FREQUENTLY ASKED QUESTIONS

1. What does GDPR stand for?

GDPR is short for the 'General Data Protection Regulation'. The first draft of this new law first appeared back in 2012. After four years of negotiation and debate this new law looks set to overhaul Europe's entire data protection framework.

2. When does the GDPR take effect?

GDPR comes into force on 25 May 2018. Unlike the piece of legislation it replaces, GDPR is an EU Regulation rather than a Directive. This means that it comes into force automatically across the EU on that date – without each of the member states having to pass a specific law to implement it.

3. Why is GDPR important?

The current EU Data Protection Directive dates back to 1995. To put things in perspective, at that time, Google wasn't even born yet, Amazon was a tiny online bookseller and Mark Zuckerberg was still in high school.

Fast forward to the present, and the majority of purchases are now made online. The average adult has somewhere between 95 and 130 online accounts. Compared to 20 years ago, the ability of organisations to harvest and analyse information about their customers – not to mention, monitor behaviour, is in a completely different league.

So GDPR represents a shake-up of the rules to reflect this reality.

For individuals, GDPR sees the introduction of new rights. Consumers will have greater control over the data organisations hold on them – including a say on when it should be deleted or transferred to other parties.

For businesses, one of the biggest challenges involves ensuring that customers are able to exercise those rights. For many firms, this will involve taking a long hard look at how consent is obtained for certain data processing activities. It also involves an ongoing review of technical and organisational measures to ensure personal data is adequately protected.

4. What type of data is protected under the GDPR?

The definition of personal data is very broad. More or less any data or set of data that, by you or someone else, can be referred to a physical personal who is alive, is considered personal data.

If you are not sure whether certain data qualifies as personal data, assume that it does!

This following is examples of personal data:

- Identity information (e.g. name, address, telephone number, credit card number)
- Health and genetic records and dataBiometric data
- Racial or ethnic data
- Data on political opinions
- Data on sexual orientation
- Web data (e.g. location data, IP address, cookies and RFID tags)

5. What is the "right to be forgotten"?

Simply put, the right to be forgotten means that individuals will have a right to have their personal data erased, if there are no legitimate reason for you to keep it. For instance, if you process data regarding your customers based on their consent, you will have to erase the data if they withdraw such consent.

6. Who owns personal data under the GDPR?

Is it the business that collect and process the data, or the individual to whom it refers?

Well, the GDPR does not deal with the question of data ownership, but it does make clear that data subjects should be in control of how their data is processed.

7. What are the GDPR requirements?

GDPR is a real doorstopper of an Act. All organisations need to consider the legislation in the whole and conduct an analysis of the impact of GDPR on their activities. That said, some of the most significant requirements are as follows…

Many organisations will need to appoint a Data Protection Officer. In particular, this applies to those companies who regularly and systematically process personal data or monitor data subjects.

Transparency is vital. You are under a duty to be upfront with customers, employees and others about how their data is processed. This means you have to know what you do and why, and be able to convey that in a clear and comprehensive manner.

Privacy Impact Assessments will become a fact of life. Where any new or existing data processing activity will result in a high risk to the rights and freedoms of individuals, companies will be required to carry out a systematic review of how best to safeguard those rights.

Deletion and portability. You need to able to delete data when no longer necessary, and transfer it elsewhere if requested by the people it refer to. Are your systems designed to make that possible?

Privacy by design and default. In other words, safeguards to ensure the protection of personal data needs to be hardwired into your processes and systems.

Accountability. Being compliant isn't enough. You have to show that you are abiding by the rules. This includes maintaining an up-to-date register of data processing activities. In the event of a security breach, it also involves being able to give a full account of what happened and the preventative measures you had in place when reporting that breach.

8. What is a 'data breach'?

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Example

Personal data breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.
-

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if

the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

Recital 87 of the GDPR makes clear that when a security incident takes place, you should quickly establish whether a personal data breach has occurred and, if so, promptly take steps to address it, including telling the ICO if required.

10. What should I do if I think or know I have breached data protection

You must inform your direct Manager immediately if you think a data breach may have occurred. Managers must inform Graham Davidson-Bowman immediately and no later than 24 hours. Graham Davidson-Bowman can then assess situation and notify the ICO within the 72 hour timescale accordingly.

11. What will happen if I am found to have breached data protection?

Employees are under an implied duty of fidelity. This means that if an employee does use or disclose confidential information without the company's permission, it could be considered to be gross misconduct and pave the way for summary dismissal.

12. What happens if my company is not in compliance with GDPR?

First off, there is a new fine regime to bear in mind. For a serious breach of GDPR (e.g. a major security breach where the organisation had woefully inadequate protective measures in place), the maximum administrative fine is up to 4% of global turnover or EUR 20 million, whichever is higher. For other breaches (e.g. inadequate record keeping or failure to report a breach), regulators will have the power to issue penalties of up to 2% of global turnover or EUR 10 million.

Also, under Article 82 of the Regulation, there's a direct right of action for data subjects to claim compensation from the data controller or processor. So if data has been incorrectly held or used and the individual has suffered damage, firms could find themselves being hit by legal action.

Finally, don't overlook the possible reputational repercussions of non-compliance. Certainly when it comes to sanctions issued by the regulator, this information will be in the public domain. Staying compliant is crucial for any business seeking to maintain their reputation as a safe pair of hands in the digital marketplace.

13. Who does GDPR apply to?

GDPR applies to natural or legal persons, public authorities, agencies or other bodies processing personal data (processing in the course of exclusively personal/household activities is excluded).

If you are not sure whether GDPR applies to you, best is to assume that it does!

14. Who within my company is responsible for compliance?

Regulator guidance recommends that firms designate a member of staff to oversee compliance – in our case it is Graham Davidson-Bowman.

15. What is the difference between a data processor and a data controller?

The data controller is the person (Graham Davidson-Bowman) who "calls the shots"; i.e. the one who decides which personal data is collected and the purposes of the processing. The data processor is the person who processes that data on behalf of the data controller (i.e. all Staff handling customer data).

Compared to the current system, GDPR places new obligations on data processors. These processors can now face fines for non-compliance and claims for compensation from data subjects for GDPR reaches.

GDPR also stipulates that processors may only process personal data where there is a written contract clearly stating the scope and limits of the processing activity.

16. Where can I find further good reading on the GDPR?

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/