THE GATHERING STORM

Recent months have seen very major data protection law changes that affect not just UK or EU companies, but any companies which are deemed to be caught by 'processing' EU data. With data centres on the hook following these changes, ***Rafi Azim-Khan*** *and* ***Steven Farmer*** *at* ***Pillsbury Winthrop Shaw Pittman*** *give an insight on what to expect.*

By way of reminder, data processors are those who process (e.g. store) personal data on behalf of a data controller (i.e. those that determine the purpose for and manner in which personal data is processed) and include those who provide data centre services, hosting providers, cloud providers and so on.

New fines increasing penalties from £5,000 to £500,000 per offence, a recently appointed enforcer with new priorities in the UK, and not to mention the new European Data Protection Regulation with even larger fines on the horizon, mean that those companies who previously thought that they had data protection 'covered' are being forced to think again. Failure to take appropriate action on the back of these developments could prove an expensive and damaging mistake, particularly for those whose business model is based around the storage of third party data.

The current regime

A criticism of the current regulatory regime i.e. the European Data Protection Directive (implemented in the UK via the Data Protection Act 1998) is that data processors are not directly liable for breaches of the law in the same way that data controllers are. Rather, the buck essentially stops with the data controller if a data processor fails to comply with obligations imposed on a data controller by the Directive.

In practice, data processors often have obligations passed on to them under a contract with the data controller (offering data controllers some degree of comfort). However, this state of affairs is far from ideal for data controllers, particularly when it is borne in mind that a large number of recent, high profile breaches have been caused by the default of data processors.

Changes on the horizon

Key changes expected to be introduced by the new regulation, which should be on a data processor's radar, include:

- **Increased prosecutions/fines**

The push for much more aggressive fine levels and enforcement is the end result of too many companies taking a half hearted approach to data protection compliance, a view expressed by the enforcers along with increasing impatience and greater appetite for enforcement action.

Possibly to be introduced later this year, the regulation may also usher in further grandiose changes with proposals to beef up and alter the current main Directive.

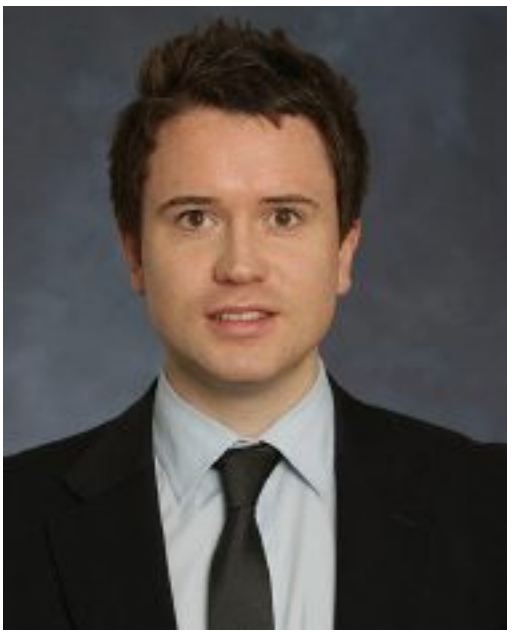
A key part of the new regulation is even larger fines – five per cent of global turnover or up to 100 million euros for data protection breaches have been proposed.

Importantly, it is proposed that these will apply directly to data processors who could previously hide behind the veil of a contract with a data controller.

Furthermore, noteworthy for processors is the fact that supervisory authorities may also have the power to impose bans on processing under the new regulation where serious breaches occur, effectively wiping out data centres who are non-compliant and others who have data processing activities at their core.

- **Technical and organisational measures**

Currently, all businesses above a certain threshold would be required to appoint a data protection officer (who must meet certain minimum



criteria to be appointed) under the new regulation. This officer will be responsible for compliance and will likely have strict notification requirements where breaches are identified, creating an administrative burden for all but the smallest of enterprises to whom this should not apply.

The regulation is also likely to require data processors to implement and maintain technical and organisational measures to keep the data they hold secure and to prevent unlawful, unauthorised or accidental processing. Whilst such obligations are likely to have been imposed on processors previously through contract, for the first time, this requirement is likely to be enforceable against processors by regulators themselves.

This scheme would encourage businesses to certify their processing with a supervisory authority. It is envisaged that if 'certified', this would potentially provide businesses with lawful grounds to transfer their data outside of Europe to that 'certified' business.

So what should we do?

Whatever the final rules will look like, the one thing for sure is that the new landscape is going to affect any businesses processing personal data. Such businesses cannot afford to stand still and need to react now to prepare themselves.

'Privacy by design' has been the mantra coming out of the EU for a while now. In order to keep enforcers at bay, processors should conduct a fresh audit that highlights awareness of the recent changes, further changes on the horizon and how they affect the company. In many cases, next steps will also include appointing/revising data privacy officers/teams, auditing how and where data is used, and importantly, what data is being transferred around the world and to where.

BCRs – a silver bullet?

Processor Binding Corporate Rules (BCRs) provide a relatively new avenue for data processors to obtain a competitive edge over rivals when bidding for contracts, and are increasingly becoming the preferred option to consider for those who both wish to demonstrate compliance now and who wish to prepare for the new regulation.

In essence, those processors who put in place Processor BCRs commit to certain data security and privacy standards relating to their processing activities. Once Processor BCR's are approved, they can then be used by that processor to demonstrate compliance with the EU data protection rules, without having to negotiate safeguards each and every time a contract is entered into. They are also invaluable in order for data controllers to obtain the necessary authorisation for transfers of their personal data outside of Europe.

Not only do Processor BCR's present themselves as an attractive option by reducing the costs businesses can incur when negotiating contracts relating to processing, they also have long term benefits in the sense that some upfront work, such as submitting an application, will undoubtedly position a processor in line for a privacy 'seal' once the regulation is introduced.

Key board agenda

To conclude, in short, data centres and other processors, wherever they are based, that deal with data in the EU, need to urgently revisit what they are doing, what procedures, policies, standards, documents they are using, and whether they are in fact as compliant as they think they are given the new landscape, and the further pending changes. The storm of new laws, fines and enforcement, with more coming shortly, should quite rightly fast track this to the top of board agendas, regardless of any perceived added cost concerns or admin burden in dealing with it. The false economy would be not to act, and assume no changes were needed.