EU General Data Protection Regulation and how it affects you and your business
Key Q&As

Background

The General Data Protection Regulation (GDPR) is an EU regulation which aims to strengthen data protection for individuals within the EU. It will harmonise the current data protection laws currently in place across all EU member states and bring the law into the 21st century and providing consistency. The existing UK legislation, the Data Protection Act, dates from 1998 and was intended to bring UK law into line with the EU's Data Protection Directive introduced in 1995.

What is the difference between a regulation and a directive?

A regulation is directly applicable to all EU member states and immediately enforceable, whereas a directive is binding but usually requires individual states to change their own laws in order to implement it.

When does GDPR come into force and who will be affected?

It was adopted in April 2016 and comes into force on 25 May 2018. It will affect everyone and it could have a big impact on any company in the world that deals with the personal data of EU citizens.

Does personal data relate only to a person's private life?

No. Personal data is any information – private or professional – relating to an individual. This includes names, photos, email addresses, bank details, social media posts, medical information, work performance, tax number, username, password, computer IP addresses and a host of other information which could directly or indirectly identify someone.

What are the main changes between the Data Protection Directive, Data Protection Act and the GDPR?

The principles of the DPA still apply. The main changes are briefly outlined on the next page:

- Increased territorial scope – all companies processing the personal data of anyone residing in the EU will come under the scope of GDPR, regardless of where the company itself is based
- Penalties – an organisation seriously infringing the resolution can face a fine of up to €20m or 4% of annual global turnover (whichever is greater). Lesser infringements could incur a 2% fine. Additionally, damage claims can be brought by individuals or groups, carrying both financial and reputational implications
- Consent – request for consent to use personal data must be given in an intelligible and easily accessible form. Users should not have to opt out of their data being used, they must opt-in to your systems. Consent must be freely given, informed, specific and unambiguous, and it must also be as easy to withdraw consent as it is to give it
- Privacy by design – the inclusion of privacy from the outset of designing of a system rather than as an addition
- Extended rights –
    - Data controllers (organisations holding personal data) are required to inform data subjects (individuals) of any data security breaches within 72 hours of becoming aware of the breach where the breach is likely to "result in a risk for the rights and freedoms of individuals"
    - Individuals can obtain a copy of personal data from the data controller in a digital format, and obtain confirmation of whether their personal data is being processed, where and for what purpose
    - Personal data obtained by an individual from a data controller is portable i.e. it can be transmitted to another controller
    - Under certain conditions individuals have the 'right to be forgotten' i.e. to ask that the data controller erase their personal data and cease further distribution of it
- Data protection officers (DPO) – controllers will no longer be required to notify their data processing activities with their own country. Controllers and processors whose core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale will be required to appoint a DPO. It is a good idea, however, for all organisations to appoint someone responsible for data protection compliance
- Accountability – companies are expected to put into place governance measures such as privacy impact statements to demonstrate they comply with the principles of the regulation.

What do we need to do to ensure our company is compliant?

We've identified ten areas to examine. Please note that this is an overview, not a step by step guide. Bear in mind that as each step is quite lengthy, you will need to push on with changes as soon as possible to be ready for 28 May 2018.

1. Data audit – document what personal data you hold (employee, client/customer, supplier etc.), where you and your employees hold it, where it came from and who you share it with
2. Privacy policy – review your current policy and update it in line with the new guidelines. When you collect data, you will need to explain your 'legal basis' for processing it, so it's best to give detail on this within your privacy policy and notices on any web pages, web forms or other data collection points
3. Code of conduct – trade associations and representative bodies may like to draw up a code of conduct covering topics such as fair and transparent procession, information provided to individuals, and data transfers outside the EU
4. Data protection impact assessments – use for large scale processing activities, new technologies or where there is a high risk to the rights and freedoms of individuals
5. Rights – ensure your procedures comply with new rights of individuals and establish how you will supply/delete data on request via your systems and processes
6. Consent – review how and where consent is sought, obtained and recorded. Consent must be a positive indication of agreement to personal data being processed; a pre-populated tick box is not acceptable, for example
7. Children – a parent or guardian's consent is needed to process a child's data lawfully. In the UK a child is likely to be defined as anyone under the age of 13. How will you establish age, communicate this consent process to children and verify consent?
8. Third party – any third party who uses your data on EU citizens must also comply with the regulations. Ensure you know who is using your data and for what purpose. Beware that your contractor may sub-contract the job
9. Breaches – what will you do to detect, report and investigate a breach?
10. International – map out where your organisation makes its main decisions about data processing. This will determine which country is your supervisory authority i.e. who will take the lead when investigating a complaint which crosses country borders.

What would be a legal basis for processing data?

Processing conditions include consent of the data subject, necessity for the performance of a contract and compliance with a legal obligation.

How many people in the organisation will GDPR affect?

A great many people in your organisation will handle personal data in one way or another, so a training programme for all staff would be helpful. Outline their roles and responsibilities from board level down and be prepared to repeat the messages more than once for it to sink in.

How do we keep control of what third parties (processors) are doing with our data?

Review your contracts now, and look at procedures to ensure they are compliant. This includes providers outside the EU who may not have realised that the regulation applies to them. Cloud services might be used for HR, payroll, document sharing and other purposes, and the terms and conditions that you agreed to may reserve the right to use the data for secondary purposes and need revising or terminating.

How can we keep data safely stored under the new rules?

Controllers must meet individuals' 'reasonable expectations' of data privacy by implementing measures that meet the principles of data protection by design and data protection by default. These include data minimisation, and making data less accessible by devices such as encryption or pseudo-anonymisation.

How can we demonstrate that our company has taken steps to comply?

If you have followed the steps above and can clearly show how you obtain, process and store personal data within the GDPR, it should demonstrate your company's intent to comply.

Where can we find out more information?

The Information Commissioner's Office (ICO) has many pages of its website dedicated to data privacy and data protection reform. It is part of the Article 29 Working Party which is developing guidelines on some of the key aspects of the law. They plan to publish guidance on contracts and liability and consent early in 2017. Reading some of their audit overviews will give you an idea of the practical measures that organisations have been required to apply.