insuranceday
www.insuranceday.com

Insurers are on an uncertain footing with new EU's data regime

New European anti-money laundering rules are also set to challenge insurers

Thomas Webb and David Varney
Burges Salmon

European Commission: the incoming General Date Protection Regulation and Fourth Anti-Money Laundering Directive will bring challenges for insurers

Two key EU directives are set to have an impact on insurers: the new General Data Protection Regulation (GDPR) and the Fourth Money Laundering Directive (FAML).

The EU's data protection regime is in a state of flux at present, with changes occurring on an almost monthly basis, leaving multinational insurers and insurers that export data from the EU on uncertain footing. Meanwhile, the new anti-money laundering directive will modify and extend customer due diligence requirements, reinforcing the "risk-based" approach to money laundering risks.

The GDPR will replace the existing EU Data Protection Directive and contains several significant changes for businesses that control and process the personal data of European citizens. It will take effect in member states from May 25, 2018 and will apply whenever EU residents' personal data is processed in connection with the offer of goods or services or the monitoring of behaviour (such as the analysis of consumers' preferences) within the EU. In a change from existing practice, the new data protection regulation will apply even where the processing organisation has no physical presence in the EU.

At present, organisations are subject to review and enforcement action by the data protection authority in each member state in which it operates. In contrast, under the GDPR, multinational organisations will have one lead supervisory authority located in the member state in which it has its main establishment.

Separately, the Court of Justice for the EU (CJEU) has had its own impact on global data protection. In October 2015, in *Schrems*, the CJEU declared the EU/US "safe harbour" regime to be invalid, effectively removing one of the grounds for ensuring data protection compliance when organisations transfer personal data from the EU to the US. Safe harbour was relied on by more than 4,000 organisations as a means to self-certify compliance with EU data protection law.

Following *Schrems*, the US government and European Commission held urgent political negotiations to seek to re-establish a new EU-wide blanket authorisation for transfers of personal data across the Atlantic, widely regarded as being "safe harbour 2.0".

In February, the commission announced the agreement of a new framework for the flow of personal data across the Atlantic, which was branded the "EU/US privacy shield". Since then, the privacy shield has been reviewed by the Article 29 Working Party (WP29), a pan-European independent advisory body, which, while acknowledging the "significant improvements" offered by the new framework, concluded it does not reflect key data protection principles. The commission is amending the original privacy shield proposals to address WP29's recommendations.

In the meantime, WP29 recommends organisations transferring personal data to the US should incorporate the EU's model data protection clauses into the contracts governing those transfers or, in respect of intra-group transfers of data, seek to establish binding corporate rules that safeguard data subjects' rights.

While this remains the approach generally accepted during this period of uncertainty, the Irish Data Protection Authority has recently stated that it intends to refer to the CJEU the question of the validity of the model clauses under the Data Protection Directive. A finding that the model clauses do not confer "adequate protection" would remove one of the few routes still available to organisations seeking to legitimise transfers of data to the US.

Confusion

The situation is undoubtedly confused and some authorities are expressing concern that the EU is entering into an era of data isolationism. Consumer confidence in the transatlantic flow of data remains an area of commercial concern for businesses and may reduce data transfers from EU to US entities. For now, the use of model clauses is still good practice, but organisations should remain alert to this area of regulation and keep an eye out for further changes in guidance.

Like GDPR, the FAML, which must be transposed into legislation by member states by June 26, 2017, seeks to further extend regulation for businesses. In particular: customer due diligence is now required on cash transactions of more than €10,000 ($11,400) – the current trigger point is €15,000; providers of gambling services must carry out due diligence on customers placing a stake or collecting winnings of €2,000+; and the definition of politically-exposed persons (PEPs), for whom enhanced due diligence is required, is now wider, catching domestic individuals with high level appointments in the UK, foreign PEPs and senior officials in international organisations.

Further, simplified customer due diligence will no longer be automatically applicable for certain types of customers and regulated firms will only be allowed to use simplified due diligence where the category of work has been identified as of low money laundering risk and the transaction itself is considered low risk.

The directive sets out a non-exhaustive list of factors which must be taken into account when determining risk levels, including customer risk factors (eg, dealing with a public company listed on a stock exchange and subject to disclosure requirements); product, service, transaction or delivery channel risk factors (eg, products where the risks of money laundering and terrorist financing are managed by other factors such as purse limits or transparency of ownership), as well as geographical risk factors (eg, non-EU countries with different standard anti-money laundering systems).

Additional risk assessment guidelines will be issued by the European supervisory authorities by June 26, 2017.

Further protections are enshrined in the requirement on member states to maintain a central register containing key information (names, dates of birth, nationality, country of residence and the nature and extent of interests) about the beneficial owners of businesses. While the UK already requires certain companies to keep limited information on such registers, this requirement for an accessible register of beneficial ownership is a potentially significant extension of that regime and is likely to provide a useful source of information for businesses carrying out due diligence on their customers.

The registers will be accessible to "authorities", "obliged entities" (eg, banks carrying out due diligence on customers) and "others". These "others" will include anyone who can demonstrate a "legitimate interest" in gaining access to the information.

Finally, where firms have a branch or majority-owned subsidiary outside the EU and the anti-money laundering (AML) laws in that country are less strict than in the EU, the firm will still be required to apply the higher standard of EU AML rules in that third country.

It is apparent that FAML provides further evidence of the shift in regulatory philosophy towards "risk-based" compliance. This means that all businesses, including insurers, will need to actively think about what money laundering risks they face and how those risks can be managed. ■

Thomas Webb is legal director and David Varney an associate at Burges Salmon