dun & bradstreet

GDPR: An evolution not a revolution

The real impact of the General Data Protection Regulation for business

THE REALITIES OF GDPR:
A POSITIVE LEGISLATION FOR GLOBAL BUSINESS

On 25 May 2018, the General Data Protection Regulation, or GDPR, will come into effect throughout the EU. This will replace the current Data Protection Directive 1995 that was used as the basis for legislation in individual member states, such as the UK's Data Protection Act 1998. The purpose of the GDPR is to update the 1995 data privacy legislation, taking into account technological developments, particularly the rise of social media. It will also help to harmonise and standardise legislation throughout Europe. As an EU Regulation rather than a Directive, it will be directly applicable throughout Europe and increase consistency of data protection across all member states (except for some minor local derogations).

This switch from a Directive to a Regulation is a significant aspect of the GDPR. While much of the focus of GDPR-related discussion in business and in the media has been on the challenges and upheaval of adjusting to new legislation, it isn't all doom and gloom. In the long term, the GDPR will make doing business with EU member states more convenient and provide clearer legislation for global companies dealing with Europe, helping them to navigate and manage their data protection responsibilities.

Whilst previous drafts of the legislation proposed extreme measures, the final regulation is widely considered to be more commercially balanced and more of an evolution of the current law rather than a revolution. It's more about building upon current practices rather than a complete overhaul.

WHAT IT MEANS FOR YOUR BUSINESS

While the GDPR is not a wholescale change of data laws, any organisation that handles personal data on EU residents needs to have a full understanding of the GDPR requirements to be able to review their processes and take any required remedial steps to ensure compliance by May 2018. The amount of preparatory work will depend on the sector in which an organisation operates, with data-reliant industries such as financial services and retail likely to be processing large amounts of personal data.

THE SIX "NEED TO KNOWS"

Below are some top tips for businesses who are preparing for the GDPR:

1 Know your … data protection definitions

It's important to remember that the cornerstone definitions of the current Directive and Data Protection Act 1998 remain generally unchanged under the GDPR. If a business has a good understanding of the concepts of "Personal Data," "Sensitive Personal Data," "Controller," and "Processor," these have not changed and will help their understanding of the GDPR.

There are, however, some notable differences between previous legislation and the GDPR. "Sensitive Personal Data" or, as it is known in the GDPR, "special categories of data" now includes biometric and genetic data (acknowledging the rise in the use of this data in digital services) but excludes criminal convictions data. However, in the UK criminal convictions will still require explicit consent to process.

The second point to note is that "Processors" (i.e., organisations that perform a task on another organisation's personal data as a service provider) will be given legal obligations under the GDPR for the first time, alongside Controllers (i.e., the party who has overall control over the data). Most obligations still fall to the Controller, but it is important that businesses are aware of (a) when they are acting as a Controller and a Processor (many businesses have dual roles depending on the nature of work being carried out) and (b) what their obligations are as a Processor – both to their Controller and to the data-protection authorities.

The definition of a data subject has not changed with the GDPR. But while reviewing the GDPR procedures, it's worth ensuring this definition is properly captured and understood.

The GDPR makes no distinction between private and business activity, and if an organisation deals with unincorporated businesses such as sole traders or partnerships, their data will be personal data, as will data relating to directors and shareholders at incorporated companies. All contact information of individuals at companies (unincorporated or not) will also be covered.

2 Know your … ground for processing

A common area of misunderstanding with the GDPR is around the lawful grounds of data processing. Generally, these standards have not changed from the previous EU Directive. Whatever ground of processing a business currently relies upon will most likely be the ground of processing it will rely on under the GDPR.

Media coverage has focused on consent under the GDPR – namely obtaining the data subject's consent in order to process their data. Consent is not the only grounds an organisation can use to process personal data – and for many organisations, obtaining consent is not the most appropriate either. The UK's Information Commissioner's Office has released a useful briefing* on this topic, highlighting the various alternatives available.

One alternative is the commonly used "legitimate business interest" grounds for processing, which can still be used under the GDPR post May 2018. "Legitimate interests" are those uses of personal data by a Controller that are deemed necessary or reasonably to be expected by a data subject – for example, if data is needed in order to provide a service to an existing customer. In a clear example of the cross-country harmonisation the GDPR will encourage, this will also be extended to countries like Hungary and Spain that have so far not incorporated this concept into domestic legislation.

If an organisation continues to rely on the grounds of legitimate business interest, it must ensure proper execution as the GDPR places new or increased obligations on businesses.

For example:

- Processing under legitimate interest – this must be balanced against the rights and freedoms of the data subject, and when using this ground, businesses must internally record why their legitimate interests are not overridden by the interests or fundamental rights of the data subjects. In addition, businesses must also publicly specify what their own legitimate interests are.
- Processing under consent – the GDPR clarifies that "affirmative consent" is required – i.e., a statement or clear affirmative action – for consent to be valid. This means silence, pre-ticked boxes, or inactivity can no longer be construed as consent. A data subject actively ticking a box or signing a document would be sufficient as long as the relevant information is "clearly distinguishable" from other matters in the documentation. In short, approval can no longer be "hidden" in the middle of lengthy contracts as is so often seen online in particular.

Whatever ground of processing a business relies on will now need to be communicated clearly through its "fair processing notice". This document details the information the GDPR stipulates must be provided to data subjects. This is also sometimes known as a Privacy Notice or Privacy Policy.

When drafting this, it might be tempting to take a 'belt and braces approach' and try to include as many grounds as possible in your fair processing notice. Whilst it's advisable to include all that genuinely apply, organisations should avoid claiming both legitimate interest and consent.

Data Protection Authorities will dimly view businesses that ostensibly process on consent only to claim another ground if such consent is withdrawn, as this makes a mockery of the consent mechanism. Instead, businesses should carefully consider their ground and be able to justify it if ever called upon to do so.

3 Know what … rights your data subjects have

Data subject rights are not a new phenomenon, and all current data subject rights will remain in place under the GDPR, with most being expanded or strengthened. In order to manage data subject rights efficiently, recommended areas of focus include correct and detailed fair processing notices, streamlining subject access requests, efficient procedures to manage "rectify and erasure requests," and restrictions on processing when a subject has raised a rectification query that has not been resolved.

Another important change is the process for responding to a subject access request (SAR) – a written request made by, or on behalf of, an individual for the information a business holds about them. A business now has 28 days to respond under the GDPR rather than the 40-day limit within the current Data Protection Act.

If a business processes data under legitimate business interest, they should also be aware of a change in burden. Currently, the data subject can only demand their data be deleted if they provide the Controller with "compelling legitimate grounds" to do so. The GDPR flips this burden and states that where a Controller processes data under the legitimate interest basis, the data subject can object at any time, and it will be for the Controller to prove compelling legitimate grounds for processing the data.

* https://iconewsblog.org.uk/2017/08/16/consent-is-not-the-silver-bullet-for-gdpr-compliance/

4 Know your … high-risk activities

Every business in every sector will use data in a variety of ways – both internally and in the delivery of certain external services such as personalised communications. Information security is key to mitigating the risk of data breaches or attacks by hackers.

The GDPR includes obligations to carry out a privacy impact assessment to determine the level of risk of a particular activity. In practical terms, this will mean a business needs to assess all of its activities to establish which ones are high risk. From here, the organisation will need to ensure it is mitigating against any dangers and is fully protecting data in those higher-risk situations.

5 Know when … to notify authorities of a breach

For the first time, all organisations controlling personal data within the EU will be under a legal obligation to notify their local data protection authority if they suffer a data breach that could result in harm to data subjects. The deadline for this is 72 hours, which is a challenging time frame for many businesses.

This obligation is something that companies with a US presence will be better prepared for as the emphasis for US privacy is on breach notification.

Businesses will need to thoroughly review the GDPR legislation around this area because not all breaches require notification. A review of current data security processes is recommended to make the necessary changes to ensure a business (a) is able to identify a breach quickly, (b) is able to limit its impact as much as possible immediately, and (c) has the processes in place to escalate internally before making the authorities aware within 72 hours.

6 Know your … international data transfers

The GDPR will do little to simplify the complex process of making data transfers out of the EU.

Companies with subsidiaries inside and outside of the EU should note the inclusion of Binding Corporate Rules (BCRs) in the GDPR. BCRs are a mechanism for intra-company transfers around the world – and are being given a legislative basis for the first time.

“Given an increasingly digitally led and data-based world, Dun & Bradstreet believes that the GDPR is a positive, progressive move forward for all businesses.”

REAPING THE BENEFITS

Given an increasingly digitally led and data-based world, Dun & Bradstreet believes that the GDPR is a positive, progressive move forward for all businesses.

It will put in place an EU-wide set of regulations that will open up opportunities for easier, faster, and more streamlined trade across the EU. And it will ensure that the data businesses hold is protected and used consistently.

While it will require consideration, planning, and, in some cases, a change in business process, the potential compliance and, ultimately, ease-of-trade benefits far outweigh the challenges in being ready for 25 May.

RECOMMENDATIONS

1. Carefully consider which third-party data providers you work with

Not all third-party data providers are equal. You need to understand how your data supplier is processing data, as this will impact your compliance with GDPR in turn. Key things to check include:

- Their grounds for processing and whether they are processing data in the manner it was collected (for example, to manage risk or protect against fraud)
- If they are relying on consent, what the level of that consent is
- Whether they remove private email addresses (or, for unincorporated businesses, they take steps to ensure it is business email)
- Whether they are collecting the minimum data necessary
- How often the data is kept up to date, how it is stored, and what technical and organisational measures they are using to ensure the data is kept confidential

2. Time to overhaul your own data management strategy

Regulation is a catalyst for reviewing current systems and processes. Building a compelling business case to have a strong, robust data management strategy is key. If you are unsure of your data health, you don't really understand your data. Now is the time to establish a common data language across corporate systems.

Dun & Bradstreet data is pre-mastered and structured. We have over 300 million businesses in our database, linked to over 5 million corporate family trees, using our proprietary Dun & Bradstreet D-U-N-S® Number as a unique identifier. Dun & Bradstreet invests more than $1 million every business day in maintaining and enhancing our database of D-U-N-S-numbered entities and linkage relationships, which are updated 5 million times per day. Implementing a common underlying data structure – such as ours, with the D-U-N-S Number at its heart – as a source of truth will not only strengthen your data compliance programme but also deliver against wider organisational goals for growth and operational efficiency – whether you're using it for risk, compliance, procurement, or sales and marketing programmes.

> GDPR does not need to be a problematic revolution."

CONCLUSION

Data is a powerful force in business, which helps firms understand customers and deliver the very best products and services. GDPR does not need to be a problematic revolution. There is a lot of hype and some panic in the marketplace, but the reality is that many of the standards and procedures the GDPR puts in place are based on, and can be adapted from, current data protection legislation.

The key is to be prepared for May 2018: Be rigorous in assessing and truly understanding how your organisation uses data, and remember that this is an evolution of current practice. We live in a digital world where more and more data-led products and services are being created. GDPR will help his future and bring great benefits to all businesses.

dun & bradstreet

ABOUT DUN & BRADSTREET

Dun & Bradstreet (NYSE: DNB) grows the most valuable relationships in business. By uncovering truth and meaning from data, we connect customers with the prospects, suppliers, clients and partners that matter most, and have since 1841. Nearly ninety percent of the Fortune 500, and companies of every size around the world, rely on our data, insights and analytics. For more about Dun & Bradstreet, visit DNB.co.uk.

dnb.co.uk