ashfords

GDPR OVERVIEW 2018

Ashfords LLP
ashfords.co.uk

WHAT IS THE GENERAL DATA PROTECTION REGULATION?

The greatest reform of data protection law for a generation.

From 25 May 2018 the General Data Protection Regulation (GDPR) will be enforced across Europe. The GDPR actually came into force on 25 May 2016 however organisations have been given 2 years to prepare for the most significant changes we have seen to data protection in over 20 years.

It's important to ask yourself, is my organisation aware of the changes and what can I do to prepare?

What are the key changes:

Wider scope - territorial

The GDPR applies to any organisation that is 'established' in the EU and processes personal data 'in the context of its activities'. An organisation with even a minimal presence within the EU will be caught when processing personal data, even if the actual processing occurs outside the EU.

In addition to this, organisations established outside the EU will also be caught if their processing activities relate to (i) offering goods and/or services to EU residents (even if complimentary), and/or (ii) the monitoring of behaviour within the EU. Such organisations will be required to appoint a representative within the EU.

Personal Data - broader definition

The definition of personal data is even wider than it was under the Directive, as it now expressly includes identification numbers, location data and online identifiers such as IP addresses and cookies. Essentially the only data that will fall outside of the definition or personal data is that which is truly aggregated. The definition of sensitive personal data (now called special category data) also now includes genetic data and biometric data.

Consent - stricter conditions

There are stricter conditions for obtaining consent – it must be freely given, specific, informed, unambiguous, distinguishable and not 'bundled' with other written agreements or statements. It must be as easy to withdraw consent as it is to give and individuals have the right to withdraw consent at any time. Additional rules apply to the validity of consent given by children.

It is also important to note that consent must be given for each processing activity, therefore if an organisation decides to process personal data for an additional purpose the organisation must obtain further consent.

Legal basis – not just consent. With individuals having a greater ability to withdraw consent organisations should consider relying on another condition for processing such as: a "contractual obligation", "legal obligation" or "legitimate interests". In terms of the latter, organisations must perform a proper assessment of the individuals data protection rights and document how the organisations legitimate interests do not have a detrimental effect on the individuals rights. This assessment and requirement to document will make it more difficult for organisations to rely on "legitimate interests" as easily as they currently do.

Increased individual rights

The GDPR provides numerous enhanced rights for individual data subjects. For example, individuals have the right to require information about whether their personal data is being processed and further information such as the purposes of processing and the recipients of the data. Individuals also have the right to object to their personal data being processed for direct marketing.

Individuals can ask for a copy of their data free of charge, which must be provided in a structured, commonly used and machine readable form. Individuals may also ask for their data to be transmitted directly to another data controller. This new data portability requirement will make it more onerous for organisations to comply with **'subject access requests'.**

The GDPR gives a statutory footing to '**the right to be forgotten**', which gives data subjects the right in certain circumstances to have their data erased, prevent further dissemination and have third parties informed of the requested erasure.

Direct obligations on data processors

For the first time data processers now have certain direct statutory obligations. For example, they must maintain written records of their processing activities; implement appropriate security standards; carry out routine data protection impact assessments; appoint a Data Protection Officer (DPO), if required; not appoint sub-processors without first obtaining the controllers consent (SaaS and cloud providers are already starting to pre-agree a schedule of sub-processors when entering into new agreements); and notify the relevant data controller of any data breach without undue delay.

Data Protection Officers

A DPO with expert knowledge of data protection law must be appointed if: an organisation is a public authority, carries out large scale systematic monitoring of individuals; or carries out large scale processing of sensitive personal data.

The DPO must directly report to the highest level of management. Each domestic regulator is free to make additional requirements in respect of DPO's, to date the ICO has not commented on any additional DPO requirements.

Breach notification

The GDPR contains the following breach notification obligations:

- Processor - notify Controller without undue delay
- Controller - notify regulator without undue delay and in any event no later than 72 hours after becoming aware

In certain circumstances individual data subjects will also need to be notified of the breach, unless

- the breach is unlikely to result in a high risk for the rights and freedoms of data subjects;
- the organisation had appropriate technical and organisational protection;
- would trigger disproportionate efforts (in such a circumstance an organisation could rely on something like a public information campaign).

Harsher penalties

The maximum fine for the most serious infringements (such as not having a legal basis for processing) is up to 4% of annual group global turnover or €20 million (whichever is greater).

Administrative failures (such as failing to report breaches) can result in a fine of up to 2% of annual global turnover or €10 million (whichever is greater).

It is also important for organisations to be aware that they can also be sued by individuals for breaches of the GDPR.

If you are reliant on your data to do business be aware that the ICO will have the power to order an organisation to delete data.

HOW SHOULD ORGANISATIONS PREPARE FOR THE GDPR?

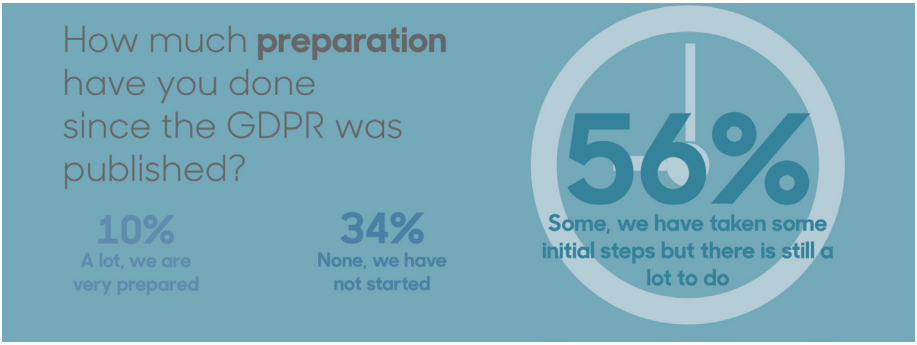
Early analysis has shown that larger organisations are aware of the introduction of GDPR, but they are unaware and under-prepared for some of the subtler or less-publicised aspects of the new rules. Smaller organisations tend to be more uncertain about their obligations, with 82% of SMEs either not having heard of it or not understanding its impact (Close Brothers Business Barometer, Q2 2016).

The main ways to prepare for the GDPR are:

- Conduct an audit of any data currently processed by the organisation and ensure that any unnecessary or outdated personal data is deleted.
- Review all data protection policies and codes of conduct to ensure they comply with the new principles. If these do not exist they should be created as soon as possible.
- Become clear about the grounds for lawful processing being relied on. Note that public authorities can no longer rely on the ground of "legitimate interests" when processing data.
- Ensure that consent for lawful processing is active and does not rely on pre-ticked boxes. Make sure that the consent relates specifically to the purposes of the processing, as consent for one purpose cannot then be used for another. Check that marketing contact lists include only those individuals who have given consent.
- Keep paper trails of decisions relating to data processing to demonstrate

compliance. Ensure that privacy impact assessments are carried out when required, and keep all relevant documentation.

- Review and update existing information notices. Specified information must be provided, including the identity and contact details of the controller, purposes of processing and the legal basis for processing, details of transfers outside the EU, the retention period and individual rights.
- Review and update internal breach procedures. Ensure that the relevant people know who to report to in the event of a breach. Prepare incident response plans.
- Train all members of staff on the new rules and ensure that any person likely to receive requests relating to personal data (i.e. data erasure requests) knows how to deal and respond. Develop template response letters. Consider developing portals on which data subjects can access their data directly.
- Consider whether there is a requirement to appoint a DPO. Most public authorities and companies that monitor online behaviour will be caught. Even if an organisation is not strictly required to appoint a DPO, it is recommended that someone with sufficient expertise is assigned responsibility for ensuring data protection compliance.
- Existing supply chains, contracts and templates will need to be checked and potentially renegotiated, particularly in light of the new direct obligations on data processors.
- Insurance arrangements will need to be reviewed. Coverage in the event of a data breach should be added to existing policies or purchased separately if possible.
- Identify any areas of non-compliance using updated risk registers and implement a mitigation strategy as soon as possible to avoid potential sanctions in the future.



* Statistics from survey conducted by Ashfords LLP and SW Business Insider, 2017

WHAT OPPORTUNITIES WILL IT BRING?

The GDPR presents an opportunity for organisations to streamline their data protection practices. Full implementation of the GDPR should result in organisations only holding onto data that is accurate, up to date and relevant, with its use being approved by the individual.

The process of reviewing existing data and removing unnecessary data may enable organisations to capitalise on useful data they did not know they had, and make customer contact lists more focussed and effective. Ultimately good data protection will add value to your organisation.

There has been a significant rise in public concern surrounding personal data and cyber security. Implementing the GDPR compliant measures should help consumers and customers have more confidence in how an organisation is handling their data, thereby enhancing the organisation's public image.

Organisations will have to implement 'privacy by design', which effectively means implementing data protection measures from the outset and building it into core business processes. This will help organisations to identify issues at an early stage, making any remedial actions less intrusive and costly.

* Statistics from survey conducted by Ashfords LLP and SW Business Insider, 2017

WHAT IMPACT WILL BREXIT HAVE?

On 24 October 2016 Karen Bradley, the Secretary of State for Culture, Media and Sport, confirmed during a Select Committee meeting that the government will be implementing the GDPR. She stated that:

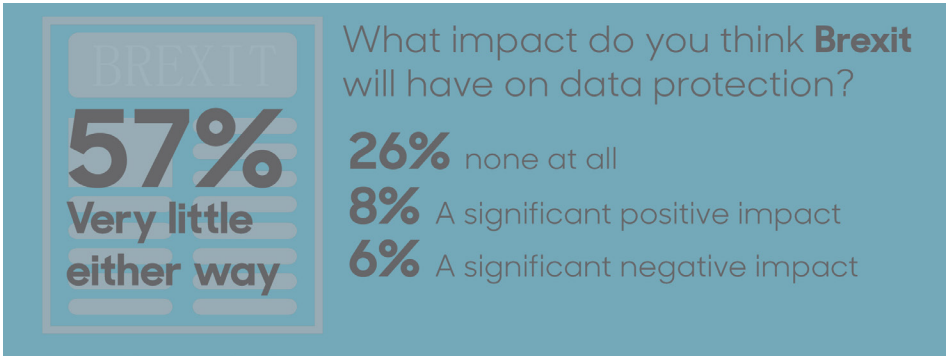
"We will be members of the EU in 2018 and therefore it would be expected and quite normal for us to opt into the GDPR and then look later at how best we might be able to help British business with data protection while maintaining high levels of protection for members of the public."

On 31 October 2016 Elizabeth Denham, the new Information Commissioner, welcomed this announcement, stating it was "good news for the UK". She declared that the ICO is committed to assisting business and public bodies to prepare to meet the requirements of the GDPR. She announced that a revised timetable will be published setting out what areas of guidance will be prioritised over the next six months.

It is clear that UK organisations need to start preparing for the GDPR before it takes effect on 25 May 2018 in order to avoid sanctions for non-compliance and reap the benefits that it will bring.

In September 2017 the government published the Data Protection Bill which incorporates GDPR into our statute book meaning it will apply in the UK after we leave the EU.

The Government has also published a position paper on data protection as part of the Brexit negotiations, post Brexit data flows between the UK and Europe are crucial and must continue to be as free as possible.



* Statistics from survey conducted by Ashfords LLP and SW Business Insider, 2017

ashfords

KEY CONTACT

Chris Coughlan
Senior Associate
c.coughlan@ashfords.co.uk
+44 (0)117 321 8060

Ashfords is a national provider of legal, professional and regulatory services.

We combine legal expertise, commercial experience and our wider network to help our clients achieve their goals. So, to many clients, we are more than lawyers, we are professional advisers, mentors, problem-solvers.

Above all, we believe that every client should expect and receive value for time and value for money. Which means that we always aim to provide advice that is not just technically sound, but that is grounded in our understanding of your world.