GETTING READY FOR THE NEW GENERAL DATA PROTECTION REGULATION

Richard Robinson
Managing Director - Legal Compliance Services

The Strategic Partner

Essential Risk & Business Insight for Law Firms

GETTING READY FOR THE NEW GENERAL DATA PROTECTION REGULATION

Richard Robinson
Managing Director - Legal Compliance Services

In our latest White Paper, our guest author Richard Robinson, Managing Director of Legal Compliance Services, outlines the steps Law Firms will need to take to ensure they are meeting their obligations when the new EU General Data Protection Regulation (GDPR) comes into effect in May 2018.

A massive shake-up in data protection law is upon us. On 25th May 2018 legislation implementing the EU General Data Protection Regulation (GDPR) and the Data Protection Law Enforcement Directive will replace the Data Protection Act 1998.

Given the amounts of information, often sensitive personal data that law firms handle, the ICO and SRA will be expecting all firms to demonstrate they are dealing properly with their obligations.

A lot of scaremongering and headlines focusing on crippling fines and punishments have led to a great deal of confusion. Due to the volume of (mis)information and less than clear nature of the task, many firms are burying their heads in the sand. However, there is no getting around the fact that the new regulations will require careful consideration and appropriate action by all firms, no matter what type or size. As of next May, you will have to be able to demonstrate that you have "the appropriate technical and organisational procedures" and that you are taking all reasonable steps to manage and protect data.

With the average implementation time for small businesses estimated at six months (and ten months and above for others), now is the time to start reviewing your existing data protection compliance to ensure you are not only ready to meet the new requirements, but also that you are already meeting your existing obligations.

Where do you start?

Besides the obvious need to keep information securely, both electronic data and physical documents, there are a number of key areas for most firms to address. Initial areas to focus on should include:

- Compiling an information assets register
- Reviewing your client care letters and terms of business with a view to client consent
- Reviewing arrangements and agreements with suppliers and providers

In order to **compile an information assets register**, you should identify all manual and electronic record keeping systems throughout the firm and maintain a central record of those systems in the form of an information assets register. This will apply to all data held, for example client files and personal information, staff records, expert registers and lists of suppliers. You should then create a central log or record of which business functions create certain records, which records are vital to the functioning of the business, where they are kept, how long they are kept for and who needs to use them now and in the future. From this you should be able to identify potentially damaging processes and how best to manage the risks they pose. All of this should then feed into your overall data protection policy. A record management risk should also be included in your risk register and reviewed regularly.

GDPR will have to become part of every firm's due diligence procedures. To this end, **client care letters and terms of business** will have to be reviewed and amended to ensure the important issue of client consent to the firm processing their clients' personal data is properly addressed. There is some confusion as to how far firms have to go in this regard. The guidance on obtaining consent, published by the ICO, talks about clear affirmative action being required for it to be valid and consent only being an appropriate legal basis to process clients' personal data when clients are offered genuine choices over the use of their data. Further, consent should not be sought where the data would be processed on a different

lawful basis in any event if consent was not obtained, such as if the data was obtained to comply with a firm's obligations under the Money Laundering Regulations 2017.

The ICO's guidance talks about 'granular' consent, which amounts to obtaining separate consents for each proposed use of the data (e. g. the provision of legal services, administration of files and records or the marketing and promotion of your services) and identifying third parties who will rely on the consent you have obtained (such as expert witnesses and professional advisers).

In respect of expert witnesses and professional advisers, a further area of difficulty is likely to be in relation to obtaining the client's consent for sending their information to these and other third parties. The ICO's guidance says that any third parties who will rely on the client's consent should be named, that "even precisely defined categories of third-party organisations will not be acceptable under the GDPR".

The guidance also states that consent requests must be separate or "unbundled" from other terms and conditions. This would suggest that it would not be sufficient to simply ask the client to agree to your terms as set out in your client care letter and terms of business by signing and returning a copy of that document without having sought separate, specific consent for you to process the clients' data in the specific ways sought.

You will need to consider, how, in practical terms, you deal with the situation where a client has consented to only some processing activities and not to others. This may be relatively straightforward in the case of refusing to consent to you sending them marketing and promotional materials where you can simply delete their details from your mailing list. However, it is likely to be more problematic if it relates to a lack of consent to providing information to third parties or administration of files and records.

Another key aspect of compliance is to ensure the protection of personal data that is accessed by suppliers and providers. You should **review**

agreements with existing suppliers to ensure they are compliant with the standards required. Whenever you outsource the processing of personal data, you are likely to remain responsible for the safety of that data and therefore you should:

- Always ensure that you deal with organisations that provide sufficient guarantees about how they will protect data;
- Ensure written and enforceable contracts are in place setting out information security conditions;
- Ensure that the contracts comply with SRA requirements (especially O(7.10);
- Consider whether outsourcing involves the transferring of data overseas (which could include hosted services or cloud computing) and ensure the recipient will provide adequate protection.

About The Author

Richard Robinson is a non-practising solicitor and Managing Director of Legal Compliance Services, a team of former SRA compliance experts who provide bespoke regulatory compliance and risk management services to law firms.

Legal Compliance Services

For further information,

visit www.thestrategicpartner.co.uk

email info@thestrategicpartner.co.uk

call 0207 842 1830

Essential Risk & Business Insight for Law Firms

The Strategic Partner

0207 842 1830

info@thestrategicpartner.co.uk

www.thestrategicpartner.co.uk