LEWIS SILKIN

Top 5 GDPR issues for... professional service firms

With the EU General Data Protection Regulation ("GDPR") looming on the horizon, we take a look at some of the key changes of how this legislation will affect professional services firms from 25 May 2018.

1. Security & Breach Notifications

The reality is that professional services firms have, for some time now, been identified as attractive targets by 'bad actors'. Firms are entrusted with confidences – both commercial and personal – which are invariably of high value in the wrong hands. Large sums of money can also pass through their accounts. A misplaced sense of security, not helped by a historic underreporting of breaches, has left some with a soft underbelly. This combination can mean rich and relatively easy pickings for attackers.

Whilst expectations regarding security standards don't differ under the GDPR from existing laws in that "appropriate technical and organisation measures" still need to be implemented, the GDPR does now hint at what "appropriate" means. "Pseudonymisation" and "encryption" are measures which can help mitigate risk, and use of them could mean the difference between having to publicise a breach or not.

Ensuring that client data is held securely is, for those professions with confidentiality obligations in respect of information about their clients' affairs, as much a matter of professional conduct as it is data protection compliance. Keeping client data secure will already be high on the priority list. The GDPR should bump data security up to the top of the agenda due to its much publicised fines of up to €10 million or 2% of global annual turnover for the preceding year where breaches are security related. Fines can be double those figures for many other types of breach. The incumbent Commissioner describes this as "a pretty big stick".

With enforcement action comes damaging publicity. Cyber insurance policies might help ease some of the financial impact of a breach, but reputations are likely to be where trusted advisors are hardest hit. So the new breach notification requirements in the GDPR, which can require a firm to notify a breach to the supervisory authority and data subjects, has the potential to be all the more damaging in the context of professional services. In deciding whether or not to notify, firms won't have the luxury of time. In a crisis, 72 hours goes by quickly. This is even more so when stakeholders are spread across different time zones. So a breach response needs to be a documented and well rehearsed process.

2. Supplier Arrangements

The ICO takes the view that providers of professional services – particularly in the fields of law and accountancy – are likely to be considered data controllers, not just of their organisations' own data, but also of personal data processed on behalf of clients to carry out their instructions. The analysis is a factual one and turns on the particular processing activity. That much isn't new. But where firms are data controllers, they will remain in the driving seat when it comes to data protection compliance.

There are, however, some important changes on the horizon where firms engage suppliers to process data on their behalves, such that existing arrangements will need to be reviewed and updated.

Agreements with suppliers will still need to be in writing. The GDPR mandates, however, that those agreements contain a range of guarantees addressing additional matters from restrictions on subcontracting to conducting supplier due diligence.

The GDPR also introduces a change to how responsibility is allocated between controllers and processors in a way which makes processors more accountable. Since (for example) processors will be directly liable for their own security obligations, the buck will no longer stop solely with a controller in the event of a breach by its supplier. Firms may experience suppliers being more likely to want to agree up front the particular appropriate security measures which may add a layer of complexity when negotiating agreements.

3. Accountability & Governance

When it comes to their clients' affairs, most professional advisors are seasoned record keepers. The GDPR also needs to be approached with that mind-set, as firms will be required to maintain internal records of their processing activities.
Record keeping is, however, just one of a number of ways that accountability and governance is promoted under the GDPR, especially since the current registration system will be done away with (although there'll likely still be a fee of some sort to pay).
Other ways include elevating what are currently considered to be good practices – such as the use of privacy impact assessments and adopting 'privacy by design' – to mandatory requirements in certain circumstances.
Firms will also need to consider whether their core activities involve "regular and systematic monitoring of data subjects on a large scale" or if they conduct large scale processing of special categories of data (think "sensitive personal data", plus genetic/biometric data).

If the answer is 'yes', a 'data protection officer' (DPO) will need to be appointed. That appointment must meet various requirements, including those necessary to ensure the DPO's autonomy.

4. International Issues

Firms regularly transfer data overseas in discharging client assignments or among their own operations, sometimes unaware that they are doing so. That is commonly the case where data are hosted remotely though use of 'software as a service' (SaaS) or where firms are (as is increasingly the case) engaging external data centre providers to replace the use of their own on-site servers. Whilst these operations can introduce efficiencies, they can also represent a significant risk, not just in terms of security and confidentiality, but to privacy compliance as well.

Restrictions imposed by the GDPR on transfers of data outside the EU aren't too dissimilar from those currently in play. Firms will still need a lawful basis to do so. There are some differences, however. Self-assessment of adequacy is 'out'. Codes of conduct and certification mechanisms are 'in'. Binding corporate rules, heralded as a facilitator of intra-group transfers, are now explicitly recognised. There are also some tweaks to derogations, notably to consent, as well as the introduction of a new derogation (of limited scope) where there is a "compelling legitimate interest."

Just as likely to impact on international transfers are further legal challenges to safeguards such as the use of model clauses and the 'Privacy Shield'. Also, whilst EU law (such as the GDPR) is to apply to the UK for the time being, the UK's departure from the EU has created uncertainty about how the free flow of data – which is vital for cross-border trade – will be maintained on the UK's departure from the EU.

Firms operating across the EU will also need to identify a 'lead supervisory authority' which, as the title suggests, will take the lead when it comes to ensuring compliance. Given differing approaches to enforcement by member states, firms will need to work out the supervisory authority to which they will be subject, and be prepared for that decision perhaps to be challenged.

5. Consent

Despite its limitations, consent is often used by professional services firms as a basis for lawful processing in a wide range of contexts, from the workplace to disclosures of client data to third parties (which also raises professional conduct issues for many regulated entities).

Whilst consent remains a legal basis for processing personal data, the GDPR introduces a higher standard which builds on previous requirements and will, in practice, be more difficult to meet – especially in the workplace. Firms will therefore need to review their processing activities across the board to determine whether consent is still appropriate and, if so, that the correct mechanisms are in place to comply with the new requirements. Don't forget that consent isn't the only legal basis for processing personal data: one of the five alternatives which are still available might be more appropriate.

Why does it matter?

For professional services firms, trust is an important currency. Once lost, it is often impossible to regain. The changes introduced by the GDPR should assist compliant firms to maintain that trust when it comes to the way they use data, but there is much to do to achieve its high standards. Given what is at stake, those firms would be best advised to prepare as soon as possible.

This note is not intended to be an exhaustive list of GDPR changes, so if you require any further information or advice about this subject please contact:

James Gill
Partner, Data & Privacy

+44 (0) 20 7074 8217
james.gill@lewissilkin.com

Ellen Temperton
Partner, Employment

+44 (0) 20 7074 8424
ellen.temperton@lewissilkin.com

Alexander Milner-Smith
Managing Associate, Employment

+44 (0) 20 7074 8196
alexander.milner-smith@lewissilkin.com

Ali Vaziri
Senior Associate, Data & Privacy

+44 (0) 20 7074 8122
ali.vaziri@lewissilkin.com