GDPR: A Summary of What you Need to Know

GDPR is a seemingly complex subject that is confusing many managers and business owners. Here we simplify the jargon and give you some ideas of where to start.

You may have heard or seen reference to something called "GDPR" in recent months. Whilst it might sound like nothing more than a snooze inducing acronym, it's actually an incredibly important new legal requirement that companies of all sizes need to be aware of.

We set out (in simple terms!) what it's all about and look to translate some of the jargon you'll soon be seeing a lot of.

A new legal requirement
The General Data Protection Regulation (GDPR) will come into force on 25th May 2018 and will apply to any data which companies hold or process within the EU.

So that's all UK companies. And it's also companies outside the EU, for example, US companies who hold any data on UK customers.

When implemented, GDPR will arguably be the most strict data privacy law in the world. Its overall goal is to safeguard consumer data and enforce data security rights. At the same time it forces organisations to think about what they collect, and how they use it.

Deciphering terminology

Data controller
The data controller is the organisation or individual who determines what happens with personal data.

If you are a business owner, that's you.

Data processor
The organisation or person who processes data on behalf of the controller.

If you are a business owner, that's a third party; often a tool/software.

An example of a simple situation where GDPR applies would be if you were holding client data in the form of an email list, and you were then using this list to send emails.

In this example you are the data controller, and the mailing company is the data processor.

Only the data controller is held liable for the data protection rules, not the processor. So you can't blame your email provider if you don't obey the rules.

Fines
Fines for non-compliance can vary, but will be as high as 4% of annual turnover.

A summary of the requirements

Consent
Data controllers must keep their terms and conditions simple and easy to read, essentially meaning complicated contracts designed to confuse users into giving their consent to selling their data to third parties are now against the law.

It must also be as easy for the user to withdraw consent as it is to give it.

Breach Notification
In the event of a data breach, data controllers and processors must notify their customers of any risk within 72 hours.

Right to access
Customers have the right to obtain confirmation of whether their personal data is being processed and how.

The data controller must provide an electronic copy of personal data within 14 days of the request.

Right to be forgotten
When data is no longer relevant to its original purpose, customers can at any time have the data controller erase their personal data and stop it from being distributed.

Data portability
Individuals have the right to obtain and reuse their personal data for their own purposes by transferring it across different IT environments (systems, etc).

Privacy by design
This calls for the inclusion of data protection from the very beginning of designing software, systems, websites etc.

It is the responsibility of the data controller to implement technical measures to keep data secure and compliant with the GDPR rules.

What you should do
Aside from making sure you can comply with the rules above, what can you actually do now to ensure you're on the way to being compliant?

For smaller businesses...

Audit your data flow

Answer and document your responses these questions:

- What personal data do you have?
- Where is it sent?
- Where is it stored?
- How is it processed?
- What do you tell people about how it's processed?
- How do you collect it?

Create a GDPR summary document
From the audit questions, produce a document you and your staff can refer to so that everyone knows what's what. You can then use this to ensure you have a resource for anyone enquiring into whether you're compliant.

Check third parties
Make sure your third party suppliers are also compliant. That's pensions, healthcare etc etc.

Customer data
In summary, you must make sure your website and any other means of collecting customer data follows these rules:

Opt-in Only No soft opt-in Right to be forgotten

All contacts must provide consent to be contacted. The sender (your business) must be able to prove they have consent.

Implied consent is no longer enough. Make sure users are ticking a box to something they can understand when you collect their data.

Anyone on your contacts list has the right to have all their data deleted at any time.

Brexit
No reference should be made to any EU legislation after 1st January 2021. All legislation has been replaced by UK GDPR rules.

For further information on GDPR, please visit:
https://ico.org.uk/for-oroanisations/quide-to-the-general-data-protection-regulation-gdpr/

Or contact us.