GENERAL DATA PROTECTION REGULATION

Guidance for Solicitors

The countdown is on to the 25th May 2018 for the European Union's ("EU") General Data Protection Regulation ("GDPR") which is a significant shake up of data privacy legislation.

Law firms in England and Wales are preparing for the changes in the law and considering what they need to do to ensure that they are prepared and how to get to grips with the changes; interpret what it means for them and how they deal with their clients

The GDPR replaces the current legislation set out under the Data Protection Act 1988. The aim of the new legislation is to protect the data privacy rights of all EU citizens and non-compliance carries much harsher penalties than the previous directive. Britain's forthcoming exit from the EU will not have any effect on the provisions of the GDPR as it will remain part of the UK legislative landscape through the implementation of the EU Withdrawal Act, and Data Protection Bill which are both currently working their way through parliament.

Anne Austin of Enderley Consulting Ltd who are specialist management and risk consultants to the legal sector explains the key points and changes to the current legislation.

WHATS ALL THE FUSS ABOUT?

There's a lot of noise around about the introduction of the EU-wide General Data Protection Regulations (GDPR) which replaces the current UK Data Protection Act on 25 May 2018. **Why is it creating such a stir? How will law firms be affected by it? What will they need to do?**

KEY CHANGES BROUGHT BY THE GDPR

PENALTIES

One of the reasons GDPR has caught the attention of business owners is the potential for eye-wateringly large fines for non-compliance – up to €20m or 4% of global annual turnover. GDPR also makes it considerably easier for individuals to bring claims for 'material and non-material damage' – ie they will be able to claim for distress, hurt feelings, or reputational damage, even when they can't prove financial loss. That's a sea change from the present law.

COMMUNICATING PRIVACY INFORMATION

Once you have a complete list of data, you need to document the lawful basis on which you're holding it. Refresh privacy notices, ensuring they are concise, clear and simple, stating how you intend to use the information and the lawful reason for processing it. The privacy notice should also tell people of their right to complain to the ICO if they think there's a problem with the way you are handling their data.

INFORMATION AUDITS

Organisations must document all the personal data they hold, its source, who can access it, where it's held, why it's held, and who they share it with. Most law firms can call up their database and list their data by client. But how many would be as confident about their paper records, including archives, and files inherited from other firms during mergers? And what's stored on individual desktops, laptops or in email records?

NEW RIGHTS

GDPR provides people with a number of additional rights, including:

- The right to be forgotten – individuals will have the right to demand deletion of personal data where there's no compelling reason for its continued processing. Law firms must have the processes and technology to be able to identify and delete data on request. What do you hold and where?
- Subject access requests – people can ask for all data held on them: organisations must provide this 'without delay', at the latest within one month, and without charge. Can you do this?

To meet the deadlines, it's vital that everyone in a law firm is trained on how to recognise the new rights, and on how to respond to requests to exercise them.

ACCOUNTABILITY

Organisations must be able to demonstrate compliance with the new legislation. Firms must have proper policies and audit trails documenting how processing decisions were made and how they achieve effective data protection. Law firms should review their policies and procedures, updating them to ensure GDPR compliance, and train all their staff on the new requirements.

LAWFUL BASIS & CONSENT

Consent to hold and process personal data is the cornerstone of GDPR. Data is defined as 'any information ... that can be used to directly or indirectly identify the person', eg electronic and paper records of names, email addresses, bank account details, photographs, medical records, IP addresses or social media posts. You must request consent in clear, simple language, separately from other T&Cs, and be specific about how information will be used.

Data subjects (this includes clients and employees) must positively opt-in, with an easy way to withdraw consent at any time. The lawful basis of consent in most cases will be contractual necessity, but it's important to gain consent for areas of work which fall outside this, such as cross-marketing or file reviews by external consultants and assessors. Using personal data for a different purpose needs a new consent.

COUNSEL, EXPERTS & OUTSOURCING

Law firms commonly transfer personal data to other individuals and organisations, eg counsel or medical experts, or to outsourced providers, such as digital dictation or secure shredding companies. Under GDPR the firm, as data controller, retains responsibility (and liability) for the proper and secure handling of their data by third parties and must only engage with those who can provide 'sufficient guarantees'. So, firms must conduct thorough due diligence and review existing agreements to ensure that they are protected.

DATA PROTECTION OFFICERS

Organisations with more than 250 employees, or which process data on a large scale must appoint a DPO. Others will need a DPO-equivalent (for law firms, most likely the COLP) to ensure GDPR compliance and to be the liaison for clients and others with privacy concerns.

DATA SECURITY

Are the firm's data security measures robust and adequately documented? This requires a thorough review of systems and policies, with data security a standing agenda item at Board or Partners meetings. Consider whether your electronic systems, firewall, and anti-virus software up-to-date. How do you ensure the security of data sent by email? How are passwords managed? Do members of your firm store data on their desktop? If you allow removal of files from the office, how do you ensure their security?

INTERNATIONAL TRANSFERS

Law firms making regular cross-border data transfers need to assess the legal basis for the transfer (is the country deemed 'adequate' by the EC, or will you rely on special derogations, most likely contractual necessity?). Devise a specific cross-border transfer privacy notice, and ensure the firm has appropriate safeguards in place to protect the personal data being transferred.

PRIVACY IMPACT ASSESSMENTS

Under GDPR, privacy risks must be assessed at the start of any new project, and reassessed continuously. You must carry out a privacy impact assessment whenever the risk of breach is high due to the nature or scope of the processing operation, eg where a firm is planning to buy new software and data will be migrated, or in a merger where datasets will be combined. It also applies to processing data concerning vulnerable subjects. GDPR defines 'vulnerable' as where there is a power imbalance between the data controller and the data subject, and the individual may not be able to consent to or oppose the processing of their data. This could apply to children and vulnerable adults, but also to HR activities.Under GDPR, privacy risks must be assessed at the start of any new project, and reassessed continuously. You must carry out a privacy impact assessment whenever the risk of breach is high due to the nature or scope of the processing operation, eg where a firm is planning to buy new software and data will be migrated, or in a merger where datasets will be combined. It also applies to processing data concerning vulnerable subjects. GDPR defines 'vulnerable' as where there is a power imbalance between the data controller and the data subject, and the individual may not be able to consent to or oppose the processing of their data. This could apply to children and vulnerable adults, but also to HR activities. Under GDPR, privacy risks must be assessed at the start of any new project, and reassessed continuously. You must carry out a privacy impact assessment whenever the risk of breach is high due to the nature or scope of the processing operation, eg where a firm is planning to buy new software and data will be migrated, or in a merger where datasets will be combined. It also applies to processing data concerning vulnerable subjects. GDPR defines 'vulnerable' as where there is a power imbalance between the data controller and the data subject, and the individual may not be able to consent to or oppose the processing of their data. This could apply to children and vulnerable adults, but also to HR activities.

REPORTING BREACHES

This doesn't just mean the loss of data, but also destruction, alteration, unauthorised disclosure of, or access to, personal data. Currently, there is no obligation to report a breach, but GDPR requires the report of data breaches to the ICO within 72 hours. There are potentially serious consequences of failing to do so – a fine of up to €10m or 2% of global turnover. Practically, this means that everyone in a firm must be able to recognise a breach, with clear reporting lines to ensure a rapid response.

With the introduction of GDPR on 25 May 2018, privacy becomes central to everything you do, and firms should start preparing now. You should review all the data you hold and assess whether you have consent or other lawful basis for processing. This is no mean feat and will require board/partner level commitment. Privacy just became real.

If you would like practical, no-jargon help in reviewing and revising your policies and procedures, or training your staff to achieve GDPR compliance, please call Anne Austin on 01743 294 866 or 07533 571871.

POSSIBLE INSURANCE SOLUTIONS

A CYBER/DATA RISK INSURANCE POLICY

Purchasing a specific cyber liability policy can include cover for data risk's such as the following;

IMMEDIATE INCIDENT RESPONSE COSTS & LEGAL REGULATORY COSTS

Dealing quickly with a Data Breach is going to be essential. The potential of mandatory reporting within 72 hours means it will be essential to quickly identify the scale and nature of a breach. It includes an external IT security consultant to identify the source and scope of breach and provide advice on remediation. This will also include obtaining legal advice to determine the correct course of action, drafting breach notification letters, notifying the ICO or other body (and then responding to any subsequent investigation or action)

CRISIS COMMUNICATION COSTS

How you have prepared for GDPR, and also how you deal with a breach will very likely depend on how any ICO investigation would conclude. The policy covers the costs of engaging a Crisis Communication consultant for advice, to formulate a plan, and to co-ordinate media relations.

PRIVACY BREACH MANAGEMENT COSTS

If it is determined that notifications must be made (whether they are mandatory under GDPR) then the policy will cover the cost of collating and issuing notices, credit monitoring, identity monitoring, and the costs of handling resultant queries.

PRIVACY LIABILITY

The GDPR creates the right to seek compensation as a result of a data loss. The policy provides indemnification of sums you become legally obliged to pay as a result of a claim following disclosure of personal information, your failure to adequately warn affected individuals, breach of confidentiality, or breach of your privacy policy.

REGULATORY FINES

The GDPR increases the maximum potential fine from the present £500,000 to a sum closer to £20m. The policy will cover any legally insurable fine as a result of an investigation by the ICO.

ADDITIONAL COVERS

Specific cyber insurance can also include additional covers (if chosen) such as cyber crime (theft of money through a cyber crime), telephone hacking (lines being hacked by third parties resulting in unauthorised call charges), phishing scams and media liability such as defamation.

We would be delighted to discuss this or your individual circumstances in more detail.

JIM BRINDLEY
ACCOUNT EXECUTIVE

james.brindley@tlorisk.com
0121 212 9090

Victory House
26 - 28 Ludgate Hill
Birmingham
B3 1DX