creditsafe

How prepared are you for GDPR?

Tips and insights to help you protect and grow your business.

Contents

Background of GDPR

On May 25th, 2018, the EU will see the biggest update in its data protection laws over the last 20 years as we welcome the enforcement of the General Data Protection Regulation (GDPR). With GDPR comes many new regulations to the way in which businesses can gather, store and process data; which has naturally become a cause for concern for many businesses. Yet, considering the vast advancement in technology and data over the past two decades and how businesses use of both of these, it is surprising that we have even waited this long.

Why are the regulations being updated now?

Since the most recent update to the UK's data regulation in 1998, we have seen the birth of technological and data advances such as social media and cloud storage to name but a few. With businesses gathering vast amounts of personal data on consumers from behavioural analytics to personal characteristics, the subject of personal privacy and protection has become a major concern. Many companies such as Google and Facebook have even developed extensive business models by trading access to their platforms with the promise that we then share our data with them. While this offers tremendous advancements in the goods and services businesses deliver, it also gives individuals little control over what their data is used for, how it is stored and by consequence, could leave them at threat to theft, fraud and other missuses. However, by strengthening measures, the EU strives to improve trust and reduce the overall threat to individuals.

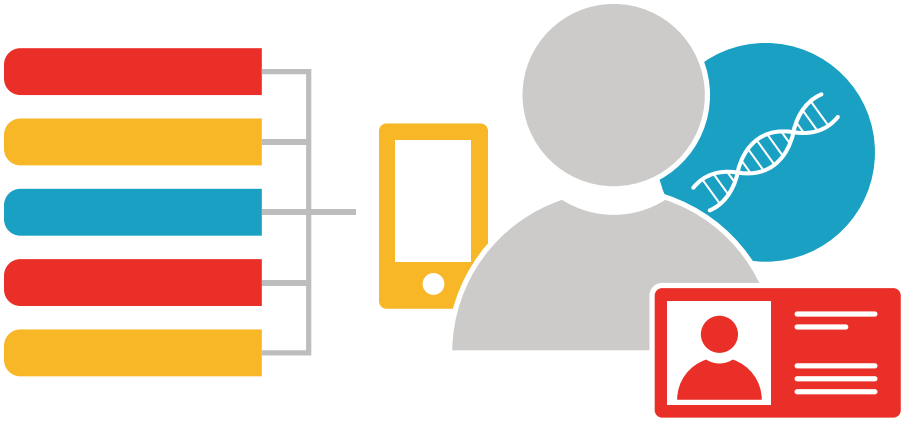
The GDPR aims to harmonise data privacy laws across Europe, creating an equal playing field and more importantly making it simpler for businesses to understand and manage their own compliance.

Who does it apply to?

If you process individuals' personal data, of EU citizens, you need to comply with GDPR. Compliance with the UK's Data Protection Act (1998) is not sufficient.If your activities are limited to the processing of UK citizen data, the position post Brexit is not yet clear, but until Brexit is formal executed compliance with GDPR will be essential.

The UK government and Information Commissioners Office (ICO) has stated it will pass a new Data Protection Bill through parliament with the intention for it to become law in 2018 this new data protection bill is expected to align with and support GDPR even after Brexit with only minor derogations; and given that the UK has historically supported GDPR as an effective data protection standard, it will provide a baseline against which UK businesses can deal with their EU counterparts.

GDPR widens the definition of personal data to encompass anything that can be used to directly or indirectly identify a person. This covers a broad spectrum of data from names, photos, email addresses, bank details and posts on social networking sites to medical information or IP addresses as an example. The new regulation seeks to protect this data, whether its filing is automatic or manual, paper or electronic.



What about B2B communication?

An area for debate has arisen when considering B2B vs B2C data, and what does or does not fall under the remit of GDPR. While B2B businesses may have felt they were exempt from the reaches of GDPR, the line separating personal and business data is not a clearly defined one. An employee's personally assigned work mobile or email address could arguably fall under personal data despite being used for business purposes.

While this leaves some ambiguity, there is another piece of legislation that fills the gap- the Privacy and Electronics Communications Regulation (PERC). PERC clearly defines what rules must be adhered to when it comes to electronic direct marketing communication, including in the B2B sector.

PERC permits businesses to send electronic communications to corporate subscribers (those from incorporated businesses, rather than unincorporated businesses) without prior consent. However, should they choose to unsubscribe or opt-out from marketing communications, the business must then halt any further communication. The rules are much stricter when dealing with individuals from unincorporated businesses such as Sole Traders or Partnerships, which it sees as individual subscribers, rather than corporate subscribers, and therefore require prior consent.

Who is responsible for compliance?

The GDPR devolves accountability to anyone who is involved in the gathering, storing and using personal data. Unlike under the Data Protection Act, responsibility for compliance is not solely tied to the Data Controller. Under GDPR both "controllers" and "processors" are accountable for making sure that the principles of GDPR are followed.

A data controller is a person or group of persons that determine what and for what purpose personal data is gathered and processed. They will control the manner in which personal data is processed, meaning they have ownership over the "why" and "how" of all data processing.

On the other hand, it is the data processors who physically gather and "process" the data on behalf of the data controller. GDPR extends the liability of data protection to all employees that come into contact with personal data, be they data controllers or data processors.

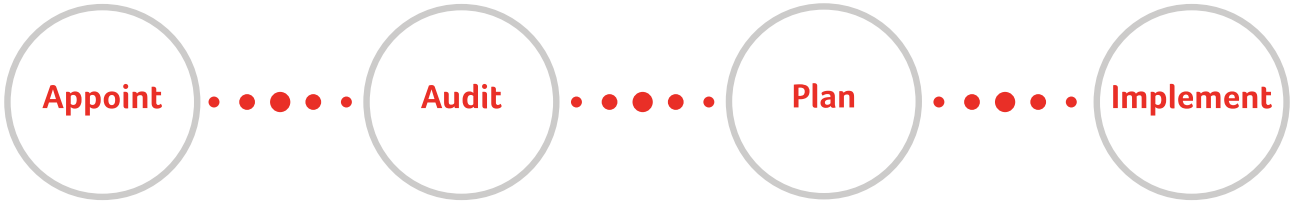
The road to implementation...

Depending on the size and complexity of an organisation, the initial implementation of the GDPR could be very demanding on its resources, including labour and time. Preparing in advance and ensuring that a thorough and realistic roadmap is drawn up will help businesses enormously as they strive for compliance by May, 2018.

The appointment of someone to manage the implementation of GDPR and ensure ongoing compliance is crucial. It may be appropriate, or in some organisations mandatory, to assign a formal Data Protection Officer. This individual will carry the responsibility of advising the organisation of their data protection obligations, monitor its compliance in line with those obligations and be their first point of contact with the Data Protection Authority (DPA).

Performing an audit of your existing data management is strongly recommended. For this, organisations will need to consider how personal data is currently acquired, stored and processed; and assess what transformations are needed to protect this data in line with the GDPR as well as enable data subjects to exercise their rights.

It's clear that the GDPR will have an impact on vast and varied aspects of an organisation, and as a result not one person or even one department can perform the transformation alone. The designated Data Protection Officer, or equivalent, will be required to raise awareness within the organisation and champion the change required. However, all departments and their members must band together and show their support as the business implements and maintains their compliance.



The Key Areas of GDPR

Accountability

Data Controllers must be able to demonstrate the organisations compliance with the GDPR. However, it is the accountability of both processors and controllers to ensure the correct procedures are followed.

Transparency

Organisations will have to be open and transparent about why they are collecting personal data and what they intend to do with it. This means explaining to the data subject what they intend to use their data for upfront and gaining consent.

Processing personal data

Personal data can only be collected for specified, explicit and legitimate purposes, and not processed in any further capacity that doesn't meet these purposes. Consequently, data legitimately gathered for one purpose cannot then be used for another objective unless they gain consent from the data subject or have a legitimate purpose to do so.

Right to Access

Data Subjects have the right to access their personal data within 30 days of a request. Organisations have a responsibility to ensure inaccurate data is updated or erased; giving data subjects the right to verify and amend personal information that is held on them.

Right to be forgotten

Data Subjects also hold the right to request that his/her personal data is removed, provided that there is no legitimate grounds for keeping it.

Data Protection by default (Privacy Impact Assessment)

GDPR calls that we evaluate the amount and length of time for which we hold personal data. In circumstances that pose high risk, a Privacy Impact Assessment may be required. It also states that if personal data is gathered on an individual, the organisation should not collect any data in excess of what is necessary for the purpose intended.

Fines for impacting privacy or breeching rights

Fines of up to 4% of annual turnover or 20 million euros, whichever is higher, could be imposed for breaches of GDPR.

Reporting Breaches

In the event of a data breach which could impact the individual or cause harm, the data controller is required to notify the supervisory authority in no later than 72 hours after the data breach was detected.

Departmental Considerations

Every organisations' application of GDPR will be unique to their operations, organisational structure and the nature of the data they gather. That said, there are some common areas for specific departments to consider across many different industries and specialisms.

Marketing & New Business Development

Quality data is an essential resource for our New Business and Marketing departments, which they continually work to gather, enrich and cleanse any data captured. Consequently, businesses often, but somewhat mistakenly, view the data they have gather as "their database" rather than belonging to its true owners, the Data Subjects.

Historically in the UK, the rules on who a business could contact were fairly limited; dictated by opt-out lists and the TPS. Yet, come May 2018 the GDPR turns this on its head, stressing the importance of the data subject's rights and that businesses must adhere to one of 6 grounds for holding and utilising personal data.

For new business and marketing, email is one area in which the new laws are going to have a seismic effect. If you currently send email campaigns, you need to make sure your audience has opted in to receive information, they are clear about the use of opt in data and that you have a record of when and where that person opted in.

As well as impacting your existing mailing list, GDPR will affect list buying. The power now lies with the recipient. In order for an organisation to communicate lawfully with an individual, they must have consented to you contacting them or you must have a legitimate interest to do so.

For many new business departments, holding a legitimate interest will, by large, be the designated grounds for communication with prospects. Yet, this must be approached with caution to ensure that you are carefully selecting prospects with which you have a legitimate interest to communicate with. With this in mind, narrowing down your target audience to ensure that your message is aligned with their needs is a crucial component for legitimate interest. At Creditsafe our marketing data is customisable on over 22 different variables, allowing organisations to be precise with their targeting for specific and relevant communication with their chosen audience.

For more details on our range of marketing solutions speak to us on 02920 886 500.

Compliance, HR, Recruitment and anyone conducting checks on individuals.

The common organisational belief that "more data is better" comes under scrutiny with the GDPR, creating a degree of conflict for some business areas, particularly compliance departments responsible for carrying out checks on individuals. For a department concerned with the protection of not only the business but also society, ensuring that enough data is gathered for comprehensive checks, which minimise the risk of false negatives, is understandably a priority.

However, in its aim of increasing the protection of personal data, GDPR concerns itself with the amount of data a business holds on an individual. The data held should be what is required to perform the action and meet the specific objective, and no more.

Compliance teams need to be mindful of the information they hold on individuals and be transparent with the individual as to what the data is being used for. Online checks from Know Your Customer and employment screening to Anti Money Laundering, have become increasingly favourable for businesses in recent time, allowing organisations to tailor their checks to their specific requirements, practices and approach to risk.

Our compliance solutions are fully customisable, allowing organisations to specify which checks are required. We also adhere to the highest levels of security standards, providing organisations the confidence that our data centres are fully protected for disaster recovery.

For more details on our compliance solutions speak to us on 02920 886 500.

Keeping customer records up to date

The GDPR stipulates that we should always strive to ensure that any personal data we hold in our database is accurate and up-to-date where necessary. Yet, clients won't necessarily think to update your business when they change details such as address or mobile number.

This application of GDPR is as much a friend to the businesses as the individual. Holding out of date information doesn't serve your business. Whether it's time, money or other precious resources within businesses, these are regularly wasted when employed with outdated information.

Using a blend of official records and publicly available data, online solutions can cross reference and validate your information, so you know how relevant and, more importantly, how accurate it is. At Creditsafe we're able to confirm, cleanse and enhance your database to reduce the costs involved with expensive and misdirected communications and more importantly improve the accuracy of the personal data you hold.

For more details on our data cleansing and enhancement solutions speak to us on 02920 886 500.

Data Privacy & Legal

These departments have an instrumental role in the implementation and maintenance of GDPR compliance within the business. Although accountability is devolved throughout the business, it remains the responsibility of those in charge of information security and data to review and create processes and procedures that meet the stipulations of this new regulation.

Leaders in these areas must have a clear and organised system for how their data is housed, and above this, they must equip their systems with effective encryption, as well as log management and incident management tools. Such tools will allow these departments to meet their other requirements, most notably to grant access to all information held on an individual, to that individual, within 1 month if and when requested.

Click here to view Creditsafe's GDPR Compliance Statement