GDPR help for small businesses

From May 25 businesses will need to be GDPR-ready. What does this mean? Here's a brief guide for small business owners worried about GDPR.

The way companies communicate with their users, and how they handle and process the information they hold about their users, will need to change from the above date. This is so all company practice falls in line with new GDPR (General Data Protection Regulation) guidelines. The guidelines are EU-led, but identical guidelines will almost certainly be written into post-Brexit UK legislation.

Privacy policies and user agreements are notoriously and unnecessarily long. GDPR is partly to end the need for such overlong, overwritten agreements that few users could reasonably be expected to wade through.

GDPR demands **clarity** in all company explanations about how it plans to use and store personal information. It requires companies to provide information that is:

- easy to find;
- free; and
- written in **clear plain English.**

The changes are to protect users. If a company is going to use someone's personal information, the user in question should be made aware in easy-to-understand terms what is happening to that information. 70000-word streams of evasive and impenetrable gobbledygook will no longer suffice. Users need to know if their information is not being treated in a way they deem suitable. To have a GDPR-ready privacy policy in place, you'll need to consider:

- what information is being collected;
- who exactly is collecting the information;
- how they are collecting it;
- why they are collecting it;
- how it's likely to be used;
- who it will be shared with;
- the effect of all this on the user or users;
- how you plan to use information and if this could lead to a complaint by the user.

Here are some frequently asked questions that we hope answer in advance some of the queries you may have.

Q Who needs to know about GDRP?

A Anyone in your organisation who stores personal data needs to understand the changes to the law and what they need to do. It's no good just you knowing about it if your staff won't keep to the regulations.

Q I'm not even sure where we keep all our personal information, what should I do?

A Make sure you know where all such information is and who is responsible for it. This includes physical copies on paper and card as well as computer files of details such as names, addresses, national insurance numbers, dates of birth and even email addresses. Take this as an opportunity to find out once and for all how you deal with the information you hold. You'll need to be able to provide a copy of someone's personal information if they request one. Designate one member of staff as responsible for keeping and maintaining such information.

Q Why do I have to be so careful about all this?

A New rules state that any information you hold about anyone else must be collected and looked after properly. The rules are meant to make sure you do not breach them by losing, giving away or misusing their details.

Q What is a 'breach'?

A A failure to look after someone's personal information properly. Once you have a good system in place this shouldn't happen.

Q If I think I have breached the rules, who do I contact?

A You should contact the ICO (Information Commissioner's Office) and they will lead you through the next stage in the process and let you know the severity of the issue.

Q What happens if I'm found to have made a serious mistake?

A You could be fined a considerable sum, 20 million Euro or up to 4 percent of your annual turnover, whichever is higher. But such amounts are very unlikely.

Q I'm still confused, sorry.

A Do you keep the information you hold about your customers/clients on one computer or several? We do not recommend the latter approach. If you keep personal information in one secure place there is far less chance of it being mislaid, lost or ending up in the wrong place.

You will need to make sure, from now on, all your information, such as names, addresses, bank details and the like are collected properly, and are stored securely and in one place. Not only that, they need to be looked after by one dedicated person, either yourself or someone else in your organisation, and deleted as requested by the person in question.

Q I read something about having a system in place for removing someone's personal information if we no longer use it, or if they no longer want us to use it?

A If you don't have such a system, put one in place. If you deal with people on a regular basis it's reasonable to hold onto their details, including their email address.

Q Can I later on use the excuse that it was all so confusing I just left it?

A We wouldn't recommend it! And, by putting in place a good data protection policy and telling your clients about it, you can significantly add to your value and reputation.

Q We were hacked last year, does this matter?

A If you've been hacked, or if you are hacked in the future, understand the measures needed to prevent this, and let anyone whose personal information you hold know about it if it happens.

Q How do I know if we have the right permission for any personal information?

A Any requests you make to store personal information must be positive (opt in, not opt out). You may need to review how you deal with permission for information. So, if you collect somebody's contact details on an online enquiry form, you must then delete those details unless you otherwise have permission to retain them. You won't usually need specific permission to use regular customers' information, as that relationship will depend on continual access to such information, for example to provide prices, invoices and so on.

Q What do I do if I already feel our privacy policies are in line with GDPR regulations?

A Don't leave any room for error!

Q Is there special protection for children's personal information?

A You may need a system to check individual ages, and may need parental or guardian consent if the person is under 16 (or 13 in the UK). Children in the UK can give their own consent once they are over 13. This may differ in other countries but all children give their own consent once they are over 16.

Q What else do I need to do?

A Don't worry too much about what might happen if you make a mistake. Unless you're an organisation with more than 250 employees, you won't need to carry out a Data Protection Impact Assessment, or appoint a dedicated Data Protection Officer, for example. Just get your personal information policy in order as explained above, and you should be fine. Although you don't need a Data Protection Officer if you have fewer than 250 employees, you will still need to choose someone in your organisation to make sure you keep to GDPR principles. If you work for yourself, that's you!