Yorkshire Finance Leaders

Future-proof your data strategy

By Emma Roe, **Partner and Head of Commercial at Shulmans LLP**

The UK's referendum result back in June 2016 defied all the pollsters when the nation voted to cut ties with the European Union and go it alone. But what does this historic change mean for how businesses handle that increasingly valuable asset of personal data.

At the time of the Brexit vote, the shock result caused political upheaval, a tumbling FTSE 100 and economic uncertainty. Some might argue those immediate aftershocks have continued as the UK government has worked towards and, on 29 March this year, triggered the Article 50 notice required to start negotiations for departure from the EU club.

Some of the more recent and upcoming developments in data protection laws in the UK and the EU may have been rather overshadowed by the Brexit vote last summer and the continuing effects of that outcome.

However, it's important to consider where this leaves businesses as they continue to handle the personal information of UK customers and contacts.

The new EU General Data Protection Regulation (GDPR) came into force in May 2016 and will automatically take effect throughout the EU (including the UK if it is still part of the EU at that time) from 25 May 2018. So, many will ask, should Brexit alter the approach to data protection being taken by any business handling the data of its UK based customers? In short, no, because Brexit, as we now know, is going to take time.

Continues overleaf

Future-proof your data strategy continued

After the Article 50 notice was issued, triggering negotiations with the EU, we were automatically in a window of at least two years. During this negotiation period data protection compliance will mean abiding by the current UK Data Protection Act 1998 and the EU Directive from which it derives.

The GDPR takes effect in May 2018, at which point those handling UK customer data or selling their goods and services into the UK market will need to comply with the new GDPR. As a result we all have less than 18 months now to prepare for and adapt our approach to data in order to meet the more stringent regime of the GDPR.

Whilst key data protection principles have not changed fundamentally in the GDPR, many have been strengthened to place more structure around how compliance is achieved. For example, aspects such as the appointment of data protection officers and reporting of security breaches have moved from discretionary to mandatory requirements.

In November 2016, the Secretary of State for Culture, Media and Sport confirmed that as the UK will still be a member of the EU in May 2018, businesses do need to continue to plan for full compliance with the GDPR. Likewise, clear comments coming from the Information Commissioner, Elizabeth Denham, also support this approach; the UK data protection regime will have to adapt to align itself closely with the new approach in the GDPR, regardless of Brexit. Once the UK is outside the EU, it is going to need something very similar to the GDPR in place in order to make transfers from the EU to the UK compliant.

Compliance with GDPR isn't a wasted effort; compliant organisations will be able to leverage from that position to react to the UK's response to GDPR post Brexit with minimal disruption.

Achieving compliance with GDPR is, therefore, not going to be a wasted effort as it will be work which all organisations can then leverage from to ensure they are then compliant with whatever UK legislation replaces GDPR upon Brexit – essentially looking at this issue now is a way of future-proofing compliance in this space.

Another key consideration relating to compliance with data protection laws is the risk posed by cyber security threats to any business. Recent attacks on the likes of TalkTalk and Sage have highlighted the two sides of this threat – the external hacking of customer data suffered by TalkTalk and the internal employee failure experienced by Sage. After an inquiry into the TalkTalk cyber-attack, the Culture, Media and Sport Committee issued a cyber security report which gave some useful guidance to organisations facing a data breach.






GDPR includes various significant changes such as the expansion of compliance requirements to include data processors (not just data controllers), mandatory reporting of data breaches within stipulated timescales and increased fine thresholds of:

- up to 2% of annual worldwide turnover of the preceding financial year or 10 million euros (whichever is the greater) for violations relating to internal record keeping, data processor contracts, data security and breach notification, data protection officers, and data protection by design and default; and
- up to 4% of annual worldwide turnover of the preceding financial year or 20 million euros (whichever is the greater) for violations relating to breaches of the data protection principles, conditions for consent, data subjects rights and international data transfers.

It's important to remember that even if a business has outsourced a business critical service, such as accounting and payroll functions, this doesn't remove or transfer that organisation's responsibility for what happens to the personal data that is involved in that service – the business will remain responsible for data protection purposes and so remains liable for the acts of that outsourced provider processing the data on its behalf.

Data compliance is key to an effective cyber strategy as well as being a legal requirement.

The Sage incident is a timely reminder of where organisations might best focus their energies in the compliance battle around protecting personal data and the privacy of individuals. Businesses are increasingly interested in how to protect themselves from the risk of external cyber-security breaches (and rightly so), but the security threat posed by internal breaches is potentially just as damaging and possibly harder to detect. Whilst it might come down to simple human error, weak password management or a disgruntled ex-employee having retained unauthorised access to systems when they should not have done, there is probably more scope for businesses to mitigate these areas of internal risk than those of the external variety.

These data breach incidents involving household name businesses continue to inform our own awareness of personal vulnerability to identity theft, an aspect which the Culture, Media and Sport Committee were also keen to encourage as a matter of public vigilance.

Likewise they highlight how the strength of a business strategy designed around full awareness of your business's data and compliance with data protection laws can help protect against such risks.

Businesses need to be looking to achieve good data protection compliance not only to counteract cyber risks more generally, but also to place themselves in a position to adapt to the developing data protection landscape. By doing so any business will be able to achieve an element of future-proofing, as the UK data protection regime adjusts to accommodate Brexit, whilst also ensuring compliance when GDPR begins to bite come May 2018.

To discuss further, contact **Emma Roe** at **Shulmans LLP** on **0113 288 2817**, or by email **eroe@shulmans.co.uk**

Shulmans

About us

Shulmans is a full service UK top 200 corporate law firm, delivering award winning, first-class legal services to its clients.

The firm is also a member of the Interlegal network, with ready access to high-quality legal advice from firms with local knowledge across the world, to help clients in their international and cross-border transactions.

The firm's Commercial offering boasts a seven-strong team of lawyers all of whom have a specialist focus in the technology and risk management space. Shulmans is committed to providing practical advice, from contract negotiations to working with clients to build solutions to the development of compliance protocol. It also provides swift and decisive incident response and regulator engagement support services to facilitate its client's successes.

With data being an increasingly crucial asset of businesses, the management of risk is a critical operational function. In this ever-changing area of law, Shulmans' support includes audits, training programmes and the drafting of compliance documentation to reflect the latest legal and regulatory requirements.

The team's international expertise also extends the firm's scope to handle global data transfers, outsourcing of information handling services and coordinate client or customer-facing documentation.

For further information, please email either Nick Horbowyj, Katie Pepper or Ryan Lewis on **shulmans@lucre.co.uk**; alternatively, telephone **0113 243 1117.**

www.shulmans.co.uk