GDPR

THE ESSENTIALS

POCKET GUIDE

DATA mindset

Gordon Hazle

DISCLAIMER: The Author accepts no responsibility for any damages or costs caused or incurred by using this book or following the information contained it in. This is NOT legal advice.

This information is created from personal research with information obtained from official sources, where possible, and from information that is in the public domain.

Whilst the author has experience in GDPR is not a lawyer and this content cannot be deemed as legal advice.

This is not an official document endorsed by or associated with the ICO nor any other government body, it is intended for information purposes only, It is not legal advice and the author accepts no responsibility or liability for any consequences.

Using this document and the information contained within it, is at your own risk.

Contents

Part I: What you need to Know

What GDPR stands for?

General Data Protection Regulation

Why GDPR?

The European Commission set out plans for data protection reform in January 2012.
Its mission to make Europe 'fit for the digital age'. It took almost four years for agreement to be reached on what was involved and how it would be enforced.

As the biggest component of its new data protection reforms is the General Data Protection Regulation (GDPR) came into effect on 25th May 2018. A European union wide framework applies to organisations in every member-state and impacts not only businesses and individuals across Europe, but globally. Because, if a company uses personal data of someone residing within the EU, then GDPR applies. Even if that company is based outside of Europe.

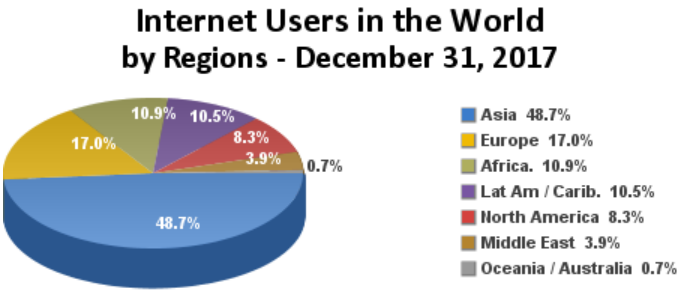
In December 2015, when the reforms were agreed, Andrus Ansip, vice-president for the Digital Single Market said "The digital future of Europe can only be built on trust. With solid common standards for data protection, people can be sure they are in control of their personal information".

What is GDPR?

GDPR is designed to give EU citizens more control over their personal data. It claims to simplify regulations so citizens and businesses in the EU can get maximum benefit from the 'digital economy'.

Many of the laws and obligations surrounding personal data, privacy and consent were outdated. The latest reforms are designed for the internet-connected world we live in today where nearly every aspect of our lives revolves around the collection and analysis of our personal data. Today's world is one where governments, banks, social media networks, and mobile apps record; what we buy, what we read, where we go, and what we eat, and this 'data' and more is willingly pushed into the public domain by almost 3 billion people worldwide (Source: https://www.internetworldstats.com) and 85.7% of Europeans (Source:

https://www.internetworldstats.com/stats9.htm#eu) who are connected to the internet.



Source: https://www.internetworldstats.com

Graph https://www.internetworldstats.com/images/world2017Q4pie.png

Who does GDPR apply to?

GDPR applies to any organisation operating within the UK or EU, as well as any organisations outside of the Region which offer goods or services to customers or businesses in the Region. So GDPR applies to organisations outside the EU that offer goods or services to individuals inside the EU.

That means almost every major business in the world needs to pay attention to GDPR.

Article 4 of the General Data Protection Regulation identifies two different types of data-handler that the legislation applies to. Data 'Processors' and Data 'Controllers'.

What is a Data Controller?

A Data Controller is a "person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of processing of personal data".

What is a Data Processor?

A Data Processor is a "person, public authority, agency or other body which processes personal data on behalf of the data controller".

The UK's Information Commissioner's Office, or ICO, is the authority responsible for; registering data controllers, taking action on data protection issues and handling concerns regarding mishandling of data in the UK, states that "You now have significantly more legal liability if you are responsible for a breach. These obligations for data processors are a new requirement under the GDPR".

GDPR makesdata controllers and processors responsible for maintaining and processing personal data records, with a much higher level of legal liability in the event of any breaches.

Data Controllers also need to ensure that all contracts with data processors are also compliant with GDPR.

What is a Data Subject?

A Data Subject is the term used in the GDPR to define individuals. The GDPR is there to protect data Subjects. A Data subject refers to any individual who has given their personally identifiable data. If you cannot identify an individual from the data provided by a person then that data would fall outside of GDPR.

A data subject can be from anywhere in the world but it has to be a living person. If a person is deceased, their data rights are not covered by GDPR. Corporations or other entities can't be a data subject.

The term data subject covers a broad remit. Perhaps more recognisably it refers to consumers. Any customer or any prospect who has interacted with your business is a data subject. But the term data subject is broader than just consumers it also includes employees. If you hold data about your employees for example their name address and National Insurance number, they are therefore data

subjects in their own right and have the same data privacy rights as your customers under GDPR.

And finally, don't forget all those business contacts you have. You probably have lots of names, Phone numbers and email addresses for business contacts stored. If you can identify an individual from that data then those individuals are also Data Subjects even though it is data about their work place.

What is GDPR compliance?

It is widely accepted and frighteningly commonplace for data breaches to happen. There are many ways our personal data can be made available to people who have malicious intent and were never supposed to have access to this data.

Under GDPR, organisations now have to ensure that personal data is gathered under strict legal conditions and those who collect and manage it are be obliged to protect it or face serious penalties and hefty fines.

What GDPR means to you?

GDPR expanded the previous definition of personal data to not only include name, address, and photographs, but also things like an IP address, biometric and genetic data. In fact any piece of data that could, on its own or in combination with other data, be used to uniquely identify an individual.

There are specific data types within the GDPR.

Is commercial data covered by GDPR?

Lots of data falls outside of GDPR. Any data that you can't identify a person from or link back to them in anyway is outside of it.

This might include your financial performance data how many products have sold the details of those products how many people have visited your website.

Any data that is anonymised, for example a post code is not covered by GDPR. You can't link a post code back to a single individual therefore it falls outside of GDPR. Where this data becomes more

relevant is when you begin to link it to data that does identify an individual. For example data that says Mrs Smith purchased 4 widgets, increases the sensitivity of that data and is now specifically about that individual. Whereas storing a customer from Bristol bought 4 widgets would not be personally identifiable and therefore falls outside GDPR.

What is Personally Identifiable Data?

The first type of data to be included inside GDPR is data where you can identify an individual or the data is unique to them. This data, officially called Personally Identifiable Information or PII for short, is data that can be used to identify a single individual. This can be as simple as a name, a date of birth, or an email address, a car registration number or even an IP address or device ID from your website visitors. All of these can be resolved back to a single individual and therefore is the first class of data covered by GDPR.

What is Special Category Data?

There is a second class of data covered by GDPR and is data that must be managed with particular care. It carries a higher level of sensitivity and is likely to have a bigger impact on a person if it became public. The GDPR defines this as Special Category data. The following are examples of Special Category Data:

- racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data;
- Biometric data (where used for identification purposes);
- Data concerning health
- Data concerning a person's sex life or sexual orientation.

This does not include personal data about criminal allegations, proceedings or convictions, as separate rules apply.

This isn’t an exhaustive list. If you think you might be processing sensitive data, you should consult the ICO website for a full list of Special Category Data.

It is very important that you always ensure that your processing complies with all principles and requirements of the GDPR. This data is taken particularly seriously by the ICO because of the impact this data could have on somebody.

The rules around special category data are far more stringent and if you are processing this type of data you have specific conditions that you must meet. In particular you should gain explicit consent from the Data Subject.

What does GDPR mean for businesses?

GDPR is a single set of rules that apply to all companies doing business within EU member states, meaning that the legislation extends outside the borders of Europe itself. Many International organisations based outside of Europe, conducting activities on 'European soil' still need to comply.

The European commission hopes to save €2.3 billion annually across Europe, by making it simpler and cheaper for businesses to operate. They also claim GDPR will encourage innovation by persuading companies to build data protection safeguards like data 'pseudonymization' into new products and technologies at the initial development stage, by fostering a 'data protection by design' culture.

What does GDPR mean for consumers?

In order to ensure EU citizens can take appropriate measures to prevent any leaked personal data being abused, consumers are given the right to know when their data has been hacked, within 72 hours of the organisation first becoming aware of it. Especially when it is likely to result in a risk to the rights and freedoms of individuals or lead to financial loss, loss of confidentiality, discrimination, economic or social disadvantage, or reputational damage.

Consumers now have more control over how their personal data is processed, with companies and government bodies now being required to explain, in a clear and understandable way, how they intend to use customer information and requiring them to actively opt-in to receive specific emails and texts. Furthermore, consumers should be provided with an easy way of opting out, if they change their minds about their details being on a mailing list.

When is a Data Protection Officer required?

An organisation must appoint a Data Protection Officer or DPO, if it is a public authority, or if it carries out large-scale processing of special categories of data, or large-scale monitoring of individuals such as behavior tracking.

But all organisations need to ensure they have the skills and staff necessary to be compliant with GDPR.

There's no set criteria on who should be a DPO or what qualifications they should have, but according to the Information Commissioner's Office, they should have professional experience and data protection law proportionate to what the organisation carries out.

What are the GDPR fines and penalties?

Fines of 20 million euros or up to four percent of the company's annual global turnover could be imposed for failure to comply with GDPR, depend on the severity of the breach.

Ignoring subject access requests, unauthorised international transfer of personal data, or failure to put procedures in place that result in the infringements of the rights of data subjects could mean a fine of 10 million euros or two percent of worldwide annual turnover (whichever is greater).

And companies can now be impacted in other ways. The ICO can investigate a business that has received a complaint from a Data Subject and instead of fining, if processes are deemed by the ICO to be putting data privacy at risk, are able to enforce that data processing is stopped. As well as the disruption of an investigation, this could prevent businesses from actively selling products.

Brexit and GDPR?

Despite the UK having now left the EU and at the time of writing, in the “transition Period”, the ICO have already confirmed that GDPR will continue in its current form until at least December 2020. The GDPR has been enacted into UK law as the Data Protection Act 2018. What happens after the transition period is anyone’s guess, however, it is our opinion that it is unlikely to be relaxed significantly. The ICO was a significant contributor to the creation of the GDPR in the first place.

It is worth remembering that GDPR covers EU citizens regardless of where in the world a business is based. So UK business that attract customers from the EU will still need to comply.

Part II: Check your GDPR compliance – are you doing these 12 things!

Awareness

Have you communicated with people in your business about GDPR and what they need to do to be compliant?

> *You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have and identify areas that could cause compliance problems under the GDPR. It would be useful to start by looking at your organisation's risk register, if you have one. Implementing the GDPR could have significant resource implications, especially for larger and more complex organisations. You may find compliance difficult if you leave your preparations until the last minute.*

Information your business holds

Did you document what personal data you hold, where it came from, and who you share it with.
If necessary did you do an Information Audit?

The GDPR requires you to maintain records of your processing activities.
It updates rights for a networked world. For example, if you have inaccurate personal data and have shared this with another organisation, you will have to tell the other organisation about the inaccuracy so it can correct its own records. You won't be able to do this unless you know what personal data you hold, where it came from and who you share it with. You should document this. Doing this will also help you to comply with the GDPR's accountability principle, which requires organisations to be able to show how they comply with the data protection principles, for example by having effective policies and procedures in place.

Communicating privacy information

Have you updated your privacy notices to clearly state what data you collect, and what you do with it?

When you collect personal data you currently have to give people certain information, such as your identity and how you intend to use their information. This is usually done through a privacy notice. Under the GDPR there are some additional things you will have to tell people. For example, you will need to explain your lawful basis for processing the data, your data retention periods and that individuals have a right to complain to the ICO if they think there is a problem with the way you are handling their data. The GDPR requires the Information to be provided in concise, easy to understand and clear language. The ICO's Privacy notices code of practice reflects the new requirements of the GDPR.

Covering all Individuals' rights?

Do your procedures adequately cover all the rights (listed below) that individuals have, including how you can delete personal data or provide data electronically and in a commonly used format.
The GDPR provides the following rights for individuals:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

On the whole, the rights individuals will enjoy under the GDPR are the same as those under the DPA but with some significant enhancements. If you are geared up to give individuals their rights now, then the transition to the GDPR should be relatively easy. This is a good time to check your procedures and to work out how you would react if someone asks to have their personal data deleted, for example. Would your systems help you to locate and delete the

data? Who will make the decisions about deletion?

The right to data portability was new in the GDPR legislation. You need to make sure you have procedures in place to accommodate this.
The right to data portability only applies:
· to personal data an individual has provided to a controller;
· where the processing is based on the individual's consent or for the performance of a contract;
· when processing is carried out by automated means.

You will need to provide the personal data in a structured commonly used and machine-readable form and provide the information free of charge.

Dealing with subject access requests

Do you have procedures in place to handle requests from data subjects to access their data.
In essence you need to:

- *Provide this service for free*
- *Complete Requests within one month*
- *If the requests are excessive or unfounded, you can refuse, but you have to say why.*

> *If your organisation handles a large number of access requests, consider the logistical implications of having to deal with requests more quickly. You could consider whether it is feasible or desirable to develop systems that allow individuals to access their information easily online.*

Lawful basis for processing personal data

You need to identify the lawful basis for processing data, document it and update your privacy notice to explain it. (to comply with GDPR accountability requirements)

Many organisations will not have thought about their lawful basis for processing personal data. Under the current law this does not have many practical implications. However, this will be different under the GDPR because some individuals' rights will be modified depending on your lawful basis for processing their personal data. The most obvious example is that people will have a stronger right to have their data deleted where you use consent as your lawful basis for processing.

Consent

You should now be obtaining, recording and managing consent in accordance with GDPR. All prospects in your database should have agreed to have their data processed by you by positively Opting-in specifically to each type of communication you send. If not they should have been removed from your list.

You should read the detailed guidance the ICO has published on consent under the GDPR, and use your consent checklist to review your practices. Consent must be freely given, specific, informed and unambiguous. There must be a positive opt-in – consent cannot be inferred from silence, pre ticked boxes or inactivity. It must also be separate from other terms and conditions, and you will need to have simple ways for people to withdraw consent. Public Authorities and employers will need to take particular care. Consent has to be verifiable and individuals generally have more rights where you rely on consent to process their data.

Children

If you offer services or handle data that belongs to children, if any children are under 16 years of age, you should have parental consent recorded, to process the data.

> *For the first time, the GDPR will bring in special protection for children's personal data, particularly in the context of commercial internet services such as social networking. If your organisation offers online services ('information society services') to children and relies on consent to collect information about them, then you may need a parent or guardian's consent in order to process their personal data lawfully. The GDPR sets the age when a child can give their own consent to this processing at 16 (although this may be lowered to a minimum of 13 in the UK). If a child is younger then you will need to get consent from a person holding 'parental responsibility'.*

Data Breaches

Do you have the right procedures in place to detect, report and investigate a personal data breach?

> *The GDPR introduces a duty on all organisations to report certain types of data breach to the ICO, and in some cases, to individuals. You only have to notify the ICO of a breach where it is likely to result in a risk to the rights and freedoms of individuals – if, for example, it could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.*

Data Protection Officer

Do you have a Data Protection Officer, in one is needed? Did you check if you were formally required to have one?

Designate someone to take responsibility for data protection compliance. Assess where this role will sit within your governance arrangements. Consider whether you are required to formally designate a Data Protection Officer (DPO).
You must designate a DPO if you are:
· a public authority (except for courts acting in their judicial capacity);
· an organisation that carries out the regular and systematic monitoring of individuals on a large scale; or
· an organisation that carries out the large-scale processing of special categories of data, such as health records, or information about criminal convictions. The Article 29 Working Party has produced guidance for organisations on the designation, position and tasks of DPOs.

Data Protection by Design and Impact Assessment

The GDPR made privacy by design a legal requirement, called 'data protection by design and by default'. It also makes 'Data Protection Impact Assessments' mandatory in certain circumstances you need to make sure any new projects you start are compliant.

A DPIA is required in situations where data processing is likely to result in high risk to individuals, for example:
· where a new technology is being deployed;
· where a profiling operation is likely to significantly affect individuals; or
· where there is processing on a large scale of the special categories of data.

Cross-border Processing

If you operate in several EU member states, you should have selected a lead data protection supervisory authority and have it documented. The Article 29 Working party produced guidance on identifying a controller or processor's lead supervisory authority.

> *The lead authority is the supervisory authority in the state where your main establishment is. Your main establishment is the location where your central administration in the EU is or else the location where decisions about the purposes and means of processing are taken and implemented.*

Conclusion

There is no escaping the fact that wherever physically located, now that GDPR is fully established, ‘all organisation’s dealing with EU citizens (and UK citizens post-Brexit), now need to ensure they've carried out all the necessary impact assessments and are compliant.

Useful Information

ICO Helpline

The ICO has a helpline if you need support. There is consistently high demand for support so it is advisable, before you contact them, and to avoid an unnecessary delay in getting an answer to your question, make sure you have searched the ICO website for all relevant guidance.

The helpline number is 0303 123 1113 (local rate – calls to this number cost the same as calls to 01 or 02 numbers).

The normal opening hours are Monday to Friday between 9am and 5pm (excluding bank holidays).

Scotland

Scotland has its own Information Commissioner who regulates the Freedom for Information (Scotland) Act which covers Scottish public authorities. Because of this, the main focus of the Scottish office is data protection, for which the ICO is the sole regulatory body in Scotland. However, the ICO does have regulatory power under the Freedom of Information Act for UK public authorities based in Scotland.

ICO Scotland contact details

The Information Commissioner's Office - Scotland
45 Melville Street
Edinburgh
EH3 7HL

Telephone: 0303 123 1115

Email: Scotland@ico.org.uk

Wales

The ICO's office in Cardiff provides a local point of contact for members of the public and organisations based in Wales.

ICO Wales contact details

Information Commissioner's Office – Wales
2nd Floor, Churchill House
Churchill Way
Cardiff
CF10 2HH

Telephone 0330 414 6421 to talk to the team.

Email: wales@ico.org.uk

Northern Ireland

The ICO's office in Belfast provides a local point of contact for members of the public and organisations based in Northern Ireland. As well as operating an advice service to address general enquiries on data protection and freedom of information

ICO Northern Ireland contact details

The Information Commissioner's Office – Northern Ireland
3rd Floor
14 Cromac Place,
Belfast
BT7 2JB

Telephone: 028 9027 8757 / 0303 123 1114
Email: ni@ico.org.uk