HRC Law TEAM

IT and GDPR - The inevitable bedfellows

Whilst we are not IT professionals here at HRC Law, we do aim to understand all aspects of our clients' businesses. Considering the role of IT in relation to the GDPR is a key element of this.

There is no avoiding the role IT management and security will have in meeting your compliance requirements and maintaining data security.

Below are some important areas for you to get a handle on:

1: By carrying out an audit of the data you hold, you should now have:

(a) an understanding of your data use. You can use this knowledge to decide on the level of IT security that is appropriate for your business. The GDPR will not require a one size fits all approach, it will place the onus on you to decide what is right;
(b) located where the data sits within your business and where it is stored. It is important to maintain an up-to-date log of this.

2: Once you understand your business, you will need to then take steps to keep your data secure, by:

(a) Ensuring employees and contractors are suitably trained;
(b) Updating (or drafting) and keeping an up-to-date policy on IT security;
(c) Limiting access to personal data so that only those who need it have access to it;
(d) Ensuring someone is appointed to update training, policies and to monitor admin access;
(e) Using appropriate encryption software. There are certain compliance standards (ISO etc.) in this regard. Encryption does not just mean password protection of devices;
(f) Ensuring that any data and information necessary for your business to operate is backed up securely and that this is reviewed regularly.
(g) Deciding your position in relation to portable devices, how you will maintain security and whether you will permit Bring Your Own Devices (**BYOD**) to work.
(h) Having robust contracts in place with all third-party website, application, IT support and data storage providers, so that you can enforce all security requirements fully and have proportionate recourses available under the respective contracts.

3: Consult with appropriate legal and IT professionals to understand any gaps in your existing security and supporting documentation, as well as to obtain advice on how to establish strong practices and protection in future.

Direct Marketing – Electronic Communications

In the main, the GDPR do not change the picture for direct marketing via electronic means (being any communication via telecoms provider, traditionally covering phone calls, faxes and emails). These continue to be governed by the Privacy in Electronic Communications Regulations 2003.

We are expecting a new e-Privacy Directive. Indications are that this will come into force alongside the GDPR, but time is getting tight for the European Commission to make this happen.

If and when changes happen regarding the e-Privacy Directive, these will drive changes for marketing, including an extension of scope to specifically include electronic communications service providers such as WhatsApp or Facebook; a more robust protection of confidentiality and restrictions on monitoring; limitations on metadata use without consent and a restriction on Spam.

We will provide updates on these changes when we have a clearer picture, but please feel free to discuss them with us directly.

The immediate impact of the GDPR will be its interpretation (and extension) of the consent requirement. Essentially, consent is required to direct market to an individual and, as we have discussed in other Toolkit documents, this is changed under the GDPR which now requires consent to be freely given, specific, informed and unambiguous.

What are the implications for your business?

This means that you will need to:

1) require a positive step to opt-in to direct marketing (unticking a box will no longer be valid);
2) ensure a log of consent is created and maintained;
3) provide the required information (prescribed by the GDPR) to the data subject when consent is obtained (The list of required information has been extended to include the details of the Data Protection Officer. You must explain consent is the legal basis of processing, detail any intent to transfer outside the EU, identify the right to complain and to whom, refer to the new data subject rights and clarify the right to withdraw consent.)
4) You will need to review your existing consent process and privacy notice to ensure it meets the new requirements;
5) You will need to consider how you may bring any mailing lists up-to-date prior to the commencement of GDPR.

In a nutshell, always ensure you have explicit consent to market (opt-in) and that a record is maintained. Consider how you collected your existing consent and whether you need to do it again.

If your existing consent is ambiguous, but you have a history of communications to an individual, it is worth reviewing whether you have enough of a basis to contact them at this stage to clarify whether someone consents. Depending on the situation this may be a reasonable step to take as a business which is looking towards meeting the new accountability requirements under GDPR.

HRC Law would be happy to assist you or your business with any GDPR issues. Graham Hansen, Associate at HRC Law, can be contacted on 0161 358 0552 or at grahamhansen@hrclaw.co.uk. You can find out more about Graham and HRC Law at www.hrclaw.co.uk.