Association of British Insurers 51 Gresham Street, London EC2V 7HQ Tel: 020 7600 3333 Fax: 020 7696 8999

Article 29 Working Party Opinion 06/2014 on the notion of legitimate interest of the data controller

The ABI is the voice of UK insurance, representing the general insurance, protection, investment and long-term savings industry. It was formed in 1985 to represent the whole of the industry and today has over 300 members, accounting for some 90% of premiums in the UK.

The ABI's registration number on the European Commission's Register of Interest Representatives is **730137075-36.**

Introduction

The processing of data is a key consideration for the insurance industry. Insurers recognise the importance of data privacy and take their responsibility for data protection seriously. Insurers need the ability to access, process and store data in order to provide consumers with the right products at the right price. Using the data enables insurers to determine the level of cover needed and to then set an appropriate premium tailored to that customer. The insurance industry, and the consumers it serves, would be negatively impacted if the insurers' ability to use the data effectively for these purposes would be restricted.

In this context, the insurance industry welcomes the Article 29 Working Party Opinion 06/2014 on the notion of legitimate interest of the data controller under Article 7 of Directive 95/46/EC, especially in the context of on-going discussions on this topic in relation to the draft EU General Data Protection Regulation.

Ensuing legal certainty

In order to ensure that the insurance market is able to continue to provide adequate, appropriate and affordable products to its customers, it is of paramount importance that insurers can continue to access, process, share and store data for the purposes of fraud prevention and detection. In order to achieve maximum legal certainty for this, we believe that:

1. Article 6 paragraph 1 of the draft EU General Data Protection Regulation should clearly state that the processing of personal data shall be lawful if the processing is necessary for the prevention and detection of fraud
2. The draft EU General Data Protection Regulation should also explicitly state that the notion of legitimate interests includes the prevention and detection of fraud. We agree that there should be a non-exhaustive list of legitimate interests, that only some examples should be provided, and that the processing and sharing of data in order to prevent or detect fraud should be listed as one of these examples.
3. The draft EU General Data Protection Regulation should recognise both legal and regulatory obligations to which data controllers are subject.

Processing of data for fraud purposes

In 2013, UK general insurers detected 118,500 cases of fraud with a value of £1.3 billion. In addition, we estimate that over £2 billion in insurance fraud goes undetected each year, adding, on average, an extra £50 a year to the insurance bill paid by each UK household.

Therefore, for insurers, reducing and deterring insurance fraud is a priority for the insurance industry. This not only protects their business but also protects honest consumers. Firstly,

the controller benefits from containing its costs and the sustainability of its business. Secondly, society benefits because being able to control fraud enables insurers to keep premiums down. As acknowledged in the Article 29 Working Party Opinion, combatting financial fraud or other fraudulent use of services is in the public interest. This should be recognised in the draft EU General Data Protection Regulation.

Therefore, as mentioned above, Article 6 paragraph 1 of the draft EU General Data Protection Regulation should clearly state that the processing of personal data shall be lawful if the processing is necessary for the prevention and detection of fraud. Furthermore, the draft EU General Data Protection Regulation should also explicitly state that the notion of legitimate interests includes the prevention and detection of fraud.

Complying with legal and regulatory obligations

The Opinion acknowledges the importance of regulatory obligations, but seems to imply that these are ‚less mandatory' compared to legislative obligations. This is not the case. If a regulator issues a regulatory obligation on the data controller, that data controller has a legal obligation to fully comply with that regulatory obligation.

For example, in the UK, insuers will have to comply with many regulatory requirements such as those issued by the Financial Conduct Authority (for instance, Treating Customers Fairly[1], FCA Handbook which includes, for example, record keeping requirements).

Therefore, the draft EU General Data Protection Regulation should recognise both legal and regulatory obligations.

Association of British Insurers
June 2014

[1] http://www.fca.org.uk/firms/being-regulated/meeting-your-obligations/fair-treatment-of-customers