Chapter 1 - Introduction

The purpose of the first part of this book is to give you an understanding of the key concepts of the GDPR. We will introduce the General Data Protection Regulation and will explore how it fits into the regulatory landscape, including a specific look at the UK position as a result of the Brexit referendum.

- We will explore how the regulation is framed around certain data processing principles that provide the boundaries for processing personal data and what these mean.
- We will cover how data processing must be in line with one of the lawful reasons for processing and will look at how to go about determining which basis of processing is appropriate.
- We will work through the rights that each data subject has under the GDPR and how those rights may be exercised and the circumstances that may apply when complying with those rights.
- We will look at the requirements for reporting any data breaches that may occur, exploring possible exemptions for reporting and how the accountability principle ensures that reporting decisions are recorded.
- We've looked at the requirement for privacy to be embedded into organisations through the principle of privacy by design and have considered the use of privacy impact assessments to encourage responsible behaviour.
- Finally we will examine the special role of the Data Protection Officer and how this role should fit into organisations who process personal data.

As mentioned at the beginning, if any of the topics covered here apply to your activities and you have any uncertainty about your obligations you should consider seeking expert advice.

The GDPR - What's it all about?

The General Data Protection Regulation, or GDPR, is a European Union regulation that comes into force from 25th of May 2018. It governs the use of personal data belonging to EU citizens and in the UK it replaces the Data Protection Act (which also implemented EU law).

This previous data protection framework was written before smartphones, before Facebook and before people started depositing large volumes of personal data online. The new framework is designed to ensure that control of data, especially online data, is retained by the individual, but it affects businesses processing data whether it is collected over the internet or by more traditional methods.

Organisations that process personal data belonging to EU citizens need to be ready to follow the new

regulations or face the possibility of investigation and possibly fines from their member state's regulator.. If you collect, store or use data relating to anyone alive in the EU today then the changes could impact you.

The regulations apply to both organisations processing data in the EU and organisations based outside the EU who are processing the data of EU citizens.

Across the EU, each Member State is implementing law in their jurisdiction to enforce the GDPR. The laws across the EU will all conform to the GDPR, however there may be some differences where existing legal frameworks necessitate variances, for example, the legal systems in Denmark and Estonia do not allow administrative fines and require a workaround that fits within their legal frameworks. There is also scope for limited national opt outs (technically known as derogations) in areas such as processing for national security.

In the UK, the government has introduced the UK Data Protection Bill to implement the regulation and to introduce national derogations. The UK Data Bill replaced the UK Data Protection Act in its entirety.
Each EU Member State has a local regulator which is charged with enforcing the GDPR and local data protection law. In the UK the regulator is the Information Commissioner's Office (generally shortened to the ICO). The ICO has existing duties under the Data Protection Act and will carry forward its role into the new regulatory environment. It is known as a supervisory authority in the GDPR.

GDPR beyond the EU

The regulations apply to both organisations that process data in the EU and to any organisations based outside the EU who are processing the data of EU citizens.

The regulations accept that, in a global economy, it is likely that transfers of data will need to occur outside the EU. For example, how many businesses or their suppliers have their main IT servers based in the UK, but also have email servers or disaster recovery backup servers based in another country? In order to ensure that EU citizens remain protected, the GDPR requires recipient organisations outside of the EU to have data privacy and protection standards of a similar standard to those in EU Member States. This is a protection referred to as adequacy.

Put simply, transfers to third countries and international organisations may only be carried with complete adherence to the GDPR. Organisations outside of the EU who wish to process personal data belonging to EU citizens must follow the GDPR or a local scheme that has been agreed with the EU as being of GDPR level compliance. If an entire country is deemed to have reached the appropriate standard then the EU will formally declare this in an "adequacy" decision.

The EU has recognised 12 non-EU countries as having adequate data protection measures in place, including Argentina, Israel and New Zealand.

If an organisation in a third party country wishes to process personal data belonging to EU citizens, then it must fulfil certain obligations, such as appointing a representative who is based in an EU Member State.

It should be noted that the EU does not accept that the United States' data protection laws are good enough to protect the rights of EU citizens, however, it has been agreed that a scheme called "Privacy Shield" is good enough. This scheme imposes certain obligations on US organisations and acts as a workaround to a full adequacy decision by imposing the obligations at an organisational level instead of at a national level.

GDPR Enforcement

The local data protection regulator has the power to investigate complaints made against organisations based in its jurisdiction or by data subjects based in its jurisdiction. Each EU Member State has a data protection regulator; for example, the UK has the Information Commissioner's Office whilst Finland has the Office of the Data Protection Ombudsman. Regardless of their name, they will all enforce the GDPR.

Guidance issued by the GDPR centralised working party has established the principles for national regulators to act within when the regulations have been breached. The guidance is clear that the nature of the breach and the circumstances must be taken into account. This means that flagrant disregard of the regulations will attract higher levels of corrective action than minor data protection issues or good intentions with poor execution.

One of the key areas that has attracted a lot of publicity is the scale of the fines that regulators can levy against organisations who are found to be in breach of the regulations. Fines under GDPR can reach as high as 20 Million Euros or up to 4% of an organisation's global turnover, whichever is greater. This provision is designed to prevent large global corporations, such as the internet giants, from shrugging off a monetary sum that would barely dent their profits.

A range of enforcement options exist for regulators. These range from reprimanding offending organisations through to issuing fines and public censure. It is also clear that, because of a principle of comparison across regulatory regimes, organisations will face similar regulatory regimes across the EU.

In reality the regulatory landscape, and specifically how data protection regulators will set the bar for enforcement, is going to evolve as the GDPR is implemented and precedents are set.

GDPR and Brexit

On the 23rd June 2016, a majority of the people of the UK voted to leave the European Union. At the time this was written, the UK government is negotiating a transition period during which final negotiations will take place about the future relationship with the EU.

The UK government has been clear that Brexit will not prevent or affect the implementation of the GDPR regulation on the 25th May 2018. As such, individuals and organisations should work on the understanding that the GDPR will apply in the medium term whilst the UK remains in the EU and through any transition periods.

However, depending on the nature of the final Brexit arrangement, it is possible that the regulatory and legal framework will change in the future. Although, it should be noted that the EU will expect equivalent protections if data is to be shared freely between the EU and the UK.

If free data transfers with the EU is a desired outcome for the country, as a third party, the UK will need to achieve an adequacy decision to allow data transfers to occur and will need to be GDPR compliant. Since the UK will already be operating under the GDPR when the transition period comes to an end, the likely way the UK will seek an adequacy decision will be by keeping most if not all of the GDPR regulations in place.

Chapter 2 - GDPR Processing principles

Data protection law has traditionally established core principles that govern all processing of personal data; the GDPR is no exception to this. In this section we will work through the GDPR data principles that underpin the law. If you are familiar with the UK Data Protection Act you are likely to already be familiar with most of these concepts as the GDPR principles are broadly the same.

The principles govern how data should be processed. For processing of personal data to be compliant, organisations must demonstrate that they are following the principles. The one exception to this is the accountability principle as this relates to the behaviour of processing organisations instead of the processing activities themselves.

So, what are the principles?

The GDPR core principles are as follows;

- Lawful, fair and transparent
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality

In addition to the core principles, there is an entirely new "accountability" principle which means that organisations must be able to demonstrate that they are in compliance with the regulations if they process personal data. This means that the emphasis is on **all** data users to understand their processes and have adequate policies, procedures and supporting documentation to show that they understand and are following the regulations. This applies equally to Data Processors as well as Data Controllers.

The principles are the most important bit to get right; if you are following these, then you won't go far wrong so we'll look at these in a bit of detail.

Lawful, fair and transparent

Data must be processed lawfully, fairly and in a transparent manner. You must be open and honest about what data you collect, why you process it and how that relates to the law. You must communicate your lawful basis for processing to people whose data is being processed.

Transparency is achieved by keeping the individual informed and this should be done before data is

collected and where any subsequent changes are made. The GDPR requires that the Data Controller provide the data subject with information about the personal data processing in a concise, transparent and intelligible manner, which is easily accessible, using clear and plain language.

It is important to remember that data is not always collected directly from individuals but may be collected from others, derived from other data sets, observed by tracking or created using algorithms. The GDPR has a mandatory list of the information which must be given to individuals where data is obtained directly from them but also where it is obtained indirectly. How you let individuals know about what you are doing will depend both on the method of communication and on the target audience.

The UK's Information Commissioner's Office (ICO) has created a "Code of Practice on privacy notices, transparency and control" which can assist with preparing a notice to comply with the GDPR. The ICO recommends creating communications that are likely to be understood and are easy to use by the target audience. They recommend that you take advantage of techniques such as layering of information, directing users to a 'privacy dashboard', using pop ups, tick-boxes and 'just-in-time' notices or icons in order to highlight particular issues. The pop up notices that interrupt you every time you visit and new website and warn you about data collection and internet cookies are a great example of a "just in time" privacy notice.

As a general rule, the more unusual your use of data or the more risk there is to the individual, the more you are obligated to make efforts to bring your activities to the data subject's attention.

Purpose limitation

Organisations must only use Personal data for the purpose it was gathered and not then use it for other undeclared purposes.

This means that processing personal data is only permissible if you stick to the original purpose for which data was collected. Processing “for another purpose” later on requires further legal permission or consent. The only exception to this requirement is where the “other purpose” is “compatible” with the original purpose.

Examining where an additional purpose may be permissible will include factors such as a clear link with the original purpose, the context in which the personal data has been collected, the nature of the personal data, the possible consequences of the intended further processing for data subjects and the existence of appropriate safeguards.

A recent case in the US, where a service that allowed the public to upload photos to be stored and shared

and then used the images to train artificial intelligence facial recognition systems is an example where users of the service appear to have been surprised by the additional use. In this case, it is possible that, if the company processes data for EU citizens, the privacy notices issued by the company may have fallen short of the GDPR principle of purpose limitation (and the transparency requirement) and could be open to challenge.

Data minimisation

Any personal data collected by organisations must be relevant to the processing and limited to that necessary for the processing.

Organisations must ensure that only personal data which is necessary for the specified purpose is processed. This means that the amount of personal data collected, the extent of the processing and the period of storage and use must be the minimum needed for the purpose stated by the organisation. Under the GDPR, data must be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed". This principle also links back to the purpose limitation principle.

Organisations must not only limit the data they collect to what is needed, but also that they need to make sure that they collect *enough* data to achieve their purpose. The reasoning here is that if you haven't collected enough data to fulfil your purpose, then the data you do hold becomes useless and you can end up holding personal data for no reason or purpose; which obviously fails under the data minimisation principle.

The data minimisation principle is all about minimising the risk to data subjects by limiting the amount of personal data that is gathered; loss of a limited amount of data is preferably to loss of a more extensive data set.

Accuracy

Organisations must keep personal data up to date and maintain it as necessary. Inaccurate data must be corrected, put beyond use or deleted.

Data that is inaccurate poses a risk to the rights of the data subject as incorrect decisions and outcomes may occur. The accuracy principle is largely unchanged from existing data protection law in place before the GDPR. Data Controllers are required to take "every reasonable step" to comply with this principle.

Storage limitation

Personal data must not be stored for longer than necessary.

Once you no longer need personal data for the purpose for which it was collected, it follows that there is no longer a lawful basis of processing in place. In this case data should be deleted, anonymised or placed beyond use. This means there should be a regular review process in place with regular “housekeeping” processes to clear up databases.

When you no longer have a need for the data, you should delete it. Many organisations have predefined retention policies for their various data types to help define when data can be deleted. Organisations need to ensure that they understand how long data should be retained. For example, it may be necessary to keep data for the duration of a contract and then for a longer period in case of legal challenge; in this case it is legitimate for the organisation to retain the data for the longer period as a legitimate basis of processing is in place.

Integrity and confidentiality

Organisations must process personal data in a manner that ensures that data is kept confidential, protected from unlawful access and is safeguarded against loss or corruption by malicious or accidental means.

Under the GDPR personal data must be protected using appropriate "organisational and technical measures". This goes to the heart of protecting the privacy of individuals. What this means is that both Data Controllers and processors must assess the risk presented by their data processing (or proposed data processing), and then implement appropriate security for the data concerned taking account of those risks and, crucially, check on a regular basis that those measures remain up to date and working effectively.

This principle is designed to create an obligation on organisations to do whatever is necessary to protect individuals' data from loss or unauthorised disclosure.

What are the principles for?

The GDPR principles are the fundamental standards that organisations should try to follow. They act as guidelines against which to compare an organisation's activities. As well as outlining the principles, the GDPR marks a fundamental shift in the approach to protecting individuals personal data by adding in a requirement for organisations to demonstrate their compliance.

The accountability principle

The accountability principle of the GDPR requires Data Controllers to demonstrate that they comply with the GDPR principles. The regulation states explicitly that it is the responsibility of every Data Controller, without exception, to be able to show their compliance.

This means that, as well as following the data protection principles and rules within the regulation, you have to be able to show that you have followed them through maintaining appropriate documentation. Think of this as a requirement to "show your workings" in an exam!

We will cover some of the documentation you may use to assist in demonstrating compliance (such as processing records and internal process manuals) in this course. This is important as, without an accountability structure in place, it won't matter if you're processing the right way; you have to be able to demonstrate your compliance should you be subject to scrutiny.

It is worth noting that under the old UK Data Protection Act 1998 the data principles were similar but applied without the need to be able to demonstrate compliance. Every organisation that processed the personal data of individuals was required to follow the requirements of that Act to ensure that data was kept safe and use of personal data was fair.

This law was written largely before the digital age, when data processing was moving towards more computerised and eventually online activities. Organisations could comply with the law by providing a privacy notice, ensuring people could exercise their rights and keeping their data safe without needing to demonstrated how this was done. Generally, an organisation would only have to demonstrate its compliance if it was actually being investigated for a data breach.