GENERAL DATA PROTECTION REGULATION

Guidance for Barristers and Chambers

Duncan Goodfellow - Director
TLO Risk Services Limited

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.

Barristers and Chambers around the country 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.

KEY CHANGES BROUGHT BY THE GDPR

PENALTIES

A tiered approach of penalties will be applied to those who do not comply with the GDPR; the maximum fine that can be applied for the most serious infringement is 20m EUR, or 4% of annual global turnover.

Whilst this is a significant increase from the present maximum of £500,000, the Information Commissioners Office ("ICO") has sought to give some reassurance. Data Commissioner Elizabeth Denham has said "It's true we'll have the power to impose fines much bigger than the £500,000 limit the DPA allows us, but it's scaremongering to suggest that we'll be making early examples of organisations for minor infringements or that maximum fines will become the norm. The ICO's commitment to guiding, advising and educating organisations about how to comply with the law will not change under the GDPR. We have always preferred the carrot to the stick."

DATA SUBJECT RIGHTS

In addition to the above key changes, data subject rights are extended and made clear including;

- The right to be notified within 72 hours of a data breach where the breach is serious
- The right to seek compensation as a result of infringement of the GDPR
- The right to access their data, free of charge and for them to have information about reasons for processing
- Rights to be forgotten which entitles the data subject to have the data processor remove the data concerning them
- Rights to transport the data to another controller in a commonly used and machine readable format, rights to privacy by design, i.e. only having data held about them that is relevant to the purpose of processing and limiting the amount of data that is accessible to the processor

In addition, Data Protection Officers must be appointed for every organisation that engages in processing of large scale systematic monitoring or large scale sensitive personal data

TERRITORY

Scope of the legislation will be applied to controlling and processing of data of all EU citizens, regardless of whether the processing takes place in the EU

CONSENT

Data Controllers and processors must now use clear and distinguishable language to request data subjects' permission for data processing and it must be easy for the data subjects to withdraw their consent as it is to give it. The permissions should be kept separate from any other terms and conditions and must not contain any long illegible legalese language.

EXPANSION OF SCOPE & RESPONSIBILITY

In the past, only data controllers were considered responsible for data processing activities but the GDPR extends liability to all organisations that touch personal data. The GDPR imposes obligations directly on data processors – which was not the case previously and therefore Chambers and staff must comply with those obligations, not just the Barristers as Data Controllers.

KEY CONSIDERATIONS FOR BARRISTERS & CHAMBERS

DATA CONTROLLERS & DATA PROCESSORS

1. Every individual practising barrister is a data controller

2. A chambers would be a data controller in respect of information about the management of chambers, although depending on the constitution, this may fall to the Head of Chambers, on behalf of Chambers.

3. A chambers will be a data processor as a result of work undertaken for Barristers

4. As a data processor, the GDPR will put specific obligations on chambers in respect of record keeping, breach notification and contractual arrangements with sub-processors.

CONTRACTUAL TERMS & PRIVACY NOTICES

It will be necessary to amend contractual terms or publish appropriate privacy notices to set out the subject matter and duration of the processing of personal data by the barrister or chambers of their client/lay client. It would be desirable for contractual terms to be drafted in such a way that explicit consent to process data is obtained. Where the lay client is instructing via professional clients, consent should be obtained indirectly.

DON'T RETAIN UNNECESSARY "PERSONAL" DATA

If personal data (in the form of past papers or drafts) is to be retained for research purposes – barristers should consider first deleting personal information from those drafts, to anonymise them and minimise Data retention.

DATA RETENTION & STORAGE

Give serious thought to Data Retention, and whether each Barrister should have a personal retention policy, as well as a chambers policy.

- Consider what data to retain, and the reason why
- Consider organising work/filing which facilitates easy future deletion
- Implement a process of redacting personal information on material retained for future reference
- Where possible, implement a process of identifying retention periods for data at the outset of a case – which can then form the basis of a future retention and deletion plan.
- In addition to Barristers having processes in place to delete data which they store themselves, Chambers will also need to consider how data would be deleted from practice management systems.
- Where data is hosted by third parties – ensure that the agreements in place are commensurate with the obligations of the data controller. Ensure that cloud storage providers are compliant, and if they are US-based, that they are Privacy Shield compliant.
- Data stored electronically should be encrypted. This is as important for historic data as current data (so backup or archive hard drives should be encrypted).
- Information Security remains key; ensure that individual Barristers employ proper password security, encryption of data, regular backups, firewalls, applying updates to operating systems, safe disposal of old equipment and also cross-border data transfer.
- Specific requirements around record keeping may also apply to Barristers or sets who carry out Criminal work, or who handle special sensitive data (medical negligence, personal injury).

INFORMATION SECURITY

Information Security remains key; ensure that individual Barristers employ proper password security, encryption of data, regular backups, firewalls, applying updates to operating systems, safe disposal of old equipment and are aware of cross-border data transfer issues. It is important to ensure all these issues are considered for "personal" equipment – so perhaps introducing some consistent chambers 'standard minimums' which should be adhered to.

PLAN AHEAD FOR CHANGES

If a barrister leaves chambers – chambers must, at the choice of the barrister, delete or return all personal data which relate to their cases, and would also extend to back up or archives.

RESPONSIBILITY FOR DATA PROTECTION

It is unlikely a Chambers would need to appoint at "Data Protection Officer" and indeed it would be inadvisable to give someone this title unless they were required to have one. It may however be appropriate to appoint an individual to be responsible for Data Protection within the Chambers.

It should be noted that this is non-exhaustive advice, and is intended to highlight some of the particular issues which would appear to require more detailed consideration within chambers. Much of this advice has been drawn from the Bar Council Guide to General Data Protection Regulation which is a very detailed guide which has been prepared to assist barristers and chambers in their compliance with the GDPR.

Overleaf we outline some of the insurance solutions which can assist as part of an overall approach to GDPR. We place various Cyber/Data covers on behalf of chambers across England & Wales from small regional sets through to many in The Lawyer Top 30.

POSSIBLE INSURANCE SOLUTIONS

A Cyber/Data Risks Insurance Policy: Where does that fit into the jigsaw?

WHO DOES IT COVER?

A policy for Chambers would cover the Head of Chambers (when acting on behalf of other members in that capacity), each Barrister as an individual, a Management Company if one exists, Clerks (including self employed) and other chambers staff. This is the most comprehensive approach – ensuring that "everyone" is included.

WHAT DOES IT COVER?

AND HOW DOES THAT ADDRESS SOME OF THE RISKS POSED BY THE GDPR?

IMMEDIATE INCIDENT RESPONSE COSTS AND 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 COMMUNICATIONS 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 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.

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.

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.

WHAT ARE THE INSURANCE OPTIONS & COST IMPLICATIONS?

OPTION ONE: PURCHASE TOP UP FROM TLO - WHICH PROVIDES THE DATA PROTECTION EXTENSION

Obviously the main purpose of this cover is to "Top up" the Bar Mutual professional indemnity cover a barrister currently holds and can be done in tranches £2.5m. This option applies to anyone currently taking out the maximum amount of cover with Bar Mutual (£2.5m) and the Data Protection extension is automatically included with TLO top up product. The extension provides costs in connection with an investigation by the ICO, and then any legally insurable fine – up to a policy limit of £500,000 with an excess of £2,500. The cover is only in relation to ICO investigation costs and legally insurable fines, and would not provide protection for the broader exposures brought about by GDPR.

OPTION TWO: CLAUSES 2 & 3 OF THE TLO TOP UP PRODUCT ONLY – PURCHASED ON AN INDIVIDUAL BARRISTER BASIS (BUT CAN BE ARRANGED COLLECTIVELY ON A GROUP DECLARATION/INVOICE)

A further option is to purchase an "element" of the TLO top up cover – where buying the entire product is unsuitable. This option provides Insuring Clauses 2 and 3 of our cover – so the Additional Legal Services and Data Protection Extension.
The ALS section would provide cover for up to £2,500,000 for the additional elements of £50,000 for Loss of Documents and £500,000 for Data Protection. £250 excess for the ALS section, and £2,500 for the Data Protection section. These are individual policies – but could be arranged/invoiced on a collective basis if there were a number of members interested. This option allows certain members to purchase the cover, but does not require all members to purchase it.

OPTION THREE: A SEPARATE DEDICATED DATA RISKS/CYBER POLICY PURCHASED ON AN INDIVIDUAL BARRISTER BASIS AND TYPICALLY COSTS £560 PER BARRISTER, ALTHOUGH LESS EXPENSIVE OPTIONS ARE AVAILABLE WITH NARROWER COVER.

Where Top up cover is not appropriate, or if you require a broader degree of cover than the extension under the Top up policy, it is possible to purchase a separate Data Risks and Cyber policy. As well as providing the same investigation/fines cover it also includes the following heads of cover: Cyber Incident Response (plus legal costs, IT costs, Crisis costs), System Damage and Business Interruption, Network Security and Privacy Liability (Privacy Liability, Regulatory Fines), and Media Liability (defamation, IP infringement). The cover focuses on Cyber risk – but also covers Data breaches from the more traditional exposures of a lost file or stolen briefcase. Limit of Indemnity would typically be £1m.

OPTION FOUR: A SEPARATE DEDICATED DATA RISKS/CYBER POLICY PURCHASED ON A WHOLE CHAMBER BASIS AND TYPICALLY COSTS LESS THAN £75 PER BARRISTER ON A RECHARGE BASIS FOR A £1M LIMIT

This provides the same degree of cover as option three, but can also be extended to include Cyber Crime (Funds transfer fraud, extortion, identity theft, phishing) – but it is purchased in the name of Head of Chambers/Chambers/Service Company – and will provide cover for all members, but also all other staff/clerks and pupils. The other options only cover the individual Barrister. It has to be purchased to cover everyone/the whole chambers – it is not possible for only a number of members to participate. The premium would be charged and paid for collectively and then recovered through expenses/recharge. Limits of Indemnity would typically be between £1m-5m.

Option Four clearly provides the greatest degree of protection for barristers, chambers and staff, and often at the lowest overall comparable costs – but does require the collective agreement of all members of a chambers in order to take this option.

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

Duncan Goodfellow
Director

duncan.goodfellow@tlorisk.com

[Credit: GDPR - Bar Council Guide for Barrister Chambers, Equilibrium Security]