. Apportion risk and responsibility appropriately. If you are a data processor then:<br>– audit your supply contracts with customers and do gap analysis between existing contractual obligations and new direct obligations;<br>– devise a compliance regime for new direct obligations; and<br>– evaluate the cost impact of compliance on your business and review pricing models. |
| **Data Handling Standards** | Privacy by Design | The Regulation introduces the concept of pseudonymisation, i.e. where the information which allows data to be attributed to a particular individual is held separately and subject to security measures to ensure that it is not linked to the individual.<br>The Regulation promotes the use of pseudonymisation as a means of achieving privacy by design.<br>Organisations using personal data for historical or scientific research or statistical purposes will usually be required to adopt pseudonymisation. | Assess the opportunities for pseudonymising personal data (for example, where the identity of the data subject is unnecessary either at the outset and once a purpose or activity has been fulfilled), and how this impacts the risk profile of the processing (e.g. whether high risk for Privacy Impact Assessment purposes, or in determining risk for the purpose of data security breach notification). |
| **Administering Compliance** | Data Protection Officers | Public bodies and organisations conducting high risk activities (systematic or large scale sensitive data or profiling/evaluation activities), must appoint a Data Protection Officer with expert knowledge of data protection law. | Assess whether your organisation will be required to appoint a Data Protection Officer and, if so, devise a recruitment and training strategy and timeline.<br>Ensure the role is integrated into governance and reporting frameworks |
| | Filing and record keeping | Data controllers will no longer need to submit notifications to their supervisory authority. Instead, and subject to some exceptions, data controllers and data processors will be required to keep records of their processing activities and compliance practices, and to evidence the obtaining of consent. | Conduct a data mapping exercise and maintain detailed records of each of the processing activities that you or your data processor carries out. |
| | Breach Reporting | Data controllers must report data breaches to:<br>– the Supervisory Authority, without delay and no later than 72 hours after the breach, unless the breach is unlikely to present a risk to individuals; and | Develop or revise your data breach response plan to ensure breaches are reported and escalated without delay and dealt with appropriately to minimise damage. Include a process for reporting breaches within the required time limits, and assign responsibility for reporting to specific individuals. Consider |

| Topic | Provision | Key Changes | How to Prepare |
|---|---|---|---|
| | | – data subjects, where the breach is likely to pose a high risk to them.<br>Data processors must notify controllers of data breaches without undue delay. | whether any contexts can properly be assessed and flagged as `low risk' so focus can be concentrated on high risk areas in the event of a data security breach situation. Consider whether data classification policy needs to be amended or expanded upon accordingly. |
| **Data Subject Rights** | Minimum Information | Data subjects must be provided with more prescriptive explanations about the processing of their personal data, and different levels of explanation will apply according to whether the data is captured by the data controller or a third party source. | Audit for third party sourced data and incorporate corresponding type of notice into procedures.<br>Review fair processing notices and privacy policies generally to ensure that they are accurate, up to date, provide the required additional information, and are given in clear, plain language.<br>Amend agreements with third parties from whom you source personal data to impose increased information provision requirements. |
| | Profiling | Data controllers must inform data subjects of the existence and consequences of any profiling activities which they carry out (including online tracking and the use of behavioural advertising).<br>Data subjects will have the right to object to solely automated decision-making that significantly affects them, though this right is subject to limited exceptions. | If your business is engaged in profiling activities, assess which legal basis you will use to justify the profiling. If applicable, consider the mechanism that you will use to obtain consent and to respond to objections.<br>Businesses engaged in profiling must implement suitable measures to safeguard the data subject's rights, freedoms and legitimate interests (for example, a right to human intervention). |
| | Right to rectification and erasure | In certain circumstances data subjects will have the right to require data controllers to delete their personal data without delay (right to be forgotten).<br>If the personal data has been made public, the data controller must take reasonable steps to notify relevant third parties of the data subject's request.<br>Data subjects will be able to directly require the data controller to rectify inaccurate data. | Plan and implement a workable process for dealing with requests under the right to be forgotten.<br>Assess whether records can be structured to easily identify the relevant features giving rise to the right to be forgotten e.g. where processing is based on consent, or for automated deletion where no longer needed. |
| | Data Portability | Personal data provided by the data subject and processed on the basis of consent or where it is necessary to perform a contract, will be subject to the right of portability i.e. data transfer to a third party service provider in appropriate machine readable format. | Devise procedures for dealing with this right.<br>Assess whether records can be structured to easily identify the relevant features giving rise to the right to be forgotten e.g. distinguish between data obtained directly from the data subject from that obtained from a third party, and whether another justification can be met which does not attract this right.<br>Monitor for emerging guidance from Supervisory Authority and engage with your industry groups to develop operational and technical standards. |

| Topic | Provision | Key Changes | How to Prepare |
|---|---|---|---|
| **Data Subject Rights** | Right to non-automated decisions | This prohibits wholly automated decisions (including profiling) which have a significant legal effect on the data subject i.e. such processing should not take place, (as opposed to the data subject merely being entitled to ask for the decision to be re-taken manually). | Review your automated processing decisions and amend your processes accordingly. |
| | Right to object to processing | The threshold for requiring the data controller to cease processing the data is lowered.<br>Processing (including profiling) based on legitimate interests or public interest must cease if the data controller cannot demonstrate an overriding compelling reason.<br>Data subjects will be able to opt out of profiling activities related to direct marketing as well as just opting out of receiving direct marketing communications. | Assess whether pseudonymisation can reduce the impact of such requests.<br>Review your suppression processes to ensure profiling, as well as opt-outs from marketing communication, is captured. |
| **Enforcement, Penalties and Liability** | Right to claim | Data subjects will have a right to claim compensation for damage suffered as a result of a breach of the Regulation, whether the damage is material or immaterial. They can claim against any data controller involved in the processing.<br>Where multiple controllers or processors are involved in the same processing, each is liable for its own and the other's applicable infringement. Clawback between the parties can only take place once the data subject has been fully compensated.<br>Public interest groups will be entitled to bring class actions on behalf of data subjects. | Assess the risks of data subjects bringing claims against you (both individually and under class actions) for any breach of the Regulation, including where this involves merely distress/non-pecuniary loss.<br>Reassess whether the risks of non-compliance remain acceptable to your business, or whether action is required to improve your compliance status and reduce the risk of compensation claims and reputational damage to your organisation. |

## Contact

DWF has specialist data protection lawyers who are experienced in steering clients along the path of major data protection reform. For more information on our data protection services and how we can help you prepare, please contact:

**Jamie Taylor**
Senior Management Director
**T** +44 (0)161 604 1606
**M** +44 (0)7712 899 712
**E** Jamie.Taylor@dwf.law

© DWF 2019. DWF is a legal business operating through various separate and distinct legal entities. Our lawyers are subject to the rules of the regulatory body with whom they are admitted. For further information about these entities and DWF's structure, please refer to the Legal Notices page on our website. All rights reserved.