LEGAL RISK LLP
SOLICITORS

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

Risk Update • March 2019

Issue No: 86

In this Issue

- Anti-Money Laundering
- Confidentiality
- SRA Standards and Regulations
- Cyber
- Data Protection
- Conflicts of Interest

Anti-Money Laundering

As predicted in previous issues of Risk Update, the Solicitors Regulation Authority (SRA) is ramping up its action with a press release announcing that it 'will be carrying out rigorous checks on law firms to make sure they are meeting their anti-money laundering obligations' and 'will shortly be writing to an initial sample of 400 firms asking them to demonstrate compliance with the Government's 2017 Money Laundering Regulations'. We understand that the SRA is also asking larger firms whether they have had an independent audit under Regulation 21 of The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLR 2017).

Note the link into the next topic, data protection, as Regulation 24 requires training in the data protection aspects of anti-money laundering and record keeping. Regulation 41 prescribes information to be provided to clients before engagement.

Terms of business need to cover the possibility that banks providing pooled client accounts may require information on clients, including those for whom the firm's services are outside the regulated sector. Although we are not aware of any banks yet asking for such information, the issue of pooled accounts is currently part of a wider review of guidance by the Joint Money Laundering Steering Group.

Estate agents have been hit with unannounced inspections by HMRC as part of a crackdown on money laundering in the property industry, and HMRC have published details of several businesses for failing to comply with the MLR 2017. Countrywide Estate Agents was fined £215,000 for failing to ensure policies, controls and procedures at group level; and for failures in conducting due diligence; timing of verification and proper record keeping. Another company was fined £68,595 for failures in carrying out risk assessments; having the correct policies, controls and procedures and customer due diligence.

There have been several publications since our last issue, including the Treasury Select Committee Inquiry report on *Anti-money laundering supervision and sanctions implementations* and a FATF consultation on *Draft Risk-Based Approach Guidance for Legal Professionals, Accountants and Trust and Company Service Providers.*

We have advised many leading law firms and property professionals on risk assessments, policies, controls and procedures, and independent audit. Links to the above documents are on www.legalrisk.co.uk/news.

Confidentiality

We are often instructed to advise firms how they can properly proceed when they have been offered client files 'for sale' by firms which are closing, or in many cases, administrators on their behalf, much as they might sell the stock of a corner shop; in so doing, they have scant regard for the solicitor-client relationship, their duties of confidentiality and data protection obligations – to say nothing of the fact that the major part of each file belongs to the client, not the law firm, which has no title to sell.

Our concerns have been confirmed (if there were ever any doubt): transferring files without consent was an issue in the Solicitors Disciplinary Tribunal judgment on an agreed outcome in *Majid* 1189-2018 which led to a six month suspension and substantial costs. This follows last year's £40,000 fine plus £26,000 costs by the SRA on a different practice for inspecting confidential files of another firm without the knowledge or consent of the relevant clients.

SRA Standards and Regulations

The new SRA Standards and Regulations, replacing the current SRA Code of Conduct and other parts of the SRA Handbook, will come into force on 26 November 2019. We commented on this in our November 2018 issue. (See https://www.legalrisk.co.uk/publications/)

The SRA has promised guidance. The problem with guidance is that we know from past experience when changes were introduced in 2009, that it is too easy for the SRA to rely on it in relation to alleged breaches which predate it, by saying that it only reflects what has always been the case.

Meanwhile, the SRA has published an updated enforcement strategy which aims to provide greater clarity about how and when they will take action. (See www.legalrisk.co.uk/news.)

The Cube, Birmingham

Cyber

Much of the debate about cyber insurance has been over whether cover for fines under the General Data Protection Regulation (GDPR) is excluded on public policy grounds. This is a side issue. A far greater concern is the impact on the business and its clients, as evidenced by last year's Financial Conduct Authority £16.4 m fine on Tesco Personal Finance plc (Tesco Bank) for failing to exercise due skill, care and diligence in protecting its personal current account holders against a cyber attack.

Two ongoing claims against insurers cause concern about whether insurers will pay out on cyber policies in the event of a claim. We defer detailed comment as the cases are still pending, save that one issue, in at least one of these cases, appears to be whether a cyber attack attributed to hostile nation state activity falls within an exclusion for 'act of war'.

We appreciate that insurance insurers should only have to pay out for the cover they have agreed, and been paid, to provide, and this is particularly so where an insured may be trying to shoehorn a cyber claim into a policy which was not intended to provide cyber cover.

However, if there is to be widespread take up of cyber insurance, and it is in the public interest that there should be, so as to enlarge the pool from which claims can be paid, we need to see reports of cyber insurers paying out on claims and the businesses they have saved. At present, those reports are few and far between.

Data Protection

The European Data Protection Board have published Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities.

The Advocate General of the Court of Justice of the European Union has issued an Opinion on cookie consent. In addition to opining, unsurprisingly, that pre-ticked boxes were inadequate for obtaining consent, the Advocate General declared that information should be provided on the duration of the cookies, whether third parties are given access to cookies, and, if so, the identity of the third parties. See *Planet49 GmbH v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V*.

HM Government has published guidance, *Using personal data after Brexit.* A Californian court has ordered discovery of documents despite a GDPR based objection: see *Finjan, Inc. v. Zscaler, Inc*.

Links to the above documents are on www.legalrisk.co.uk/news.

Finally on this topic, The Times reported on 26 March 2019 that 2,940 data security incidents were logged by the Ministry of Justice last year. Litigation practitioners may care to spare a thought before including excessive copies of medical and employment records in multiple court bundles: who knows what becomes of them?

Conflicts of Interest

Client-imposed terms through outside counsel guidelines are an ever-growing concern, particularly as they may widen the scope of individuals and entities against whom the firm agrees not to act. The risk is enhanced because terms may be imposed through the 'back door' through e-billing arrangements which lead to accounts staff inadvertently accepting changed terms of business.

The case of *Falk Pharma GMBH v. Generico, LLC* 2019 WL 692670 (Fed. Cir. Feb. 20, 2019) demonstrates that the risk is not purely theoretical. The court disqualified lawyers from acting against a client's 'affiliates'. However, given that the company in question was a subsidiary of the client with which it shared a legal department, the result is perhaps not too surprising.
See www.legalrisk.co.uk/conflicts.