Association of British Insurers

31 March 2017

ABI response to ICO consultation on GDPR consent guidance

About the ABI:

The Association of British Insurers (ABI) is the leading trade association for insurers and providers of long-term savings. Our 250 members include most household names and specialist providers who contribute £12bn in taxes and manage investments of £1.6 trillion.

Response:

We believe that the ICO guidance is helpful and broadly appropriate. However, we are concerned that there are some insurance products and service offerings that will have no legal basis for processing special categories of personal data, particularly given the interpretation of consent. This may potentially leave people without insurance cover. It will also add excessive costs, or administrative burden, or contribute to an overly long customer journey. This response highlights our key concerns.

- **Explicit consent/Processing special categories of data**

  Currently in order to process special categories of data, in particular health data, the only legitimate processing ground available is "explicit consent". However, given the ICO's interpretation this would now appear invalid under GDPR.

  Insurers need to process special categories of data in order to provide a number of types of insurance (for example, but not limited to: health insurance, travel insurance, life insurance). The data is needed to carry out a number of functions, such as to price and underwrite according to the level of risk presented, and to process claims.

  If we have interpreted GDPR and the guidance correctly this consent is now likely to be inappropriate. Health data is fundamental to providing most insurance products. This means without it the service cannot be provided and provision of explicit consent to process health data is therefore a precondition of accessing a service. If consent is not appropriate in this context, then this leaves no appropriate ground to process this data or provide the service.

  Given the above, we would be grateful if the ICO could add some further examples in relation to the processing of special category data within the ICO consent guidance, particularly as a condition of the service.

  If consent is still not appropriate, and in order to ensure that insurers have a legitimate ground on which to process special category data, we have called on DCMS to provide a new legal ground for processing special category data. We endorse the comment in the ICO guidance, "explicit consent is one way to legitimise processing special category data, but not the only way. Article 9(2) lists nine other conditions and there is some scope for UK legislation to add more".

We wrote to the Department of Media, Culture and Sport (DCMS) in February 2017 (see Appendix one), seeking that it retain the provisions of **Statutory Instrument 2000 No.417 The Data Protection (Processing of Sensitive Personal Data) Order 2000** in new legislation. This Order contains a range of exemptions to the DPA 1998 that are vital to insurers' ability to serve their customers, including a provision to allow insurers to process fraud, and certain health data without explicit consent.

We are also seeking that DCMS recognises principles in the **Consumer Insurance (Disclosure and Representations) Act 2012:** This recognises that an individual may act on behalf of, or as an agent, and provide information on behalf of another in order to obtain insurance cover on their behalf. This benefits the third party and makes it easier for individuals to obtain insurance. For example, one member of a family may arrange travel insurance on behalf of all those travelling, thereby authorising an insurer to process the third party's health data. This principle is recognised by sections 7, 8 and 9.

We would greatly value the ICO's support in our representation to the DCMS regarding the need to pass legislation as enabled by Article 9 (2), to provide insurers with a legitimate ground to process special category data, in a manner that will support good consumer outcomes.

- **Naming organisations/third party organisations relying on consent**

The ICO consent guidance states that in order for consent to be "specific and informed", controllers must "name your organisation and any third parties who will be relying on consent – even precisely defined categories of third party organisations will not be acceptable under the GDPR".

We recognise that Recital 42 states that "for consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended", however, we had interpreted this as being limited to identifying the insurer and any categories of third party to whom the data may be sent. This interpretation appears to be in line with ICO guidance on privacy notices which states that "you should give people a clear idea of the types of organisations you are supplying their information to, what purposes it will be supplied for".

Large insurance organisations send personal data to a number of service providers. It would not be practical to provide a list of all the names of these third parties, for example the third parties are subject to change; the list of third parties is potentially very long and unknown at the point of purchase; the identity of the third party may be commercially sensitive.

If such processing requires a separate consent (under the "unbundled" consents requirement) then there is a risk that data subjects will refuse this aspect of the consent when it is integral to the functioning of many types of insurance. A lack of consent could impact the availability of reinsurance cover, which is an essential function of the insurance market and enables provision of cover to customers.

We therefore ask that the ICO guidance be amended to reflect a proportionate approach to disclosure of third party organisations.

- **3rd party consent, e.g. for travel, motor, or health insurance**

  The ICO guidance does not address whether or not an individual can provide consent on behalf of another individual. The GDPR places greater emphasis on Data Controllers to demonstrate that the Data Subject has consented to the processing of their personal data. As such, we remain concerned that there is a lack of practicable processing ground to provide customers with insurance cover on behalf of third parties.

  Whilst we welcome the point that it appears it will be possible to process personal data for other policy beneficiaries under the processing grounds of "necessary for performance of a contract" or "legitimate interests", there is no legitimate basis for processing sensitive personal data.

  As noted in our previous position papers, we continue to be concerned about the impact this will have on the ease with which consumers can access and obtain insurance on behalf of family, friends and children. Third party insurance cover is provided to benefit the third party and is commonly arranged by one policyholder on behalf of third parties for example with motor insurance when adding a named driver to the policy; travel insurance for a family or group of named individuals; private medical insurance for members of the main policyholder's family.

  We would welcome any clarity or examples within the ICO guidance that clarifies a GDPR compliant ground for processing special category personal data to enable continued provision of third party insurance.

- **Grandfathering of consents**

  Customers are currently used to their policies being automatically renewed on the basis of grandfathering of previously given consent. If insurers are required to gain active consent from all individuals named on a policy, annually, to process personal and sensitive personal data, this could lead to periods of time where the individual is uninsured, and create time-consuming administration and a lengthy customer journey, to ensure individuals have continued cover.

  We would welcome clear examples as to the extent that existing DPA consents can be relied upon. We would also appreciate guidance about the extent to which consent must be obtained from third parties named on a policy.

- **Direct marketing**

  It would be beneficial if the ICO guidance referenced Recital 47 of GDPR when referring to legitimate interests for processing personal data. Recital 47 states that "the processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest". Further guidance on this would provide clarity to firms that they are able to use customers' personal data for direct marketing, for example contacting customers when their insurance policy is due for renewal. The customer's interest remains protected by Article 21 (2) which provides a right to object to processing of personal data for marketing.

- **e-Privacy and GDPR**

  The relationship between e-Privacy Regulation and GDPR is not clearly explained in ICO guidance. There are question marks as to whether the e-Privacy Regulation will be finalised to meet 25 May 2018 deadline and what the final text will be. The ICO need to clarify the

position of consent requirements for electronical marketing to individuals. If the e-Privacy Regulation is not finalised in time to enter into effect alongside the GDPR (as a number of commentators have suggested) then the question will be if GDPR consent requirements trump those laid down in the existing Privacy & Electronic Communications Regulations, particularly in regard to the soft-opt in rule and the extent this can be relied on. The ICO guidance only contains a very short paragraph about e-Privacy Regulations and PECR, so greater clarity would be helpful.

- **Duration of consent**
  We would welcome clarity about how long consent lasts. GDPR Recitals 65 and 68 note that personal data may be retained "for as long as the personal data are necessary for the performance of that contract". The ICO example provided within the consent guidance is not pertinent to insurers, and we would welcome a further example that provides greater clarity in the insurance context. We would also welcome an explanation as to when consents should be refreshed, as this is not explicitly referenced in GDPR.

Appendix One – ABI Paper to DCMS February 2017

Background

At a meeting on 23 January, the ABI agreed to send DCMS a paper outlining insurers' key outstanding concerns regarding General Data Protection Regulation (GDPR) legislative changes and operational impacts. This paper outlines the four key issues:

Issue 1: Processing criminal conviction and offences data

Insurers process data relating to criminal convictions and offences to more accurately assess risk and help prevent fraud. Consumers benefit with reduced premiums resulting from a lower level of fraudulent claims as a result of fraud screening. In 2015 insurers detected claims fraud with a value of £1.3bn.

Approach under the existing data protection regime

Under Directive 95/46/EC "Processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law…".

The UK implemented the Directive in the form of the Data Protection Act 1998 and included criminal convictions data within the definition of "sensitive personal data" which therefore provides "suitable specific safeguards". Insurers are therefore currently able to process criminal convictions data in reliance on one of the processing conditions set out in Schedule 3.

Approach under General Data Protection Regulation (GDPR)

Article 10 of the GDPR states that "processing of personal data relating to criminal convictions and offences or related security measures based on Article 6 (1) shall be carried out……when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects". This appears to be a two-limb test. Insurers will therefore be unable to process criminal conviction data unless:

(a) it is explicitly authorised by UK law – maintaining the current arrangements will not be adequate as consent alone is not an adequate basis for processing or holding this data under GDPR; and

(b) such authorising law provides for appropriate safeguards for data subjects.

Insurers therefore need DCMS to legislate to authorise them to process criminal conviction data for the purposes of identifying risk and preventing fraud and ensure that any such authorising legislation provides for appropriate safeguards

Issue 2: Fraud prevention

Insurers also use fraud databases, including the Insurance Fraud Register (IFR) and the Health Insurance Counter Fraud Database ("HICFG"), use of which can lead to referrals to the National Crime Agency (NCA). These registers are currently permitted through existing exemptions (Data Protection Act 1998 and the Serious Crime Act 2007) which permit insurance companies to cross-check against fraudulent behaviour.

CIFAS and the Insurance Fraud Bureau (that operates the IFR) have Specified Anti-Fraud Organisation (SAFO) status (awarded under s.68 Serious Crime Act) meaning that they are trusted to share data

with public sector bodies for the purposes of preventing fraud. Databases help to prevent fraud and support compliance with requirements from the Proceeds of Crime Act and 4th Money Laundering Directive.

Employee screening within financial services is currently undertaken through the Disclosure Barring Service (DBS). This provides an assurance that potential employees in roles with access to confidential information are not listed as barred by the DBS, protecting customers' and firms data. In addition, the PRA and FCA approved persons regimes under the Financial Services and Markets Act 2000 require firms to make sure Approved Persons are 'Fit and Proper' to perform their function.

Approach under GDPR

To maintain the protections provided by current counter-fraud activity we need DCMS to explicitly authorise processing for the detection and prevention of fraud under Article 10 of GDPR. Furthermore, fraud databases and prevention processes use automated decision-making processes to identify fraudulent activity and to cross-reference information with other fraud databases.

Under GDPR this automated individual decision-making is required to be authorised by member state law under Article 22 (2.b). Recital 71 of GDPR refers to profiling to ensure security and reliability of services, or in connection with the monitoring of fraud and tax evasion, as types of automated decision which could be justified based on Union or Member State law. Insurers need DCMS to legislate to clarify the position of pre-existing UK statute, to allow them to utilise fraud data to meet their regulatory obligations and help prevent fraud.

Issue 3: Retaining the provisions of Statutory Instrument 2000 No.417 The Data Protection (Processing of Sensitive Personal Data) Order 2000.

Statutory Instrument 2000 No.417 The Data Protection (processing of Sensitive Personal Data) Order 2000 (SI 417) contains a range of exemptions to the Data Protection Act 1998 that are vital to insurers' ability to serve their customers. Of particular importance to insurers are paragraphs 1, 5 and 6.

Paragraph 1 - allows the processing of sensitive personal data when it is in the substantial public interest, is necessary for the prevention or detection of any unlawful act, and must necessarily be carried out without the explicit consent of the data subject. This allows the processing of fraud and criminal conviction data in the substantial public interest and allows processing of this data for the detection, not just prevention, of any unlawful act, including fraud.

Paragraph 5 - allows insurers to process data relating to the parent, grandparent, great grandparent or sibling of the insured person, or member of a group scheme, for the purpose of carrying insurance business and where they cannot reasonably be expected to obtain explicit consent. This provision is essential for enabling individuals to obtain health insurance, using their family health history to inform the level of risk, despite the fact that by doing so a family member's data will be used without their explicit consent.

Paragraph 6 - allows for the grandfathering of existing sensitive personal data processing prior to the implementation of the order. We ask DCMS to review whether this is possible for existing consents prior to GDPR. There is a significant risk that a number of insurance customers will be left unwittingly without cover at renewal if insurers are unable to obtain consent. Obtaining consent will be particularly challenging in respect of third parties named on a policy.

Approach under GDPR

Under GDPR sections of the DPA will be repealed and new legislation is going to be required. We assume that SI 417 will therefore become obsolete. The inability to process sensitive personal data in the manner outlined above will have a significant impact and we believe that DCMS should replicate the provisions of SI 417 in new legislation. We understand that GDPR makes allowance for such provisions through either Recital 10 or Article 9 (4).

Issue 4: Recognising the principles in the Consumer Insurance (Disclosure and Representations) Act 2012

The Consumer Insurance (Disclosure and Representations) Act 2012 (CIDA) recognises that an individual may act on behalf of, or as agent, and provide information on behalf of another in order to obtain insurance cover on their behalf. This benefits the third party and makes it easier for individuals to obtain insurance. For example, one member of a family may arrange travel insurance on behalf of all those travelling, thereby authorising an insurer to process the third parties health data. This principle is recognised by sections 7, 8 and 9 of CIDA.

Approach under GDPR

It is vital that the principle of obtaining insurance for the benefit of a third party is maintained after the implementation of GDPR. If this principle is not maintained there is a high risk that a number of customers will be left without adequate insurance cover, this risk will be especially high in regard to travel insurance.

Certainty may be provided by suitable ICO guidance on consent that recognises the importance of this principle for customers. However, DCMS could consider using the scope for derogation contained within Recital 10 and Article 9 (4) to make explicit provisions that enable individuals to obtain insurance for the benefit of a third party.