GENERAL DATA PROTECTION REGULATION WHITE PAPER

GENERAL DATA PROTECTION REGULATION

- Introduction
- What it means for you and your business
- The questions you need to ask
- The key principals of GDPR
- Summary

Introduction

With GDPR coming into force in May 2018, every business needs to review the way they gather, store and use personal data – and that includes employee, prospect and customer data. The need to comply with the new Regulation will be compulsory, and heavy fines will be levied at those found to be in breach, so the time for action is now.

The whole thing began at the end of 2011 with the EU Commission's stated intention to unify and strengthen data protection by modernising legalisation within the EU. This revamp of data protection legalisation directly sprang from the increase in internet services and serves to reflect the changing times and the different demands of our digital world. After not an insignificant amount of time the long awaited adoption of the General Data Protection Regulation ("GDPR") took place on the 27th April 2016. This replaces the 1995 Data Protection Directive which deemed to be no longer fit for purpose. What follows is a 2 year transition period resulting in the Regulation coming into effect in May 2018.

Because the GDPR replaces the 1995 Directive the outcome is that the Data Protection Act (DPA) 1998 will need to be revised, as well as the Privacy and Electronic Communications (PECR) 2003.

The DPA sets out data protections principles, conditions for consent, conditions for handling personal data. PECR sits alongside the DPA and provides the 'rules' in relation to electronic communications i.e. direct marketing calls, emails and texts and cookies. The process of revising PECR has started and will take a minimum of 4 years.

What it means for you and your business

Changes to the governance of data will have far-reaching consequences for your business. The new General Data Protection Regulation (GDPR) will determine how your business does business, and particularly how it manages, protects and administers data in the future. The new regulations come into place in 2018 and you need to start preparing now.
– DMA, 2016

The GDPR will provide a single legal framework which will apply to all members of the EU, streamlining and hopefully simplifying what is currently a hotch potch of laws for each member country. Directly concerned with the collection, storage and use of personal data, this will impact every business that holds any personal data in format.

If a business collects, stores or uses personal data then the GDPR applies and now there is an obligation for compliance, with serious penalties for those that don't. In the past it was only controllers who had compliance obligations, this now also applies to processors. This means that where the controller has agreements with processors these must be reviewed to ensure that processors who work on behalf of controllers are within the requirements of GDPR including the process for identifying and reporting any breaches to the controller.

Definition of personal data – Article 4 of the Regulation:

Personal data means any information relating to an indentified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Some questions you need to ask yourself

Do you process personal data?

Consider if your business is involved in any of the following:
- Do you have personal data in a CRM system?
- Are you collecting information on your customers?
- Do you market your products using electronic and/or direct marketing?
- Do you buy B2B data for marketing?
- Do you have a clear audit trail of exactly where the data you hold originated from?

If yes, then you must have a full audit trail and document where the data came from and any third parties it has been shared with.

What personal data do you currently hold?
Be clear about what personal data you hold, where it's come from and if shared with third parties that the correct consents are in place. This also involves a full audit trail which has been documented should evidence of compliance be required.

What does this mean in relation to data already in my systems?
Do you know where the data came from? Are the correct permissions to use the data in place? Have you made contact with the data subject within the last 12 months? You need to ensure that all personal data complies with GDPR or remove it.

How does the GDPR impact on how I gather new data?
You need to ensure that any data added to your systems is compliant with GDPR and that you can prove this and provide appropriate documentation if needed.

How do I prove the data is compliant?
Retain audit trails of where data was sourced (third parties, incoming enquiries, your own sales force) and information that confirms that consent was given.

Are my privacy statements still adequate?
These need to be reviewed and very likely revised to ensure they are compliant with the GDPR.

The key principles of the GDPR

European Commission:

The current rules also need modernising – they were introduced at a time when many of today's online services and the challenges they bring for data protections did not yet exist. With social networking sites, cloud computing, location-based services and smart cards, processing of personal data has grown exponentially. We need a robust set of rules to make sure people's right to personal data protection – recognised by Article 8 of the EU's Charter of Fundamental rights – remains effective in the digital age. This will at the same time be beneficial for the development of the digital economy.

1. Accountability and Transparency

Accountability is one of the key tenants of the new Regulation and data controllers will need to have evidence of compliance and be able to demonstrate that compliance if necessary. It is highly likely that privacy policies and statements will need to be reviewed to ensure transparency around the process of a subjects' data. Individuals should have more information about how their data is processed and this should be made available in a 'clear and understandable way.'

2. Consent.

The 2 grounds for processing personal data are consent or legitimate interest. The GDPR states that consent must be:

"...freely given, specific, informed and unambiguous, and given by means of a statement or clear affirmative action."

Silence or pre-ticked boxes are likely to be acceptable forms of consent under the regulation. A controller cannot make a provision of a service conditional on consent; consent must be specific to each data processing activity; consent can be withdrawn at any time and must be easy to do.

3. Right to be forgotten

This allows for an individual to request that their data is deleted provided there are no legitimate grounds for keeping it. Data controllers must take reasonable steps to inform other data processors with whom the data has been shared.

4. Subject Access Request
An individual can request access to their data and this must be within one month and no fee charged. If the Data Controller processes a large quantity of data about the individual, it is reasonable to ask for the request to be narrowed down.

5. Data portability
Individuals can ask for their personal data to be provided in a useable format so it can be transferred to another data controller.

6. Data protection by design and default
Data protection and privacy will be at the forefront of any project from the very start. It is also concerned with the amount of data collected, the purpose and the length of time the data is kept. Where necessary, Privacy Impact Assessments (PIA's) may need to be conducted to identify and reduce any privacy risk from the earliest stages of development. In fact, PIAs are mandatory for companies dealing with processes that present high risk to their data subjects.

7. Fines
There will be heavy sanctions for breaches – including fines up to 4% of annual turnover or 20 million Euros whichever is the higher, for the most serious breaches.

8. Reporting Breaches
Reporting breaches is mandatory, and companies and organisations must notify the supervisory authority of data breaches within 72 hours as a general rule. They must also communicate to the data subject any high risk breaches so that appropriate measures can be taken.

9. Does Brexit change things?
The GDPR will apply to all UK entities that do business in the EU and so it seems that the UK Government is likely choose to reform the current UK data protection laws in line with the requirements of the GDPR. To achieve the necessary "adequacy" which would be required to trade with the EU the UK will need to implement similar standards of compliance – or face the additional regulatory and administrative burden on EU rules.

> *The Data Protection Act remains the law of the land irrespective of the referendum result. If the UK is not part of the EU, then upcoming EU reforms to data protection law would not directly apply to the UK. But if the UK wants to trade with the Single Market on equal terms we would have to prove 'adequacy' – in other words UK data protection standards would have to be equivalent to the EU's General Data Protection Regulation framework starting in 2018.*
> **- 24 June 2016 - ICO Spokesperson**

10. Appointing Data Protection Officers
This is required for certain organisations, those whose core activities consist of processing operations that require regular monitoring of individuals on a large scale.

Summary

In about 18 months every business that holds or processes personal data must have reviewed their processes and put in place whatever changes are required to ensure that they are GDPR compliant.
If you are still unsure about what you need to do, get in touch and we will be able to provide you with guidance and practical advice.

About us

Mib Data Solutions are the specialist B2B data provider and leading fleet data owner in the UK with over 20 years of experience in the database and direct marketing industry. With their dedicated team of data experts, mib Data Solutions are fully compliant with the requirements as set out in the GDPR.
Mib Data Solutions have developed an in-depth understanding of data requirements and sophisticated database analysis techniques, so whatever the need, bespoke data solutions or marketing from a trusted source, mib Data have the solutions.

Contact Details

Tel: 0845 053 3411

Email: sales@mibdatasolutions.co.uk

Website: www.mibbusinessdata.com

2nd Floor, 26-34 Bedford Court, Bedford Street, Leamington Spa, Warwickshire, CV32 5DY