sage

General Data Protection Regulation (GDPR):

The Sage quick start guide for Australian and New Zealand businesses

Contents

Introduction

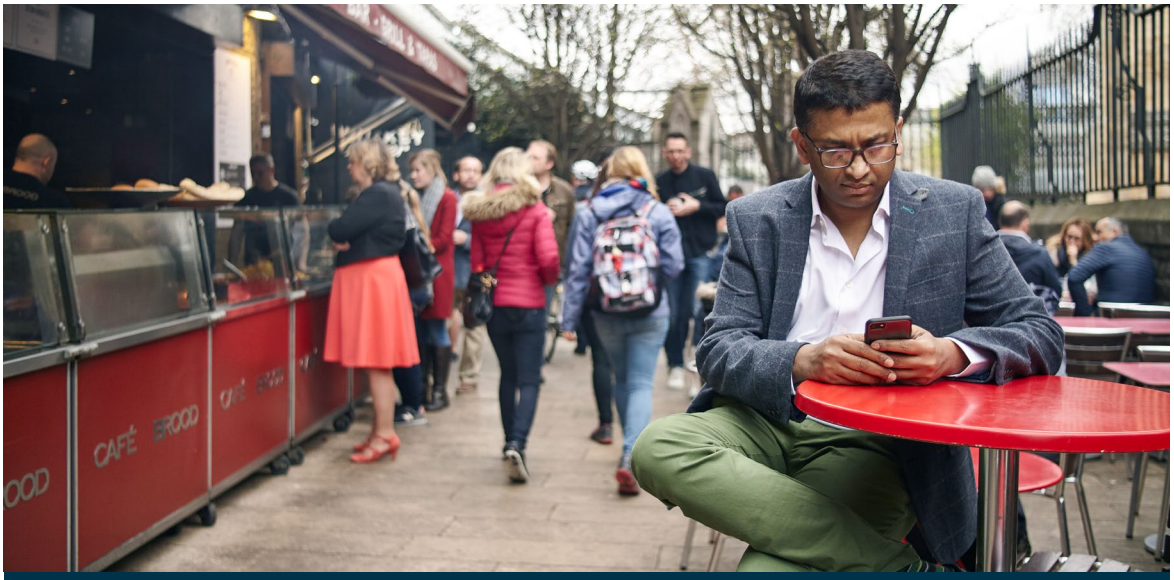
The General Data Protection Regulation ("GDPR") is the new legal framework that will come into effect on the 25th of May 2018 in the European Union ("EU"). EU Regulations have direct effect in all EU Member States, meaning the GDPR will take precedence over any national laws.

As an Australian or New Zealand organisation that offers goods or services to individuals in the EU – whether directly or through a third party – you will need to comply with the GDPR's obligations. Your organisation is bound to comply even if it doesn't have a physical presence in the EU.

The GDPR's focus is the protection of personal data, i.e. data about individuals. In fact, GDPR is one of the biggest shake-ups ever seen affecting how data relating to an individual should be handled—and potentially it affects not just companies but any individual, corporation, public authority, agency or other body that processes the personal data of individuals who are based in the EU. This includes suppliers and other third-parties a company might utilise to process personal data.

It has a surprisingly extensive scope, including all Member States of the European Union along with the UK post-Brexit in 2019, as the GDPR will be also incorporated into UK law. Unlike the EU Directive 95/46 personal data protection rules, the GDPR also affects any companies outside of the EU.

The GDPR has massive implications for every department of many businesses worldwide. Some might need to employ or assign a Data Protection Officer, for example. Nearly all will need to put in place additional practices and safeguards. An audit by a suitably-qualified individual is highly recommended and with the prospect of incurring fines of up to 4% of annual global turnover or 20 million Euros, whichever is the greater, knowledge of GDPR should be considered mandatory.



This document is intended to be a concise and simplified guide for businesses. More information can be found via the Office of the Australian Information Commissioner or the New Zealand Office of the Privacy Commissioner. Please read the Sage Legal Disclaimer set out at the end of this guide.

Infographic:

GDPR at a glance

General Data Protection Regulation (GDPR)

Consent

Must be confirmed by a statement or other clear affirmative action. You cannot assume consent or even use pre-checked website boxes

Individual rights

Significantly expands the rights of individuals and what information they must be provided with regarding processing activities

Data Protection Officer

Might be obligatory. Requires expert knowledge of data protection law. Could be an employee or via a service contact

Penalties

Could be up to 4% of annual global turnover, or €20m, whichever is greater. You might be fined even if there is no actual loss of data

Privacy from start to finish

Privacy considerations must be built-in everywhere and only data strictly required for stipulated purpose can be used

Data portability

Individuals now have the right to move, copy or transfer personal data—even to a competitor

Wider scope

Covers your business, plus those who process data for you—even outside the EU

Mandatory breach reporting

Data controllers must tell local supervisory authorities, such as the ICO in the UK, within 72 hours of becoming aware. In serious breaches individuals must be informed

The basics

The GDPR sets out the minimum requirements for the treatment of all personal data. Personal data can be defined as any data identifying or relating to an individual in most ways (including things like physical appearance or even biometric data).

Most businesses collect personal data from the minute they interact with an individual, and in some cases might not even be aware they've done so. For example, personal data collection might be as elementary as website tracking cookies that identify a user of your website. It runs all the way through to something as detailed as an individual's record on a customer relationship management ("CRM") database, and far beyond. The personal data might be collected or processed for the sole benefit of the individual but this still falls under the remit of the GDPR.

As with the EU Directive 95/46 legislation, the GDPR restates three basic sets of rules that relate to personal data: Data Protection Principles, Lawful Processing, and restrictions on International Transfers. Most businesses should already be aware of these, and many individuals will be aware too. These three sets of rules are described in greater detail in this document, and are well worth reading even if only as a refresher for existing knowledge.

However, the GDPR introduces several major new requirements.

The GDPR in summary

Here are the key areas of the GDPR, with particular reference to the EU Directive 95/46 data protection directive.

Individual rights—and informing people about them

The current EU data protection legislation (Directive 95/46) gives individuals rights over their personal data and describes what information individuals have to be provided with by businesses, including information about what that business was going to do with that personal data. Often this was done via privacy statements or notifications provided on a website.

The GDPR extends this significantly, providing additional rights that must again be communicated to individuals. In particular, individuals must be informed that they have the following (non-exhaustive) rights:

1. to complain to supervisory authorities, such as the ICO in the UK;
2. to withdraw their consent to processing of their personal data (see below);
3. to access their personal data and have it rectified or erased (the 'right to be forgotten') by the business and also any third-parties that have accessed it;
4. to be informed of the existence of any automated personal data processing (including profiling);
5. to object to certain types of processing, e.g. direct marketing and decisions based solely on automated processing;
6. to be told how long their personal data will be held for;
7. to be provided with details of any appointed Data Protection Officer (see below).

In addition, individuals have the right to ask non-profit organisations to exercise rights and bring claims on their behalf, similar to a US style class action.

Consent

If you are collecting data based on the consent of individuals, while EU data protection legislation has always required such consent to be freely-given, specific and informed, with the GDPR this has to be confirmed by a statement or other clear affirmative action. In other words, pre-ticked consent boxes on websites, or silence/inactivity on behalf of the individual after reviewing a privacy statement, will not constitute consent.

Additionally, consent cannot be one-size-fits-all, so a business can't use an individual's single consent at one stage in their business dealings as consent for other kinds of personal data processing. Separate consents

are required for different personal data processing operations.

Finally, individuals must not only be informed they have the right to withdraw consent at any time but it must be as easy for them to withdraw consent as it was to give it.

Existing consents given by individuals should be revisited to make sure they comply with the requirements of the GDPR. If there are conflicts or ambiguities then companies will need to either establish a new lawful basis for processing the data (e.g. it's necessary for the performance of a contract), get new consent, or cease processing that personal data.

Right to move or transfer personal data (data portability)

Individuals now have the right to move, copy or transfer their personal data from one place to another, even to a competitor. For example, a playlist might be generated for a user by a music service, and should they switch to a new provider then they can take this with them. As such, the personal data needs to be in a structured, commonly-used and machine-readable format so it can easily be utilised and shared.

The requirement to make data truly portable and easy-to-use by others is likely to incur significant IT adjustments and therefore costs.

Much wider scope

Put simply, the GDPR makes liable for breaches not just the business that collects the personal data, but also any third-party that processes the personal data on behalf of that business, whether that's another business, organisation, or individual. However, this does not mean a business can simply hand the personal data to a third-party and then cast a blind eye. The business must ensure the third-party supplier is also compliant with the GDPR.

Additionally, the potential geographical scope is extended beyond just the EU to any business—or again to any third-party processing personal data on its behalf—who offers goods or services to individuals in the EU, or who monitors the behaviour of individuals in the EU. Notably, it doesn't matter whether or not payment is required for the goods or services, so the likes of charities and NGOs fall under the GDPR.

Because the EU is a trading partner of most countries, the GDPR's wider scope means it has implications for many businesses worldwide, and will effectively require them to be compliant if they wish to operate in EU member states either directly or as a third-party for others.

Proof of compliance

It's not enough to merely comply with the GDPR. A business needs to prove it's doing so under the GDPR's requirement for "accountability", and this means complying with some rather onerous record-keeping requirements. In particular, records should be maintained that detail processing activities*, subject access requests, breaches, how consents are obtained, and Privacy Impact Assessments (see below).

This requirement again also affects those third-parties processing personal data on a business' behalf, although the requirements are not as detailed.

** Applies to companies employing more than 250 people, or companies employing fewer people where the processing carried out is likely to result in a risk to the rights and freedoms of individuals, is not occasional, or includes Special Categories of Data, such as information on health, religion or sexual orientation.*

Privacy from start to finish

Technical and organisational measures need to be in place throughout the lifetime of the personal data to match the privacy expectations of the individual—from inception through to execution and finally cessation of that activity. This is referred to as "Privacy by Design", meaning that privacy considerations must be built into every aspect of that processing by design.

Additionally, only the personal data strictly required for that purpose should be actually processed—something referred to as data minimisation or "Privacy by Default".

In reality, implementing Privacy by Design and Privacy by Default will involve continuous training, undertaking regular audits, minimising the data collected, restricting access to personal data to a need to know basis, and implementing appropriate technical and organisational security measures such as pseudonymisation and encryption.

Mandatory breach reporting

In the event of a breach of the GDPR, companies collecting personal data must tell supervisory authorities—such as the ICO in the UK—within 72 hours of becoming aware. Third-parties processing the personal data on behalf of those companies must tell that business without undue delay.

If the breach poses a high risk to the individuals concerned, companies must also notify the affected individuals without undue delay.

Data Protection Officer (DPO)

Under the GDPR companies and any third-parties that process personal data on their behalf will need to appoint a Data Protection Officer ("DPO") if: (i) they are a public body; (ii) if the core activities of the business or third-parties involve monitoring of individuals on a large scale; or if the core activities consist of processing on a large scale of special categories of personal data, including data relating to criminal convictions and offences. The DPO needs to have expert knowledge of data protection law, although doesn't necessarily need to be an employee and could instead be employed on a service contact to fulfil the role. Details of the DPO will need to be communicated to the supervisory authority, such as the ICO in the UK.

Penalties

The penalties for non-compliance with the GDPR are tough and could be up to 4% of annual global turnover, or €20m, whichever is greater. You might be fined even if there is no actual loss of data. One thing to note is that there are no exclusions or exceptions for small businesses. Additionally, there is the ability for individuals to file a class action lawsuit requesting a formal regulatory investigation if a business does not comply with the GDPR.

Brexit

Following the UK general election in 2017 the Conservative government was returned for a five-year term. During this term, specifically in 2019, the UK will leave the European Union. As with all EU member states, the GDPR will apply to the UK until that time. However, in the announcement for new legislation following the election it was stated that new data protection laws will do the following:

"... implement the General Data Protection Regulation and the new Directive which applies to law enforcement data processing, meeting our obligations while we remain an EU member state and helping to put the UK in the best position to maintain our ability to share data with other EU member states and internationally after we leave the EU."

Source: Queen's Speech, June 2017

Therefore, it is possible, but cannot be assumed, that post-Brexit the UK will be considered a country deemed to provide 'adequate' protection by the European Commission, so may not be affected by potential issues such as data protection transfer prohibitions. Watch this space to learn more about future decisions.

The new UK legislation replaces the Data Protection Act 1998, that was based on EU Directive 95/46.

GDPR basic principles

In addition to new requirements detailed earlier, and as with the EU Directive 95/46, the GDPR restates three basic sets of rules relating to personal data. In simple terms these can be outlined as follows:

- ***Data Protection Principles:*** Personal data must be processed lawfully, fairly and in a transparent manner in relation to the individual concerned. It must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with this. Personal data collected must be adequate, relevant and limited to what's necessary. It must be accurate and kept up to date, and every reasonable step must be taken to ensure that personal data that's inaccurate is erased or rectified without delay. It must be stored in a way that identifies the individual for only so long as it's needed, and it must be processed in a way that ensures appropriate security—including protection against loss, destruction, or damage, and unauthorised or unlawful access.
- ***Lawful Processing:*** Processing of personal data is only lawful if at least one of the following applies: the individual has given consent for one or more specific purposes; it's necessary for a contract to which the individual is a party, or will soon be; a legal obligation must be complied with (e.g. submission of tax records by a business); there's a task that's in the public interest or is carried out in the interest of official authority; it's necessary for legitimate interests (or those of a third party) except where overridden by the interests, fundamental rights and freedoms of the individual.
- ***International Transfers:*** The GDPR continues the general prohibition on sending personal data outside the European Economic Area to a country that does not provide adequate protection. At the time of writing, the countries deemed by the European Commission to provide "adequate" protection are: US companies that self-certify to the European Union-US Privacy Shield arrangement (note: this does not mean the US as a country is considered to provide adequate protection), Andorra, Argentina, Canada (limited to PIPEDA), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, and Uruguay. Where no adequacy decision exists, transfers can only be made in limited circumstances, including on the basis of consent, the use of standard contractual clauses published by the European Commission or, in the case of inter-company transfers, the use of Binding Corporate Rules.

Actions you can take now

- To learn more about the GDPR and your requirements, visit the *Office of the Australian Information Commissioner* or the *New Zealand Office of the Privacy Commissioner*.
- Review your personal data collection and data processing systems to ensure they're in line with the GDPR. You might consider a GDPR audit from both legal and technological standpoints, amongst others.
- Ensure your employees and partners are aware of the GDPR and secure training to prepare them. Remember the GDPR makes you also responsible for third parties who process personal data for you.
- Seek legal advice to better understand the implications of the GDPR on your businesses.

To learn more, visit:
Sage.com/GDPR

Sage Legal Disclaimer

The information contained in this guide is for general guidance purposes only. It should not be taken for, nor is it intended as, legal advice. We would like to stress that there is no substitute for customers making their own detailed investigations or seeking their own legal advice if they are unsure about the implications of the GDPR on their businesses.

While we have made every effort to ensure that the information provided in this guide is correct and up to date, Sage makes no promises as to completeness or accuracy and the information is delivered on an "as is" basis without any warranties, express or implied. Sage will not accept any liability for errors or omissions and will not be liable for any damage (including, without limitation, damage for loss of business or loss of profits) arising in contract, tort or otherwise from the use of or reliance on this information or from any action or decisions taken as a result of using this information.

© 2018 The Sage Group plc or its licensors. Sage, Sage logos, Sage product and service names mentioned herein are the trademarks of The Sage Group plc or its licensors. All other trademarks are the property of their respective owners.