Association of British Insurers One America Square, 17 Crosswall, London EC3N 2LB Tel: 020 7600 3333 Fax: 020 7696 8999

GDPR KEY IMPLEMENTATION CONCERNS - JULY 2016

ISSUE 1: PROCESSING OF PERSONAL DATA RELATING TO CRIMINAL CONVICTIONS AND OFFENCES (Article 10)

There is a risk that the Regulation will no longer allow insurers to process conviction data, which will affect insurers' ability to:

- Underwrite risk accurately.
- Verify claims.
- Maintain internal fraud registers.
- Vet their employees, to the standard required by other regulations.

We consider the above risk, if realised, to be material to the underwriting performance of ABI members.

Insurers rely on data to accurately assess risk and provide individuals and businesses with cover that meets customers' needs for a vast range of risks and eventualities. Data is also key for insurers to continue to be able to prevent and detect fraud. In 2014, the ABI estimates insurers detected over 130,000 fraudulent general insurance claims, worth £1.3bn. These frauds could only have been detected using sophisticated data analysis, which combines thousands of individual cases of fraud to detect patterns and trends on a large scale, and therefore enable an accurate identification of crimes.

If the implementation of the GDPR prevents insurers from using conviction data, it will play into the hands of would-be fraudsters and increase the average cost of insurance premiums to all law-abiding customers. The safety of wider society would also be compromised; for example, fraudulent activity is often linked to dangerous activity, e.g. "crash for cash", and a higher level of uninsured driving, which statistically result in a greater number of accidents.

The ABI is seeking that the DCMS modifies the existing legislative framework in a way that enables insurers to continue to process information relating to criminal convictions and offences for the purposes of underwriting, fraud detection and prevention. We are seeking that the implementation of the GDPR strengthens, not hinders, insurers' ability to assess risk, detect and prevent fraud. We believe there may be opportunity for the UK Government to invoke the "legitimate interests" or "public interest" considerations that the GDPR appears to allow member states to apply. We are also seeking clarity regarding the definition of "official authority" including the criteria that would need to be fulfilled to be classed as such.

ISSUE 2: CONSENT FOR THIRD PARTIES (Article 6: Lawfulness of processing)

The requirement for the data subject to give consent to the processing of their personal data for one or more specific purposes (Article 6 (1) a) is strengthened by the Regulation. It is a key concern for insurers that provide cover that can currently be extended to cover third parties without the need to obtain third party consent.

We are seeking to work with the DCMS to ensure that the implementation of the GDPR continues to enable quick and easy third party insurance, and that the administrative and compliance processes required will be both practical and cost-efficient.

We are also seeking clarity regarding:

- the extent to which insurers must obtain consent from third parties with which the insurer does not currently have a direct relationship, e.g. third party motor insurance, family travel insurance, Group insurance provision e.g. health, income protection and pensions
- GDPR-compliant ways for insurers to demonstrate that they have achieved consent.
- the extent to which the grounds of public interest and vital interests of the data subjects, as described in Recital 46, can be invoked so that third parties can continue to be insured against a range of risks to themselves and wider society
- the extent to which the responsibility for the data provided, including those of the named third parties within the insurance contract lies with the data subject rather than the data controller.

ISSUE 3: AUTOMATED INDIVIDUAL DECISION-MAKING, INCLUDING PROFILING (Articles 4, 22 and 9)

The Regulation introduces new rules for 'profiling'. As the underwriting process involves systematic profiling of individuals so that they can understand the level of risk posed by an individual before entering into a contract, there is a risk that this could affect insurers' ability to underwrite. The ABI is seeking clarity regarding:

- which data will remain permissible for underwriting purposes (as it can be considered necessary for a contract) (Article 22.2(a)) and which requires consent.
- whether data provided to anti-fraud databases can typically be processed under 'legitimate interests'.
- the extent to which profiling for marketing purposes will always require explicit consent.
- The impacts of the Regulation for automatic renewals and policies that were incepted before the start of the Regulation coming into force.

As stated in the Government's response to the Science and Technology Commons Select Committee's fourth report of session: "The big data dilemma", paragraph 22: "… more needs to be done to unlock the power of data". The ABI is seeking that insurers can continue to use the power of data, innovate and build on its centuries of experience in underwriting risks within today's new era of digital technology, to manage and minimise the risk of loss to society.

ISSUE 4: RIGHT OF DATA PORTABILITY (Article 20)

Many insurers and intermediaries hold personal data on different systems (e.g. underwriting and claims systems). Insurers are seeking clarity about:

- the definition of machine readable format. For example would 'machine readable' include paper format, or should it be interpreted as including only electronic formats.
- which data will need to be ported and therefore accessed and combined into a structured, commonly used and machine readable format. For example, is it only the data that the individual has actively provided at the start of the contract, or any

data captured as part of the contract or to inform the terms of the contract, e.g. via wearable technologies such as fitbits for health insurance, telematics for motor insurance and connected devices for home insurance.

- whether this requirement relates to third parties, e.g. reinsurers or insurance intermediaries, that hold data on an insured customer, but do not have any interface with the insured customer.
- approved methods by which they may provide such data to customers and other companies on request (e.g. email or portal).

ISSUE 5: FAIR PROCESSING NOTICES (Recitals 39, 42, 45, 58, Articles 7 & 12)

It will be hard to engage customers with the new Fair Processing Notice. Customer feedback received by ABI member firms indicates that customers prefer to progress through the customer journey via a number of stages and not be presented with all the information at once. We support the ICO's proposal in its recent consultation on privacy notices, to develop an example of a layered privacy policy, for online and mobile. The ABI would be keen to work with the ICO to ensure that privacy notices can be provided to customers in an engaging, concise, informative and helpful way. Insurers are seeking a regulatory framework that:

- supports the ability to provide information that builds up in layers.
- allows the use of electronic communications and a "point to the website" approach.
- is built on a proportionate approach to consumer disclosures to ensure communications are not overwhelming in length or volume.

Insurers are also seeking clarity as to whether the requirement will relate to all data subjects or only new contracts once the GDPR is in force in 2018. This question is of particular relevance to long-term contracts including life insurance and pensions. We are also seeking clarity as to whether fair processing notices will now need to be sent to individuals covered as a third party via insurance contracts, as these third parties currently have no direct relationship with the insurer.

ISSUE 6: INTERPRETATION OF LANGUAGE WITHIN THE GDPR TEXT

Insurers are seeking clarity on a number of language points within the GDPR text. Some terms are qualified with varying levels of degree, others are similar and firms would like clarity to understand the differences or nuances between each term so they can develop systems and procedures that will comply with the GDPR. The following terms have been highlighted as needing clarity:

- Public/significant/legitimate/important interest
- Significant effect/legal effect
- Ordinary/explicit consent
- Risk/high risk

The ABI is seeking to work with the DCMS and ICO to develop an approved glossary of terms or similar, to help insurers communicate with clear, consistent language relating to data protection throughout the customer journey and across the industry.