Panama Papers – A practice note on how to deal with data breaches

What compliance issues might organisations be facing following large data leaks and breaches such as the Panama Papers, and how can they protect themselves against such breaches? **André Bywater, Principal Adviser - European Regulatory at Cordery**, outlines the issues to consider.

What is the Panamanian breach about?

It is still not clear what the source of the breach is, i.e. who might be behind this and how the documents got into the public domain. What is known is that the materials from the Panamanian law firm came into the possession of the German newspaper, *Süddeutsche Zeitung,* which then shared the information with the investigative journalist community. News continues to emerge about what is in the information but of immediate great significance is that this issue goes to the top as the documents show links to some 75 current or former heads of state. It seems that the leak reveals the beneficial owners behind companies set up by the law firm for their clients. As is well-known, companies, especially in so-called 'offshore' jurisdictions can be used to disguise the true ownership of assets and bank accounts. These companies go under various names, notably 'front' companies or 'shelf' companies, or, 'shell' companies and these companies appear to feature prominently in the leaked documents. More than 214,000 offshore entities appear in the leak, connected to people in more than 200 countries and territories. It should be stated that using a front company does not (usually) of itself amount to criminal conduct, and, Mossack Fonseca denies any wrongdoing on its part.

Just how significant is this and what happens next?

We see this as an extremely significant global event which, in data breach terms, may even eclipse the Snowden NSA leaks in breadth as many individuals will be personally affected, including very prominent people. Already authorities in various countries are reporting that they have begun investigations into various individuals, especially in the field of tax. Information in the documents also appears to include data connected to at least one ongoing corruption and money-laundering case in the UK. This story can be expected to run for some time especially as further details of those allegedly involved are scheduled to be released next month including emails, financial spreadsheets, passports and corporate records from 21 offshore jurisdictions. Apparently 2.6 terabytes of data going back almost 40 years will be released. As can be imagined, this is going to keep a lot of people busy, including lawyers.

What kinds of areas of legal compliance might be affected and what should organisations be doing?

Most immediately we see the following compliance areas as being affected—bribery, sanctions, and, money-laundering/politically exposed persons (PEPs). As you may know the UK Bribery Act 2010, which came into force in 2011, introduced a new offence of failure to prevent bribery under which a company can be liable for the acts of an individual or company 'associated' with it. Many organisations will have done due diligence based on the apparent owners of companies they associate with—they may have also taken legal advice on the information yielded. It is likely that in light of the Panamanian leak that there may be doubts as to whether those apparent owners are the beneficial owners of a given entity. Front companies can and have been used in bribery schemes, as has been seen in the recent UK cases concerning Standard Bank and Graham Marchant. In light of the Panamanian leak, organisations should renew their 'associated persons' due diligence. As you will be aware there are various sanctions schemes imposed (such as by the EU) on certain countries and/or individuals and organisations in those countries—notable countries concerned include Iran, Zimbabwe and Russia. The Panamanian leak has exposed a number of individuals, including for example some prominent Russians, and it may be that some of these individuals have masked their connection to sanctions by using front companies. Once again, we stress that organisations should consider renewed and/or more rigorous due diligence, for example where transactions are envisaged in areas of the world where sanctions have been imposed. Anti-money laundering legislation is prevalent throughout the world and a key feature is that it invariably requires due diligence when parties, such as lawyers, process taking on new clients of course. Further, many jurisdictions also have legislation requiring what might generally be called an exercise of caution when officially dealing with PEPs, which lawyers are usually also required to respect. Once more, it may be that companies are used as a mask for money-laundering and/or to disguise the fact that the real owner is a politician, and so once more consideration should be given by law firms and institutions such as banks to doing fresh due diligence where appropriate.

What should organisations do if they think they might be affected by the Panamanian leak?

Most organisations will need to act fast in order to reduce their exposure. In addition to carrying out the above-mentioned due diligence, if there are particular concerns it may be that an internal investigation needs to be undertaken, possibly by external lawyers and auditors, for which proper procedures will have to be set up. Careful thought will have to be given as to how to handle particular information with regard to data protection legislation. The issue of professional legal privilege will also likely need to be addressed. Such a review should be forward-looking in light of the fact that further information is going to be released.

How can organisations protect themselves against data breaches such as the Panamanian one?

There are three main issues we think should be addressed. The first thing is to have clear, accessible (in easy-to-read language) and engaging policies in place for your employees about how to prevent data breaches. Next, ensure that your technology is up to the job of protecting data and enabling you to know that a breach has occurred. Finally, train people on how to prevent breaches, with more in-depth training for personnel who may be exposed to more risky scenarios. Unfortunately, these days it is more likely a question of when a breach might occur and not if a breach may occur, and so you might also consider setting up a breach team who should rehearse breach scenarios.

And what should organisations do if they actually have a data breach?

If an organisation has a security breach, the following steps could be taken in order to manage the situation as best as possible. First, undertake an investigation as to why the breach took place, and, the nature of the breach. Second, stop and/or mitigate the breach—having understood the breach and its cause, the organisation can then act to mitigate the effects of the breach and prevent the breach from continuing and/or recurring. Such action may involve a combination of notification, contractual, disciplinary and procedural steps. Third, the organisation will have to consider who should be notified of the breach. In this regard, looking to the future, under the new EU Data Protection Regulation (awaiting finalisation and expected to be fully applicable in just over two years' time) there will be mandatory data breach reporting to data protection regulators which will have to be undertaken within 72 hours of the breach (and the breach will also have to be communicated to those directly affected by it). An organisation should also check its insurance, not least because the insurers will likely have to be notified of a breach.

For more on the Panama Papers, watch André Bywater talk about sanctions, bribery and anti-money laundering among other things in this LexisNexis video.

André Bywater is a commercial lawyer with a focus on regulatory compliance, processes and investigations. His practice has engaged both the private and public sectors. He was Brussels-based for many years focusing on a multitude of EU issues during which time he worked across Europe and beyond. He has assisted and advised mainly European and US in-house counsel and other company personnel. Further, he has also addressed a variety of legal matters in the context of EU-funded projects building the expertise and capacity of government ministries and agencies in Central and Eastern Europe and further afield.

Interviewed by Yacine von Welczeck.

The views expressed by our Legal Analysis interviewees are not necessarily those of the proprietor.