LEGAL RISK LLP
SOLICITORS

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

Issue No: 99

Risk Update • May 2021

We have audited many leading US and UK law firms for anti-money laundering compliance

In this Issue

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.

Anti-money laundering (AML), independent audits, and financial sanctions

AML developments continue apace, including updated Tax Adviser guidance from the Solicitors Regulation Authority (SRA), Part 2 of the Legal Sector Affinity Group (LSAG) Guidance (in three parts – for barristers and advocates, Trust and Company Service Providers, and notarial services), The Money Laundering and Terrorist Financing (Amendment) (High-Risk Countries) Regulations 2021, and Financial Services Act 2021 extending the application of the Proceeds of Crime Act 2002to electronic money, and to overseas trustees.

On a practical level, there can be no doubt that the SRA will be extending its programme of reviewing firms. Those firms which have concluded that they are not required to have an independent audit under Regulation 21 of The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 should keep a written record to justify to the SRA how and why they do not meet this requirement, considering how the firm will not benefit from the extra protections that these measures might provide. (See 9.1.)

The audit can be conducted internally if the firm has the requisite expertise outside its AML compliance and client and matter engagement team(s). Benefits of external audit may potentially include legally privileged advice on good practice in your peer group firms, benchmarking, identifying weaknesses before they become too embedded, and helping to keep up to date with the pace of change.

Financial sanctions have also been subject to numerous updates since our March 2021 issue, as the UK Government establishes a separate regime from independent of the European Union, including updated guidance from the Office of Financial Sanctions Implementation (OFSI) on monetary penalties for breaches of financial sanctions (effective 1 April 2021), OFSI Introduction to licensing, and The Global Anti-Corruption Sanctions Regulations 2021.

Note that there are differences between UK and EU sanctions, such as the application to parents and subsidiaries.

Links to the above documents can be found on www.legalrisk.co.uk/news and other AML resources on www.legalrisk.co.uk/AML.

Data Protection

The Information Commissioner's Office (ICO) will be consulting in the summer on UK Standard Contractual Clauses (SCCs) for international data transfers. It is not expected that these will be identical to the revised European SCCs, the final approved form of which is currently awaited. Given the position on the proposed European Commission adequacy decision in relation to the UK, it is unlikely that the UK version will be any less onerous to implement. It also means that contractual arrangements will remain in a state of flux for some time to come.

Bavaria's Supervisory Authority, BayLDA, applying the Schrems II decision, concluded that the email marketing service Mailchimp, which involved the transfer of email addresses by FOGS Magazin to the US, relying on the SCCs, was unlawful. BayLDA considered that Mailchimp could qualify as an 'electronic communication service provider' under US surveillance law, and consequently additional measures were required to ensure that the data transferred were protected from US surveillance.

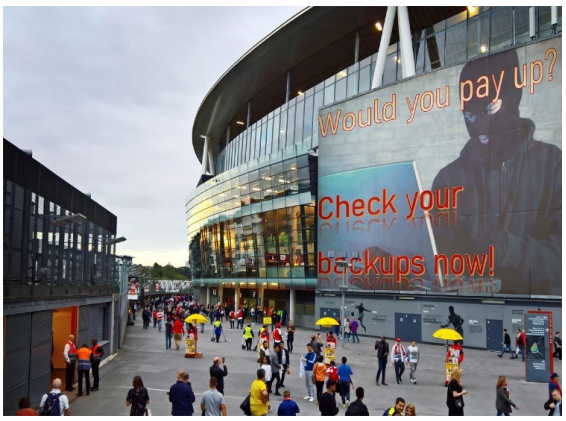
A European Parliamentary Research Service report on EU-UK private-sector data flows after Brexit analyses the proposed European Commission adequacy decisions under the GDPR and the Law Enforcement Directive, in particular criticisms which have been levelled at UK surveillance, the immigration exemption and the Digital Economy Act 2017, levels of enforcement by the UK Information Commissioner's Office, onward transfer of data; and the UK's level of commitment to EU data protection standards. A link can be found on www.legalrisk.co.uk/news and other data protection resources on www.legalrisk.co.uk/data.

See further below under *Cyber security.*

Cyber security

As we have noted in previous issues, law firms are a target for cyber attacks. Larger firms may for example hold valuable data in connection with intellectual property and mergers and acquisitions, as happened a decade ago in an attack on Canadian firms by Chinese-based computers, and smaller firms are no less exposed because they hold personal data, as shown by a recent example involving medical records for personal injury claims, which can be monetised through ransomware attacks.

A report by information security provider Sophos, *The State of Ransomware 2021*, addresses the prevalence and costs associated with ransomware. A link is on www.legalrisk.co.uk/news.



Ransom payments may be evidence of data protection non-compliance

Of the companies which paid up, whether for speed of recovery or inadequacy of backups, on average, only 65% of the encrypted data was restored after the ransom was paid. 4 per cent of victims who paid up received nothing in return, and only 8% claim to have recovered everything after submitting to the blackmail.

Perhaps the biggest risk identified in the report, however, is not the loss of confidential data but having it exposed on the internet. Payment of ransomware to decrypt data may not be the end of the matter: a second payment may be demanded to prevent the release of data.

Cyber security was addressed at the ICO's Data Protection Practitioners' Conference 2021 on 5 May 2021. In the last 12 months the ICO opened investigations into 1700 data controllers; there was a monthly average of 42 incidents, up from 13.4 in previous year. Guidance is expected shortly on ransomware and incident response, covering notification, and demonstrating compliance in the event of a successful attack.

Firms should have the support provided by cyber insurers. Advice and details of private sector support may also be found on the National Cyber Security Centre website.

The ICO have a cyber investigations department and will want to know what personal data were held on which servers, recovery time objectives, whether intruders are still present in the system, interim systems which are being deployed and the policies and procedures in place to mitigate the risks associated with them (such as staff using gmail or similar personal accounts).

Risks include erasure and encryption of backups; even temporary unavailability for a few hours may amount to a personal data breach, though it may not be necessary to report to the ICO if there is no threat to the rights and freedoms of individuals (but it will still be necessary to consider reporting to the SRA). Paying a ransom fee may prompt questions as to whether backups were segregated from the live environment so as to prevent access. It is not currently an offence in the UK to pay a ransom unless it involves terrorist funding or financial sanctions. Criminalising payments would raise difficult questions—criminalising victims, focusing investigations on victims rather than perpetrators, and discouraging reporting.

See also the next section on insurance.

Professional indemnity insurance: cyber exclusion

The SRA is consulting on a cyber exclusion clause to be added to the Minimum Terms and Conditions of PII. Their intention is to preserve the status quo, providing cover for claims by clients and third parties but excluding indemnity for the firm's own losses. We believe it substantially achieves that objective, though we have identified some drafting points. It will need the support of insurers. See link on www.legalrisk.co.uk/News.

Events

Frank Maher will be speaking on cross-border conflicts of interest at a joint online event hosted by The Law Society and the US Association of Professional Responsibility Lawyers (APRL), *Transatlantic legal ethics 2021: law firm regulation and legal ethics in a post-Brexit world*, 25-26 May 2021.

He will also be delivering an online session on *Anatomy of a crisis: a case study with self-reporting issues*, covering cyber fraud, reporting obligations, common regulatory breaches, insurance issues, and traps for the unwary. This forms part of the *2021 Compliance Conference* hosted by Liverpool Law Society.

See www.legalrisk.co.uk/events.