LEGAL RISK LLP
SOLICITORS

www.legalrisk.co.uk | 0345 330 6791 | info@legalrisk.co.uk

GDPR:
6 months on—An update for US law firms

December 2018

In this Issue

The General Data Protection Regulation (GDPR) came into force across the European Union on May 25, 2018, and in the European Economic Area countries (EEA: Norway, Iceland and Liechtenstein) on July 20, 2018.

We review what has happened since then from the perspective of US law firms. We have advised 25 large US law firms, some international, others with only US offices but impacted because they are serving clients in the EU.

We have three webpages which will assist US law firms –

- **GDPR for US law firms - What do you need to do? www.legalrisk.co.uk/GDPRUSA**
- **Data protection - www.legalrisk.co.uk/Data**
- **News www.legalrisk.co.uk/News**

Links to all the documents mentioned below can be found on our Data and News pages.

While the intention of a European Regulation is generally to ensure consistency in all EU countries, there are several areas where GDPR permits member states to vary this through derogations. Our Data page has a link to a useful EU Member State GDPR Derogation Implementation Tracker.

Legal Risk LLP listed in The Times Best Law Firms 2019

Extra-territorial scope

Article 3 seeks to extend the scope beyond the EEA where firms offer services to, or monitor the behaviour of, data subjects *(i.e. living individuals)* in the Union.

The European Data Protection Board adopted guidelines on this provision 16 November 2018. These include a number of helpful examples.

Action under this provision so far has been limited. The UK Information Commissioner's Officer (ICO) served a formal notice on a Canadian analytics firm, AggregateIQ, which worked in the Brexit campaign; we understand this is under appeal.

The ICO has also issued a warning to The Washington Post over its approach to obtaining consent for cookies to access the service on the basis that as the newspaper has not offered a free alternative to accepting cookies, consent cannot be freely given and the newspaper is in breach of Article 7(4) of the GDPR. It seems unlikely that this will result in further action however. The ICO and the Federal Trade Commission signed a memorandum for mutual assistance in 2014; however, cookie consent is not subject to US privacy law.

Controller or processor?

We have advised many firms on the issue of Outside Counsel Guidelines which purport to decree that the firm is a (data) processor (which has significant downsides) rather than a controller. If there were any lingering doubt, the latest guidance from the ICO (updated December 2018), Contracts and liabilities between controllers and processors, and the new section in the ICO's Guide to the GDPR, What are 'controllers' and 'processors'?, should assist in resolving this.

Consent

GDPR is not all about consent. Consent must be explicit, and it is revocable. So although it has its uses as a lawful basis for processing, it will not be the first option in many cases. Firms which sought consent for marketing emails were disappointed by the level of response, so many have relied on legitimate interests, though that requires the firm to undertake a 'Legitimate Interests Assessment'. The ICO published guidance on Legitimate Interests in March 2018 and on Consent in May 2018.

Cross-border data transfers

Transfers of data from an EEA country to a 'third country' must satisfy the requirements of Chapter 5 of GDPR. Many firms rely on the EU Standard Contractual Clauses (the "Model Clauses"). The recent ICO £500,000 fine on the UK subsidiary of Equifax, following a data breach at the US parent company which affected £143 million people, contains some useful lessons, even though the relevant events predated GDPR; among the many criticisms of Equifax set out in the ICO monetary penalty notice, note that Equifax were unable to provide a signed copy of the data transfer agreement, and that the UK subsidiary had failed to audit their US parent. We know that the same criticism could be levelled against many international law firms.

The ICO updated its guidance on international data transfers in August 2018.

Article 28 stipulates several provisions which are required in contracts between controllers and processors. Where there is an international element involved, many organisations are using the Model Clauses. Note, however, that there are a number of areas where these do not meet the requirements of Article 28.

Brexit, with or without an agreed deal, will present challenges to compliance in managing dataflows from Europe to the UK and beyond. Firms will need to re-examine their arrangements over each link in the chain of data transfers and implement appropriate mechanisms. The wording of the draft withdrawal agreement is unclear: much will depend on whether the UK secures an adequacy decision during the Transition Period.

Links to several advice documents from HM Government, the Law Society and the Solicitors Regulation Authority (SRA) on data protection are on our Data page (see link above).

Anti-money laundering

Regulation 41 of The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 imposes requirements, with criminal sanctions for non-compliance, on training in data protection issues and the duration for which records are kept. The SRA are auditing firms for AML compliance: the SRA are themselves subject to audit by the Office for Professional Body Anti-Money Laundering Supervision (OPBAS), so this is an issue which is unlikely to go away. The Heathrow Airport monetary penalty notice highlighted the need for training.

In *Lonsdale v National Westminster Bank Plc* [2018] EWHC 1843 (QB), the High Court ordered a bank to disclose a suspicious activity report ("SAR") to a customer (who happened to be an English barrister), observing that SARs may amount to "personal data".

Data breaches

The ICO has received over 8,000 breach reports since GDPR came into force, making reporting mandatory in some high risk circumstances, according to a speech by the Information Commissioner, Elizabeth Denham, in New Zealand on 4 December 2018. The obligation to report within 72 hours has provided a significant challenge in many cases.

In practice, ICO statistics pre-GDPR show that the most common cause of breaches in the legal sector are email errors, followed by cyber incidents, data posted or faxed wrongly, and loss or theft of unencrypted data. So, while attention to technical issues such as anti-virus, firewalls and software patching is essential, are you addressing the largest single cause of data breach? There are measure which can be implemented to help address email error, software solutions using artificial intelligence, and applying a delay to outgoing emails.

The ICO published guidance on Security in April 2018, and on Passwords in online services and on Encryption in November 2018.

Cyber Crime and GDPR: the need for training

Many data losses result from cyber crime. We have developed a sequel to our popular online training course, Phishing for Trouble, used by many leading practices worldwide. The latest version PFT 2.2, like its predecessor, is designed with the typical user in mind, who often has only a hazy familiarity with phishing, vishing, twishing etc. It is designed to bring them up to date, using a relaxed question and answer format.

Common problems

A number of common issues with GDPR aspects continue to engage minds –

- Mergers and acquisitions involving businesses with a European presence: GDPR can influence due diligence work - as well the price;
- Foreign Corrupt Practices Act investigations;
- Immigration services;
- Legal professional privilege, which differs in extent and application from attorney-client privilege and work product doctrine;
- Subject Access Requests being used as a tool to obtain pre-action discovery in employment and partnership claims;
- Client requirements for diversity data and diverse representation.

The ICO issued updated guidance on exemptions, including legal professional privilege, in September 2018.

Note

This newsletter is a general guide. It is not a substitute for professional advice which takes account of your specific circumstances and any changes in the law and practice.

Subjects covered change constantly and develop.

No responsibility can be accepted by the firm or the author for any loss occasioned by any person acting or refraining from acting on the basis of this.