Confused about GDPR - don't be!

Keepabl's Robert Baugh reviews the statistics on the Legal profession and GDPR, how the industry's leaving itself open to data risk, and easy remediation steps.

"Many law firms are confused about GDPR. This puts client data, and even firms themselves, at risk."

GDPR is now one year old, and with it the legal obligation to notify certain data breaches to the UK Information Commissioner's Office within just 72 hours.

How is Law doing as an industry? Well, not so good, judging by recent statistics. Aon's December 2018 survey of UK SMEs found that 40% of the Legal industry is confused by GDPR and 68% of UK SMEs were unaware of the need to notify certain breaches to the UK ICO.

This presents a real risk to law firms' revenues and their client base, given the sensitive nature of client information processed by firms. More realistic risks for firms than fines perhaps, include not being able to answer the vendor due diligence that clients carry out, so work is lost, and the impact if a client's data is put at risk by a breach.

Speaking of GDPR fines, how does your firm measure up on these examples?

- September 2018: the Austrian DPA fines a sports betting café €5,280 on its use of CCTV. It covered public areas, they kept no logs, they retained images without justification, and they had inadequate signs.
- November 2018: a German DPA fines a social media organisation €20,000 after the organisation itself notified them of a breach. The DPA found that passwords were stored in plain text. The 'low' fine was due to the organisation's exemplary co-operation and response, and the DPA estimating that, including the fine and remediation costs, the organisation's total costs were more than €100,000.
- February 2019: Malta's DPA fines the Land Authority €5,000 after investigating a breach (initially reported by a newspaper) as its website lacked the necessary technical and organisational measures to ensure the security of processing.
- March 2019: the Danish DPA recommends a fine of £140,000 against a taxi company for retaining phone numbers for 5 years with no justification (having deleted most personal data after 2 years).

The German social media example is a good reminder that the fines for a breach are likely to be dwarfed by other costs. There, the remediation costs (encrypting passwords, implementing secure backup, etc) overshadowed the fine by a ratio of 4 to 1.

These fines may be well below GDPR's maximums, but a £100,000 total cost will impact most law firms. You'll also see the fines go beyond security, into privacy governance failures.

So, what can firms do? The immediate, easy step is to encrypt data at rest (in the memory of phones, laptops, servers etc.) and in transit (e.g. by using HTTPS not HTTP). It's very easy to implement, with most devices and services offering this by default or built in as an option. Encryption addresses the risk to your clients, and it addresses your risk as a firm. And many encryption services allow you to remote wipe lost devices. Win, win.

Next you do need to review (or probably implement) your Information Security Governance and Privacy Governance. For security, you can start by working towards Cyber Essentials. For privacy governance, plenty of providers (including Keepabl) offer a SaaS solution.

You'll need to implement policies and procedures for each, train on them and make sure you follow them. It may sound a lot, but so does £100,000.

And there's no real choice: GDPR requires you take 'appropriate technical and organisational measures to ensure a level of security appropriate to the risk'. There are plenty of Managed Service Providers who can look after a law firm's security needs and many can go beyond, and help with GDPR too, bringing in specialist technology without breaking the bank.

Robert Baugh
is CEO at Keepabl