DRAGON

GDPR: General Data Protection Regulation

The new data law that starts in May 2018

GDPR:

It sounds dull but it's massive... and your company needs to act NOW

We'd love to tell you this guide is a highly entertaining and humorous piece about a really exciting subject. Sadly, we'd be lying, and you'll be pleased to hear we don't ever lie to our audience! So let's be totally upfront about this now. We're talking about the new laws surrounding data protection and all the associated paperwork.

Yawn, right? Yep, we know. The trouble is, it's coming soon and it WILL affect you, so it's important that you know exactly what's expected of your business and start planning for it now.

Non-compliance will not just mean a slap on the wrist, either. With potential fines of up to €20 million or 4% of annual turnover (whichever is greater) this is something you simply cannot afford to ignore.

So make a cuppa, treat yourself to a biscuit or two and we'll try to make it as painless and far from mind-numbingly boring as we possibly can.

Are you sitting comfortably? Then we'll begin

The background

Since the Data Protection Act (DPA) was launched in 1998, the world has changed. A lot. According to the latest figures from Ofcom, the average adult now spends 20 hours a week online - double the time we spent surfing the web ten years ago. It's not surprising when you think about it. We shop, bank, work and even date online, and whilst that's great for convenience it throws up some huge issues around data security.

So, how do we keep our businesses and their customers safe when there's so much personal information floating around in cyberspace? It's not always easy, that's for sure.

So, the General Data Protection Regulation (GDPR) is on its way to help make things simpler for businesses and organisations to manage their day to day data protection responsibilities.

The GDPR comes into force in May 2018. If you're like a lot of small and medium businesses in the UK you might be thinking you've got plenty of time to think about it and it'll be OK on the back burner.

You'd be wrong.

This is one of the biggest and most important acts to affect European businesses for a long time, and it's pretty complex. It's absolutely essential for the future of your business that you start taking care of it now and do everything you can to ensure you're ready.

Here's what you need to know

The whole idea of personal data is changing

Up until now, we've thought as personal data in terms of things like addresses and dates of birth. The GDPR takes this idea much further, and even something like an IP address can now be classed as personal data and have to be managed accordingly. The directive will apply to automated personal information, manual filing and paper records - and if it's already subject to the Data Protection Act, you can bet your bottom dollar that the same will apply with the GDPR.

There will be special categories of personal data. These are pretty much the same as those listed in the DPA but there are some amendments, as outlined below in extracts from Articles 9 and 10 of The Act.

ALERT: If government speak turns you off, here's a bit you can skip

1 Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

2 Paragraph 1 shall not apply if one of the following applies:
(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;
(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
(e) processing relates to personal data which are manifestly made public by the data subject;
(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;
(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89 (1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

3 Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.

4 Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.

(Article 9)

"Processing of personal data relating to criminal convictions and offences or related security measures shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of the official authority."

(Article 10)

You'll need up to date policies and procedures

All companies and charitable organisations in the UK will need to show that they are compliant to the new standards and only use personal data if absolutely necessary to their business objectives. That means no asking for information that you don't really need just to fill some space on a form or because you have a vague idea that it might come in handy one day. If you ask for it, you'll have to be able to justify why you're doing so.

This is going to mean updating policies, conducting regular audits and implementing data protection strategies. As you might expect, this will be a long and unwieldy process that requires patience, attention to detail and a lot of background knowledge.

It applies to controllers and processors

This is all outlined in the Data Protection Act, but if you need a refresher it's worth remembering that there are two categories of people who have responsibility for handling data – controllers and processors. Controllers have the overall say on what and how personal data is used within an organisation, and processors act on their behalf.

Processors will be legally required to follow specific guidelines and will be liable for any breaches, and controllers will be expected to ensure that everyone in their team is up to date with compliance. So if you're the head of a company or department you'll be the "controller", meaning the buck stops with you.

If your staff haven't done what's expected of them - even if you've asked them to - if it causes any confidentiality breach at all then it will still be your fault for not checking. It's ok to get another trusted member of your team to check on your behalf, but it must be signed off in writing and you'll need to have a constant eye on things.

> *" It's for all data processing carried out by organisations working in the EU".*

This is a directive created for all European organisations AND to those working outside of the EU but offering services within it.

And in case you're wondering, even though this is a EU directive, Brexit won't have any effect on us Brits having to tow the line. It's happening, and all UK businesses will be subject to it regardless of Boris, Theresa or anyone else.

Still with us?
Good, let's carry on!

There are some (but not many!) exclusions

Certain activities carried out by the Law Enforcement Directive will be exempt from the new legislation, as will activities relating to national security and some personal/ household activities.

Although the GDPR will be harmonising Data Protection laws across the EU, Member States will have the ability to introduce some supplemental laws for special purposes that will be specific to the country. These exemptions are in two main areas regarding restrictions and specific processing situations. Article 23 of the GDPR allows individual Member States to introduce derogations on topics including national security, public security, the protection of judicial independence and proceedings, and the enforcement of civil law matters.

The specific data processing situations include:

- Freedom of expression and information
- Public access to official documents
- National identification numbers
- Scientific and historical research purposes or statistical purposes
- Employee data
- Archiving in the public interest
- Obligations of secrecy
- Churches and religious associations

You are responsible for your organisation's compliance to the GDPR

If you don't take the GDPR seriously, you WILL be liable.

This is not just a piece of flimsy legislation you can get away with ignoring; personal data is serious business and if you put any of your customers or other stakeholders at risk then you'll be liable for a hefty fine which could not only mean embarrassment and expense, but the total loss of your business.

So, now comes the tricky part. How do you manage consent?

Unsurprisingly, this is one of the biggest challenges throws up for all organisations.

Managing consent doesn't just mean asking permission to send your customers directing marketing communications, it's about ensuring they're happy for you to hold their personal data in the first place. Whichever way you look at it, this is going to involve some hard work. You'll need to communicate with all customers and have a clear, easy to follow audit trail detailing any changes to data and written consent.

Remember, all individuals have the right to access any data that is held about them and they also have the right to object. If anyone does exercise this right it must be clearly documented and respected. You will be legally required to uphold your clients' rights at all times.

For proven, trusted IT systems support to keep your business trading profitably

Dragon Information Systems Ltd
6 Bassett Court, Newport Pagnell, Bucks MK16 0JN
Tel: 01908 613 080 | helpdesk@dragon-is.com | www.dragon-is.com