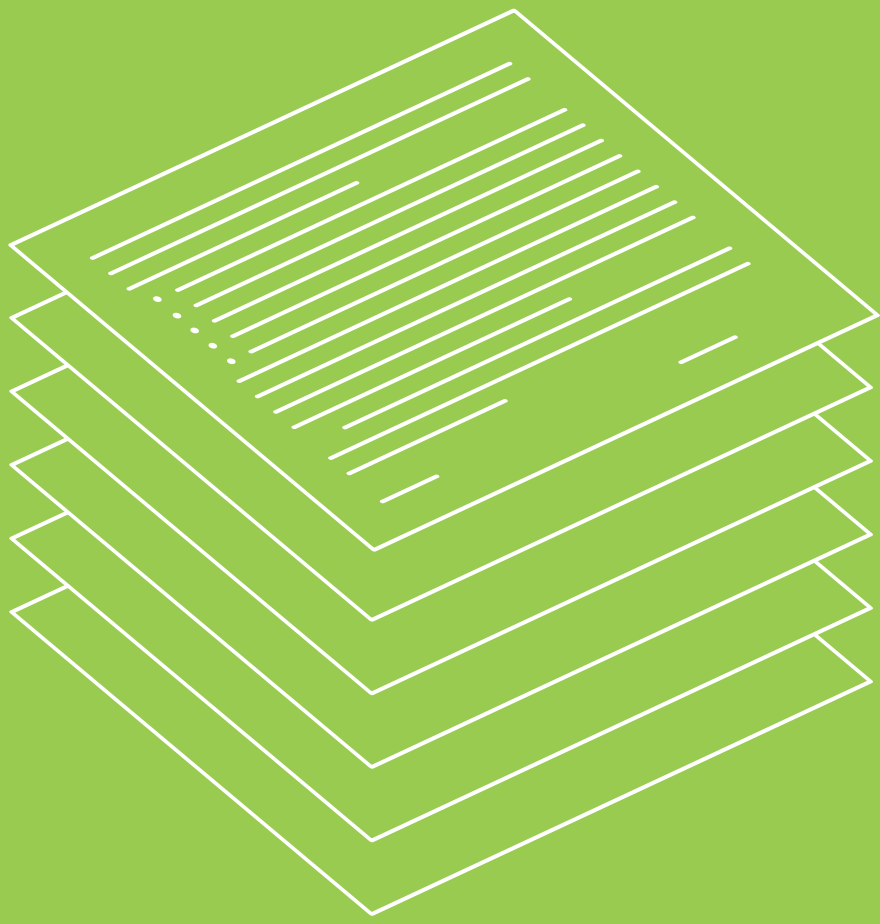
LEGAL CORNER

2018 BRINGS NEW CHALLENGES



Data Protection

On 27 April 2016, the European Parliament and European Council approved the General Data Protection Regulation. This revokes Directive 95/46/EC and comes into force on 25 May 2018.

Such is the territorial scope of the new Regulation, that some data controllers and subcontractors based outside the EU whose processing activities relate to offering goods or services (even free of charge), will need to appoint a representative within the EU. Another substantial change, among others, is for subcontractors to maintain a physical register of each data controllers' activities, and appoint if necessary, a data protection officer or notify the data controller immediately upon detecting a personal data breach.

A breach of personal data should also, whenever possible, be reported to the regulatory authority within 72 hours of becoming aware of it. In the event of the breach affecting personal security or privacy, the data subjects must be notified immediately by the data controller.

In order to safeguard personal data access and transparency, the new Regulation aims to extend the rights of the data subjects and enhance their legal status. This includes a 'right to oblivion' on the part of the data subject and a requirement for each user to consent to the processing of personal data (which will have to be explicit when it comes to sensitive data, clearly identifying the specific purpose intended). These guidelines are more stringent than what has been in force up until now.

Although the new Regulation is an important step towards personal data protection, it brings an increased administrative burden for data controllers, subcontractors and the regulatory authorities. According to a report presented by Verizon, in 2016 there were about 1,935 security breaches in 82 countries. Given data controllers and the supervisory authorities must comply with the deadlines for notifying breaches, it is expected that most reports will be brief in detail. The person in charge will most likely seek to demonstrate – to the satisfaction of the regulatory authority – that adequate security measures were implemented and they were in use at the time of the breach in question. The effects of this administrative burden therefore, are likely to extend to all involved parties and those showing a lack of effective measures may incur additional costs. Regulatory fines are heavy – a maximum of 20 million euro or, in case of a multinational company, four per cent of worldwide turnover.

With the post-Brexit deadline approaching, the Queen's speech of last June revealed the United Kingdom's intention to include the new Regulation within its internal legal framework (whose rules will continue to be in force after its withdrawal from the EU). This move puts more emphasis on London receiving information than supplying it, because in anticipation of its treatment as a non-EU country, the Government intends to create a high-quality system for personal data protection.

Cyber risk insurance with cover for third parties is one mechanism to compensate for and mitigate losses associated with data breaches. Policies available on the market support the client with services that offer advice and help prevent technological failures. In a broader perspective, this new Regulation reflects the European legislator's commitment to cyber security.

Changes in Distribution

Also in 2018 is the new (EU) 2016/97 Insurance Distribution Directive (IDD), which replaces Directive 2002/92/EC, combats the fragmentation of the European insurance market and promotes trade between Member States. And as did the former Directive, it also applies to the distribution of reinsurance.

On 21 September 2017, an additional regulation to complement the IDD was also approved. Following the commission's proposal to postpone the IDD's effects until October 2018, this regulation will be in force from 1 October 2018, it aims to 'specify the criteria and practical arrangements for rules concerning conflicts of interest, incentives and the assessment of suitability and appropriateness'.

When it comes to market behaviour, the guiding principle will be 'know your consumer', particularly when it comes to price discrimination and cross-selling. In order to ensure the product is right for the consumer, the intermediary must inform the client of its specifications and while noting a specific interest, the opportunity to acquire it elsewhere. This type of sale with personalised or tailor--made advice is not often promoted by agents; it is however given by brokers who have a greater influence and can impose conditions on the insurance company. The role of an exclusive agent is to focus on offering advice and product/benefit information.

The suitability of products for different types of customers is dependent upon their needs and the policies' complexities, but there is an expectation that the target market for more simplistic products will expand with a greater emphasis on identifying potential customers. The real focus of the IDD however, is to put the contracting decision and communication flow into the hands of consumers. •

Paulo Almeida

Paulo has extensive experience in advising insurance and reinsurance companies on policy provision and developing/revising products for various lines of business, particularly in the financial chapter. Areas of focus include; professional civil liability, directors and officers, plus commercial and corporate law, including banking litigation.

He was a lawyer at Lisbon City Council, partner of Almeida & Athayde, and is currently a managing partner of Kennedys Portugal. Paulo is a member of the International Bar Association, the Portuguese Sector of the International Association for Insurance Law and the Federation of Defense & Corporate Counsel.

He was admitted to the Portuguese Bar Association in 1989 and speaks Portuguese, English and Spanish.