advantage
Independent Accreditation in Learning

A BRIEF GUIDE TO THE NEW

GENERAL DATA PROTECTION REGULATION

FROM THE ADVANTAGE QUALITY TEAM

TABLE OF CONTENTS

What is the GDPR?

One

What is the GDPR?

The General Data Protection Regulation (GDPR) is a European Union (EU) regulation on the use of individual persons' data. The GDPR came into being partly as a response to the growing use of private data by digital companies, such as Facebook and Google. It comes into force across the EU from 25 May 2018.

Even though the UK is leaving the European Union in 2019, the GDPR is expected to remain part of UK law for the foreseeable future. Therefore, all organisations affected should plan accordingly. It will replace the Data Protection Act 1998.

The health and social care sector is particularly impacted by the GDPR. Although the GDPR was created in response to the growing use of online data, its rules effect every type of organisation that uses, stores or processes personal information in some way. This can cover everything from a person's name, their age, date of birth, gender, religion – every conceivable bit of information that could be construed as private or that could reveal the identity of that person.

For people who want to go straight to the source, the Information Commissioner's Office has produced some helpful and detailed guides on their website. For those who want a quick introduction before they dive in to the detail, read on. Please note, however, that nothing in here constitutes legal advice, but is intended to give a basic overview.

Two

What's changing and why?

As stated above, the GDPR has partly come about as a result of the increasing use of personal data by digital companies. We all handover some of our personal data to these companies, such as Facebook, Google, Instagram. This, however, has just highlighted the huge amounts of personal information held by the organisations we come into contact with throughout lives, such as banks, hotels, airlines, train companies, and so on.

The core purpose of the GDPR is to give individuals more control over their own data and to enhance their right to privacy. The GDPR gives people more rights to know who has their data and how they use it, which means the old Data Protection principles will be changing slightly. It also increases the sanctions for non-compliance, emphasising the importance that the EU and national governments are now placing on privacy in the digital age.

The big change is that organisations must be constantly conscious about why and how they are storing personal data. Just getting consent or getting the information and then forgetting about it is no longer an option. Privacy must now be by "design and default". What this means in practice is covered in Part Three.

Just getting consent or getting the information and then forgetting about it is no longer an option. Privacy must now be by "design and default".

Three

What's changed?

Here are the key changes from the old Data Protection laws and regulations:

Tougher sanctions
The fines for data breaches or failing to report data breaches will become much more severe, reflecting the increasing importance people and governments place on data security and privacy. Fines for non-compliance will be as high as 4% of global annual turnover. This doesn't just mean breach of the GDPR itself, but any additional regulations or laws that the UK decides to put in place.

Compensation
As part of putting individuals back in control of their data, the GDPR makes it easier for people to claim compensation for compliance failures. In future, not handing over the details of what data you hold on someone could lead to them issuing a court claim against you. This includes claims for emotional distress and personal hurt as well as financial distress.

Another big innovation of the GDPR is that it brings into play something just shy of the 'class action' suits common in the USA, whereby large groups of claimants can band together to issue claims against organisations. From May, people will be able to have consumer protection bodies issue claims on their behalf.

Accountability
There is much more responsibility on organisations to protect data and report any breaches, with big fines for failing to do so. In future, any unauthorised disclosure of personal information must be reported to the ICO within 72 hours, and the people impacted must also be informed. Larger organisations, with 250 or more employees, will need to have very detailed processes documenting the data they collect, where they store it and why they use it. Larger organisations will also have to appoint a data protection officer, which may mean appointing a new member of staff in some cases.

Consent

There have been some myths spread around consent and the GDPR. Of course, the GDPR does make consent more important. It specifically bans 'opt-in' boxes, for example, and forces organisations to clear and ambiguous in their reasoning for obtaining consent from people to process their data.

However, consent is not the be all and end all. There are other reasons you can process or store someone's data set out by the GDPR:

- **Contract** – You may need to collect and process personal information to fulfil your contractual obligations to them. For example, if the contract is to provide a hotel room to someone, you must know at least some of their personal information to hold the room and be able to check them in.
- **Legal obligation** – Sometimes you will need to store personal data to comply with the law. It is good sense to check that you are doing this correctly.
- **Vital interests** – You can process personal data if you can demonstrate that you need it to save their life or protect their most vital and basic interests. An A&E department will be able to process someone's information to perform a life saving act.
- **Public task** – If you are a public body or acting on behalf of a public body. The task you are performing must be based firmly in the law, however. Water companies, for instance, will be able to rely on this reason because they are performing an act of public administration and have the legal power to do so. This reason will also cover the vast majority of healthcare tasks.
- **Legitimate interest** – This will be the reason most organisations will rely upon. You will need to demonstrate that you are processing someone's information for their benefit without unnecessarily infringing on their right to privacy. The GDPR specifically mentions "use of client or employee data, marketing, fraud prevention, intra-group transfers, or IT security as potential legitimate interests". There is a Legitimate Interest Assessment (LIA) you can carry out to ensure you are compliant.

- **Special category data** – This is data that is particularly sensitive and so requires special protection. Any reasonable person could guess what is particularly sensitive, such as information on a person's sexual orientation, religion, ethnicity, political affiliation, etc.
- **Criminal offence data** – You must have a lawful basis to process criminal offence data.

Data access

Individuals will have more rights to access their data than before. Currently, a person has to file a Special Access Request and pay a fee to force organisations and public bodies to tell them what data they hold and why. Those fees are now being scrapped, and the information requested must be supplied within 28 days.

Automatic processing

People can no longer be subject to automatic decision based on their personal data. Automated decision-making will only be able to happen with the individual's consent or if it is to perform a contractual obligation or fulfil a law. Either way, the person must be informed.

Changing Data Protection principles

Chances are the Data Protection principles from the 1998 Act are ingrained into you thanks to years of training courses. There are some slight changes to these, however. For the record, the new principles state that personal data must be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;
b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ...
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d) accurate and, where necessary, kept up to date ...
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ...
f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

The GDPR also establishes the following rights for individuals:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

By design and default
Organisations will have to demonstrate that they have carefully considered data protection when creating their processes and systems. This was always an implicit requirement of the law, but now it is explicit. There are numerous tools to help you do this, covered in Part Four.

Security
Data breaches are a hot topic right now, with security lapses at large corporations such as Yahoo rightly creating uproar. The GDPR places obligations on organisations to store personal data securely, whether that be in hardcopy or digitally. You should make sure your cyber-security is fit for purpose and that only authorised personnel can get access to personal data.

Children
The GDPR includes a lot of detail on the protection of children's personal data, which will not be covered here. Again, you should make reference to the ICO website if you need more information:

Fines for non-compliance will be as high as 4% of global annual turnover. This doesn't just mean breach of the GDPR itself, but any additional regulations or laws that the UK decides to put in place.

Four

What do I have to do?

The main thing is that you don't panic. The GDPR, as the ICO has said, is an evolution of the law, not a revolution. The ICO has launched podcasts, blogs and news articles to try and discredit some of the media scaremongering you may have seen, some of which is discussed in Part Five.

Consent and reasons for processing data

Most health and social care providers will likely be able to continue to store and process data under the legitimate interest, vital interest and public task tests. Those who care for people who lack capacity to give consent or make decisions should check they are covered under the special category data tests.

The ICO's website has a number of checklists and tools to help you make sure you are storing and processing data legitimately. If in doubt, you should contact your organisation's data protection officer or the ICO.

Data protection by design and default

You should think about all the personal information you store and process. Map out how you collect it, why you collect it, where it is stored, how it is processed, and who has access to it. This will give you a good insight as to where the weaknesses may be.

Once you have done this, you may want to engage in the following activities:

- Conduct a Data Protection Impact Assessment (DPIA) where there is particularly high risk data processing, including if you're using new software or if there a risk to the person's wellbeing if the data is breached.
- If you process personal data on a particularly large scale, you should consider appointing a data protection officer. Consult the ICO if you're unsure if you fit into this category. All public authorities must appoint a data protection officer.

- Consider signing up to a data protection code of conduct if your particular sector has one.
- Conduct legitimate interest assessments (LIA) where you believe that is the justification for processing personal data. The LIA applies three tests – purpose, necessity and balancing – to the decision-making process. The full test can be found on the ICO website.
- Always err on the side of consent when you are unsure of where you stand.
- Consult the ICO directly if you are unsure on anything. Their helpline number is 0303 123 1113. If you are a small organisation, press option 4 for specialist support.

Five

The GDPR myths

The ICO has helpfully been rebuking some of the more extreme myths perpetuated in the media of late. We've tried to summarise those rebukes here:

Myth: All personal data breaches must be reported

This is only the case if there is a risk to the person's rights and freedoms. There's also no need to provide all of the details straight away, since it's highly unlikely you will know all of the details as it happens without an investigation.

Myth: The fines will be strictly enforced and crippling

The ICO has made it clear that the large fines are a deterrent and a last resort. The Commissioner herself has said that she prefer the "carrot to the stick", and prefers a stern letter and working with organisations to fix practices.

Myth: The costs of compliance are going to be enormous

Any regulation imposes some kind of cost on either people or organisations, but the GDPR – or at least, the UK interpretation of it – is actually fairly reasonable in recognising that there are some tasks that just have to happen and there are some small businesses and organisations that can't afford huge compliance teams. Check the different reasons you are collecting data and check on what scale you are processing it. It may turn out that you have to change very little.

Myth: Consent is needed for everything, and it will be the 'silver bullet'

As discussed earlier in this guide, consent will not be the only justification required for processing personal data, and neither will it excuse bad behaviour. Of course you should always try and give people more control over their data if you can, but there are a myriad of legitimate and reasonable reasons why you might be processing personal data with little impact on that person's rights. The ICO's blog post on this is particularly helpful.

Myth: If I'm not ready by May 25 2018, I'm done

Not quite. You should aim to get yourself in shape, but not if it's going to impose unreasonable cost on your organisation. Again, the ICO is about working with organisations, not just punishing them. Hopefully you already take privacy and data protection seriously anyway, and you won't need to change much!

Consent will not be the only justification required for processing personal data, and neither will it excuse bad behaviour.

Six

Some more resources

The ICO should be your main source of information on the GDPR, since it's responsible for implementing and enforcing it. It has a helpful step-by-step guide and many tools and checklists to help you:

• Guide to the GDPR: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/
• GDPR: 12 steps to take now: https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf
• Getting ready for the GDPR: a checklist: https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/getting-ready-for-the-gdpr/

The Commissioner herself, Elizabeth Denham, has published a number of blog posts that explain key tenets of the GDPR and debunks some of the myths. Whether she wrote them herself or not, it's all pretty useful information:

• The ICO blog: https://iconewsblog.org.uk

Of course, you can always read the full 88 page regulation on the EU's website, if you're into that:

• The GDPR: https://ec.europa.eu/info/law/law-topic/data-protection_en

There is also, naturally, a huge amount on Google, some good, some not so good. We recommend starting with what the ICO actually says and then branching out onto search engines if you want more information or if you want to see what other's may be doing. That way, you will be able to sift out the real from the fake news.

What can Advantage do for you?

CALL NOW TO SEE
HOW WE CAN HELP
020 7405 9999