A short GDPR guide for small businesses

Are you concerned about the GDPR? If you do not have an up-to-date privacy policy on your website, you may attract an audit from the DPC which could lead to a fine.

What is the 'GDPR'?

The General Data Protection Regulation is an EU law that came into effect on May 25, 2018 applying across all EU member states including Ireland in order to protect and safeguard the privacy rights of individuals.

Who does GDPR apply to?

In essence, it is difficult to think of a business that GDPR does not apply to because in order to do business most organisations need to collect personal data. GDPR applies to any individual or organisation that processes personal data so if you have a 'Contact Us' page on your website for individuals to submit their details, then you are collecting (and therefore processing) their personal data.

The GDPR does not *just* apply to large companies but also individuals, SMEs, not-for-profit organisation and community groups.

There is little difference in the application of the GDPR whether you are a large company, a SME or an individual. Very few exemptions under the GDPR apply to SMEs, one example would be that you may not be required to keep records of processing activities if you have 250 or less employees (depending on the type of personal data that you process). Apart from that, there are few differences in the application of the regulations based on the size of an organisation.

What is 'personal data' and 'processing'?

'Personal data' is any data that relates to an identifiable living individual. The definition of 'processing' of personal data is very wide and includes collecting, recording, storing, adapting, using, disclosing and deleting data.

Therefore, an organisation is 'processing' personal data, if it stores the personal data of customers or employees electronically or in hard copy. It is important to note, that GDPR covers personal data held in hard copy files also, therefore if your organisation only keeps personal data physically in hard copy files it is still subject to the GDPR.

Personal data may be held by an organisation in various forms such as emails, Customer Relationship Management (CRM) systems, images or recordings of individuals (e.g. CCTV).

Why do I have to comply with the GDPR?

Under the GDPR there are heavy fines for non-compliance of up to €20 million euros or 4% of global turnover. Additionally, individuals may sue an organisation for material or non-material damage if there is breach of the GDPR.

We live in a time that clients, employees and anyone whose personal data you hold, have a greater awareness of their rights and expect and trust organisations to safeguard their data. As such, another very serious consequence of a data breach is reputational damage.

An individual's rights

Individuals have more rights under the GDPR that ever before meaning that they can make a subject access request to an organisation, requesting all of the personal data that the particular organisation holds on them. They could also ask for the 'right to be forgotten' or could object to receiving direct marketing from your organisation. Organisations need to be prepared for this as you have 30 days to respond to these requests or risk being fined by the Data Protection Commission ('DPC').

The principle of transparency

The principle of transparency runs to the core of the GDPR and it means that organisations have to be open and transparent about how they deal with an individual's personal data for example, by having an up-to-date privacy policy on your website.

Don't tell us, show us

The principle of accountability runs throughout the GDPR and the emphasis is on each organisation to show how they are compliant with the legislation. It means that if the DPC conducts an audit on your organisation, they will expect to see documentary evidence and good record keeping to show that you have complied with your obligations – don't tell us, show us.

What do you need to do?

GDPR applies to the entire life cycle of the personal data that you collect. From the day that you collect it until the time that you safely dispose of that personal data, you have to safeguard it and not just from a IT and data security point of view, although that is also very important.

You need to assess and keep a record of all of the personal data that you hold i.e. what personal data you hold, where you hold it, who has access to it, what you do with it and who it is shared with inside or outside of the organisation.

You must be able to identify and document the legal bases for the personal data that you process – all of the legal bases are set out in the GDPR. Consent from an individual must be informed and freely given and affirmative action must be taken, so where consent is required, you have to give very clear information to the individuals concerned about what you are going to do with their personal data.

You need to review all the contracts that you have outsourced where you are sharing personal data (i.e. you may be sharing employee data with a third party who does your payroll) and make sure that the protections set out under the GDPR are included in those contracts.

Staff need to be trained on GDPR so that they understand what is personal data and what is a data breach and if there is a data breach within your organisation who they should report it to (also are they aware of how you as an employer use their personal data?).

You need to have an external policy (such as the privacy policy on your website) and internal privacy policies up-to-date.

Through a recent survey, we found that many SMEs still had either no privacy policy and/or cookies policy or a deficient privacy policy and/or cookies policy on their websites. By having an up-to-date privacy policy on your website, you are telling users and potential clients, what personal data you are collecting about them, how and why and what you are using it for, whether you are sharing with anyone, if you are transferring their personal data outside of the EEA, who they should contact if they have any queries, what their rights are and how to make a complaint etc. – if you do not have an up-to-date privacy policy on your website, you may attract an audit from the DPC which could lead to a fine and the risk of reputational damage to your organisation.

If you would like Data Privacy International to guide you through your GDPR compliance or if you would like us to update your privacy policy and/or cookies policy, please get in touch by following the link below to our website: www.dataprivacyinternational.com.

By Adelaide White (co-founder and director of Data Privacy International – a data protection consultancy).

Disclaimer

This a short guide of key considerations and not by any means exhaustive and is not intended as definitive analysis or legal advice or otherwise on the compliance with GDPR.