CoffinMew

Guide to GDPR

introduction

The General Data Protection Regulation (EU) 2016/679 (GDPR) is the biggest overhaul to data protection law in twenty years. Its aim is to establish a single set of rules for all EU member states and do away with national data protection laws. The GDPR extends the data rights of individuals and requires organisations to develop clear policies and procedures to protect personal data and adopt appropriate technical and organisation measures. Fines for non-compliance can now be as high as 4% of global turnover.

The GDPR is data protection law with muscle.

Doesn't Brexit mean I don't have to worry about the GDPR?

All UK companies must be compliant with the GDPR by 25 May 2018. Even after Brexit, the GDPR cannot be ignored. It will set the rules for handling personal data for the foreseeable future as the British Government has announced it will adopt the GDPR into our national law once the UK leaves the European Union. In any event, UK companies wishing to do business with the EU after Brexit will need to demonstrate data handling to GDPR standards.

So what exactly is personal data?

"**Personal data**" is any information about a living individual where it can be connected to that individual (via their name, home address, date of birth, National ID or passport or tax number). Data such as device identifiers, cookie IDs and IP addresses can also count as personal data.

There is a special category of personal data known as **"sensitive personal data"**. This relates to a person's physical, physiological, genetic, mental, economic, cultural or social identity and includes their biometric data. Anything which reveals a person's political opinions, racial or ethnic origin, religious beliefs, sexual orientation and/or health status is sensitive personal data and enhanced rules apply to collecting and processing it.

I'm aware the law has changed but what does this mean for my business?

There is a vast amount of material freely available about GDPR but it can be a case of information overload. Not much of the available information is easy to digest, or use, to help you update how to collect and handle personal data. The most reliable and comprehensive guidance on the scope and effect of the new rules is published by the Information Commissioner's Office at https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/. If your business already complies with the DPA you are on the right track, but there is more to do.

But knowing what the rules are and knowing what to do about them are two very different things. The 4 Steps and Roadmap to Compliance set out in this guide will help you break things down into manageable stages. You may also like to take our GDPR Compliance Survey, details of which are at the end of this guide.

Step 1 Data audit

You will need to conduct a data audit to map where you keep personal data. Put simply, you need to think about how personal data currently flows across your business, in particular:

1. what personal data does your business hold and why?
2. where does this personal data come from?
3. who do you share it with?

It is essential that you pinpoint all data interactions across your business before you can dive into the detail of the GDPR requirements.

The data audit should help you identify:

1. the different categories of data you hold on employees and potential recruits, customers and prospects, and business contacts;
2. why you are holding that information and whether it is strictly necessary for conducting your business and delivering products and services or whether you hold it for another reason;
3. whether you are relying on one of the automatic rights to process each person's personal data (the so-called 'exemptions') or on their consent (and, if so, how you're obtaining that consent);
4. all the third parties you contract with;
5. what marketing activities you conduct;
6. how long you retain each type of data for; and
7. whether the information is securely protected at all stages and if there may be vulnerabilities in your security.

Controlling/Processing

For any personal data you hold, you'll also need to assess whether your business controls that personal data or whether you process it on the instructions of a third party. Whilst the DPA does not impose any obligations directly on a business purely processing personal data on behalf of a third party, the GDPR does. So even if you're only a data processor, you need to bring your operations in line with the GDPR, for example, with respect to keeping accurate records of data processing.

Privacy Policy

If your business collects personal data under the terms of a privacy notice, the content of that notice will need to be amended. The GDPR prescribes certain information it must contain. You'll need to balance the requirement to add this detail against the need for the notice to be transparent, easy to read and reader friendly. Technology may be of assistance here. For example, some companies are replacing their written privacy notices to consumers with easy to follow videos accessible on their website. It is no longer about hiding behinds words, but ensuring people understand exactly why you want to collect their personal data and give express, specific consent to each non-exempt use you want to make of it.

Step 2

Internal policies and procedures

Asking questions across your business to complete the data audit will inevitably start to flag whether your policies and procedures for data handling are adequate. Consider:

1. Does your business have a Data Protection Policy? Is this policy in alignment with the requirements of the GDPR?
2. Do you have established procedures in place to deal with data compliance or is your business reactive?
3. Do you have a procedure for dealing with information requests, commonly known as Subject Access Requests? This is not a new concept, but the time period a business has to respond to such a request has reduced from 40 days to one month. The ability for an organisation to charge a fee has been removed and the breadth of information that has to be given back to the individual has increased. Has your procedure been updated to reflect these changes? Are staff aware?
4. Do you use Privacy Impact Assessments ("PIA's") within your project and risk management procedures? Again, PIA's are not new but these assessments are now mandatory for any high risk processing.
5. Are all your staff aware of GDPR and how this will impact them? Any individual handling personal data should be trained to understand his/her responsibilities and how this fits into ensuring your business is compliant. Training staff is essential to both evidencing compliance and mitigating the risk of data misuse/loss.
6. Could your business respond to a security breach within 72 hours? Do you have a team/policy/training to support this outcome? The GDPR introduces mandatory reporting to the ICO, within 72 hours or less, for security breaches (with some exceptions). If your business controls personal data you'll need to ensure you have a robust procedure in place to deal with incidents within the required timescales. Even if you're a data processor, the controller of that data may start to place higher demands on you to report issues within these timescales (if not shorter ones).

Step 3

Data governance

It is one thing having a policy that says how you're going to comply. It's another thing to instil a culture of compliance into your company and ensure you actually comply at all times.

Consider, does your business have an individual who holds responsibility for dealing with/managing data protection issues/queries? Are they dedicated to this role? Under the GDPR it is mandatory for certain organisations to designate a Data Protection Officer ("DPO"). These will include public authorities, public bodies and organisations that conduct, as a core activity, large-scale, systematic or regular monitoring of individuals or large-scale processing of sensitive personal data.

Even where an organisation doesn't fall within these categories, it would be good housekeeping to have an individual nominated to deal with data compliance, whether or not such individual officially adopts the title of DPO. The key principle underlying the GDPR is accountability and the DPO takes a pivotal role in both evidencing and achieving this. If it is not mandatory for your particular company to appoint a DPO, and you also decide you don't need one, we strongly advise you to record your reasons at Board level along with how you plan to monitor and ensure compliance without a DPO.

Step 4

Contracts

It is inevitable that you'll identify, somewhere in your data audit, that your business is sharing personal data with a third party.

Typical cases are outsourced administration functions such as with IT providers, cloud storage services and payroll companies, along with business contracts with sub-contractors, agents and consultants. You will need to ensure any such data sharing with third parties is governed by a contract.

Any current contract which will still be in place after 25th May 2018, and any contract entered into from 25th May 2018, will need to be reviewed if it deals with the transfer of personal data (in whole or in part and in any capacity). The GDPR prescribes certain information that must be included in the contract to document the data processing being undertaken. It is therefore sensible to use this opportunity to impose additional obligations on other parties to assist you in maintaining compliance within your supply chain.

Don't forget that you'll need sufficient time to review contracts and, if necessary, renegotiate terms so start as soon as possible.

Employment contracts and employment policies should also be considered.

Is this everything?

The steps outlined above will help you approach compliance in a structured and manageable way and give your business time to implement and embed change. Complacency and inaction risks misuse of personal data and, in consequence, exposure to fines which are significantly higher than those under the DPA, pay-outs of compensation to affected individuals and reputational damage.

The steps are not consecutive., it is inevitable that you'll have to consider these issues in parallel. You'll need to identify your weak spots and prioritise accordingly. To assist in this process we've developed a questionnaire to guide you through your data audit.

The Coffin Mew GDPR Compliance Questionnaire

If you would like a copy of the questionnaire please contact us at **GDPR@coffinmew.co.uk**

There is no charge for receiving a copy of the questionnaire. You are free to use it to assist you in your internal compliance project, even if you do not require any further assistance from us.

If you request a copy of the questionnaire we will only hold your contact information for the purposes of communicating with you about GDPR and, in any event, we will delete your contact details at the end of May 2018 (unless you have separately instructed us).

If you would like us to assist you with using this questionnaire and carrying out your compliance assessment, please contact us at **GDPR@coffinmew.co.uk** and we would be delighted to discuss with you how we can support you to become GDPR ready.