New York State Bar Association

Tokyo Conference

Ethical Issues for Lawyers and Law Firms

Concerning Cyber Security

Panel 17

Introduction

In Europe, lawyers are subject to the General Data Protection Regulation (GDPR) and local privacy laws (such as the UK Data Protection Act 2018) just as any other organisation might be. You can find out details of GDPR here www.bit.ly/gdprfaq and details of DPA 2018 here https://www.corderycompliance.com/client-alert-data-protection-act-2018/

In addition, lawyers are subject to professional requirements generally laid out by their local bar. The regulatory regime for lawyers across Europe can be complex with national and regional bars in some countries. There are other complexities too – for example in the UK there is a split profession (barristers and solicitors) and the regulatory regime can be complex. Prosecutions are not brought by the bar in the UK but by regulators with special authority over law firms including the Solicitors Regulatory Authority (SRA) for solicitors and the Bar Standards Board (BSB) for barristers.

General Regulation

Data Protection Authorities (DPAs) including the Information Commissioners Office (ICO) in the UK have taken action against lawyers for data breaches. For example in March 2017, the ICO fined a barrister £1000 for a data breach. The name of the barrister was not given. She was reported by a solicitor who informed the barristers' chambers that confidential information processed by her was publicly accessible on the internet. It turned out that the barrister's husband had decided to back-up 725 documents from her laptop prior to a software update from the computer she had used for her practice. In backing up the files he had inadvertently made some of the documents publicly accessible. Six documents were highly confidential and related to proceedings in the Court of Protection. The ICO decided that the barrister had failed to put in place appropriate technical measures (as was required by GDPR) and fined her £1000. Whilst GDPR is the best-known law in Europe dealing with data security it is not the only one. The NIS regime, explained on film here http://bit.ly/cordonnis affects many sectors and will be especially relevant to in-house counsel. Additional provisions exist across Europe in local law or regulation.

Lawyer – Specific Regulation

In some respects professional obligations can overlap with GDPR obligations. For example both GDPR and the SRA rules will require breaches to be logged and reported. The SRA guidance says:

> "*You need to have a system in place to record any failures in compliance so that you can monitor overall compliance with the firm's obligations and assess the effectiveness of its arrangements and systems. The record of breaches also allows you, in your compliance officer role, to decide whether you need to report breaches as material, because they form a pattern of non-compliance. Breaches which are material – either in themselves or because of a pattern – must be reported to the SRA as soon as reasonably practical. In most cases that should mean immediately*".

Note that under GDPR there is also a requirement to report most breaches to a Data Protection Authority (DPA) which also should be done immediately and in most cases within 72 hours.

The SRA guidance says that a number of factors should be taken into account when deciding whether a data breach is material or not including:

- The detriment or risk of detriment to clients
- The risk of loss of confidence in the firm or in the provision of legal services
- The scale of the issue
- The overall impact on the practice, clients and third parties

In the UK solicitors are increasingly the target of cyber-crime. 103 reports were made to the SRA in 2016, 157 reports in 2017 and 76 reports in the first half of 2018 (the last period for which figures seem to be publicly available). In 2016 £9.4m of client money was reported to the SRA as lost due to cyber-crime, increasing to £10.7m in 2017. Email modification fraud accounted for 80% of all cyber-crime reports to the SRA in the second quarter of 2018. This is commonly used in real estate transactions to divert money.

The SRA has taken action after a data breach. For example in July 2018 it was reported that the SRA fined two branches of Slater & Gordon £40,000 each and ordered them to pay £26,000 in costs for disclosing unredacted data from client files to other firms.

Barristers also have a core duty to keep their clients' affairs confidential. In March 2017 for example the BSB fined a barrister £750 who had been disposing of documents that contained confidential and sensitive information in household refuse sacks. The same rules apply to hard copy and electronic data.

It is important to remember this is not an either or situation. For example in 2012 solicitor Andrew Crossley formerly of ACS: Law was suspended by the Solicitors Disciplinary Tribunal and ordered to pay costs of £76,326.55 after he threatened file sharers resulting in his firm's network being hacked. Crossley had installed a network more suitable for home use rather than for a law firm. The SRA heard how his 15 year relationship had broken down and that he was in danger of losing his house. Crossley was also fined by the ICO for the data breach in 2011.

Jonathan Armstrong
Cordery
Lexis House
30 Farringdon Street
London EC4A 4HH

Office: +44 (0) 20 7075 1784
jonathan.armstrong@corderycompliance.com