Insurance

RE: DCMS CALL FOR VIEWS

Dear Sir/Madam

We thank and welcome DCMS's call for views regarding the General Data Protection Regulation and how organisations like ours are dealing with the challenges of implementing the new provisions.

Please find attached a paper which summarises the Co-op Insurance's key concerns relating to the implementation of the GDPR. We would strongly urge DCMS to implement additional legislation to address these concerns.

Our main concerns relate to the fact that 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, administrative burden and contribute to an overly long customer journey. We are also concerned that it would appear that online offering of insurance would no longer be possible.

We sincerely hope that you find our paper informative and useful. In the meantime should you have any further questions please do not hesitate to contact us.

Yours sincerely

Issue 1: Processing of Personal Data relating to criminal convictions and offences

- **Issue**

Article 10 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 only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority*". This removes the ability currently within the DPA 1998 for insurers to process personal data:

- for the purposes of the prevention or detection of crime (DPA1998 Part IV – Exemptions, para 29 Crime and taxation)
- where it is necessary for the purposes of preventing fraud or a particular kind of fraud (DPA 1998 Schedule 3, para 7(1)A 9b).

- **Impact**

Without additional legislation from the UK Government, insurers like Co-op, will not have a legitimate basis for continuing to process criminal conviction data, or data that is indicative of potential criminal activity, on named individuals, to:

- underwrite according to the level of risk and price the insurance premium accordingly.
- detect and reduce fraud, both by screening for previous fraud at point of quote/sale, and by assessing whether a claim is likely to be fraudulent.
- prevent fraud: via their own internal fraud registers and the Insurance Fraud Bureau, insurers keep data relating to individuals and their conviction and offence data. In motor insurance, for example, insurers also use enhanced information from external databases such as the Claims and Underwriting Exchange (CUE) and MIAFTR (Motor Insurance Anti-Fraud Theft Register, No Claims Database (NCD) and driving licence (DVLA) databases. These wider data sets are important sources of information for insurers to identify and reduce fraud.
- vet potential recruits or employees for past fraudulent activity or criminal conviction data.

Motor insurance businesses. in particular, currently use enhanced information from wider data sets, or external databases such as 'CUE' database, NCD and driving Licence (DVLA) databases, as well as our own fraud registers. This allows more data to be analysed at quote or sales stages, enabling accurate pricing, and helping to reduce fraud.

If we were no longer able to process conviction and offence data or can no longer ask customers whether they have a criminal conviction or have committed an offence, this will have a negative impact on consumers, society and business:

- Insurance premiums for honest, law-abiding customers are likely to increase. The majority of consumers will end up paying higher premiums to cross-subsidise payments made for fraudulent claims.
- Wider society is likely to suffer from a range of behavioural changes. Criminals and would-be criminals will have a reduced disincentive to offend, as they will be treated in the same way as law-abiding citizens. This is likely to lead to a greater number of offences and fraudulent activity, including offences that put people's lives and safety at risk. These activities, for example, "crash for cash", in turn create an avoidable burden on public services (e.g. police, emergency services and NHS) to investigate and treat injured parties.

- We understand that the Association of British Insurers (ABI) estimates UK insurers like ourselves had detected over 130,000 fraudulent general insurance claims, worth £1.3bn in 2014. 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.

➢ **Possible Solution**

It appears that new legislative measures will need to be introduced to legitimise the processing of conviction data, if the obligations under GDPR Article 10 cannot be met.
We would urge DCMS to use its flexibility under Article 10: "processing…shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law…", and request that DCMS to introduce legislation that:

- clarifies the meaning of 'shall be carried out only under the control of official authority' in the context of Article 10 to legitimatise insurers like Co-op Insurance and our third parties that process criminal conviction data for the above purposes
- support Insurance companies like Co-op Insurance to process criminal data lawfully under Article 6 (Lawfulness of processing) states that "Processing shall be lawful only if and to the extent that at least one of the following applies…". The list includes c) "processing is necessary for compliance with a legal obligation to which the controller is subject".
- provides an alternative to explicit consent as we have concerns that this would not constitute an appropriate legal basis for this type of data processing.

Issue 2: Consent for special category data processing

- **Issue**

Article 9 of the GDPR details the applicable legal bases that Co-op Insurance can use in order to process special categories of personal data, such as health or criminal convictions. There are a number of Statutory Instruments that are applicable under the current Data Protection Act 1998 for Insurance Contracts, for example they allow current and future policyholders to enter into a contract with sensitive health data via the process of obtaining the insurance contract direct or via a main policyholder.

To maintain the provision of cover on policies which include health data to new and existing policyholders our understanding is that existing legalisation will need to be maintained because GDPR offers no appropriate legal basis to respond to an individual's claim that includes health data because the individual is not in a position to a) provide consent and where b) Article 9c is not appropriate. Therefore it would not be possible to objectively comply with the requirements of Article 7(4) and Recital 43 as explicit consent to process sensitive data is deemed invalid when health data forms part of the contract. This is unlike the current position where Statutory Instrument (SI) 417 provides the legal basis for processing sensitive data when entering into an insurance contract. Furthermore, Recital 43 states "*Consent is presumed not to be freely given... if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance.*" The process of entering into an Insurance Contract is determined by the provision of information, and in some cases sensitive information.

Explicit consent is one way to legitimise processing of special category personal data, with some scope for UK legislation to add more. Without an exception for 'Sensitive data as part of an Insurance Contract' as is now, the process of providing an insurance contract, whether would be complex and disruptive for the policyholder. This includes the claims stage at a time when the individual may be in peril, (i.e. an accident abroad or a car accident), and the additional requirement to obtain a necessary consent before the claim can be processed would not be the individual's principle focus. In addition, the requirement for onward transfer of health data to organisations remains essential in the provision and administration of insurance, including the ability to reinsure individual large claims, or claims portfolios at a later date to the benefit of wider policyholders.

There are other circumstances which are unique to the insurance sector where health data is passed on for insurance related purposes. For example, an insurance company may re-insure the risk out to a reinsurance organisation to manage the maximum exposure the primary insurer and could include any one claim or set of claims within a portfolio. This is a commercial practice to reduce the expense for the primary insurance company. The risk transferred may or may not include health and criminal conviction related data. At the point of purchase, the insurance company would not necessarily have made the decision to reinsure. The process is determined by the Insurance Treaty arrangements which could be based on a) the 12 month period value or b) individual high value claims. This is common practice, but without explicit consent from the policyholder risk sharing of this nature would prohibited. The nature of Reinsurance practices within the UK Insurance market should be explored in detail by the relevant UK consultative governmental bodies, as this is a common commercial practice within the UK Insurance Sector.

There appears to be a strong rationale to maintain the Consumer Insurance (D&R) Act 2012 which authorises one party to act on behalf of another. Without this, Home and Motor policies will be rendered unviable in their current form, again removing existing cover from current and future policyholders. Our experience tells us that a the majority of home and motor policies organised for on behalf of family members are done so by a family member

responsible for the well-being of that family, the same would also apply for organisations providing insurance for their employees and families. It is likely there will be a deluge of dis-satisfied customers as they would not be permitted to organise cover for those they are responsible for and are dependent on a secondary call with another family member seeking consent, if sensitive data forms part of that policy. This will also be problematic where nominated spokesperson (i.e. interpreters, adult children acting on behalf of elderly parents) are prohibited from seeking quotes, or purchasing insurance on behalf of an individual for which they have taken responsibility.

In Motor Insurance we ask "*whether there are any restrictions relating to other named drivers*", the main policyholder would not be able to provide this information on behalf of a named driver. For example, a father calls to add his son to the policy, the son has a medical condition, but the father cannot discuss this on the son's behalf. A second call or subsequent follow-up with the insurance company and the son would then be required. The son may not contact the insurance company and, in the event there was an accident which was a direct result of the son's illness, the son and any other party involved would not be insured.

- **Possible solution**

Given the complexities of current underwriting practices specific to the processing of sensitive data as part of an insurance contract and the restrictions around the appropriate use of explicit consent under the GDPR detailed above we would urge DCMS to maintain both the existing SI 417 and the Consumer Insurance (D&R) Act 2012 to address these complexities where health data forms part of the insurance contract and where the main policyholder acts on behalf of others.

Issue 3: Consent from Third Parties

- **Issue**

The GDPR (Article 6 (1) and Article 7) places greater emphasis on Data Controllers to demonstrate that the Data Subject has consented to the processing of their personal data. There is a risk that insurers will no longer be able to legally provide cover to named third parties without obtaining (and demonstrating they have achieved) direct consent from the third party(ies).

- **Impact**

This would place significant burden on consumers who want to access and obtain insurance on behalf of family and friends. Third party cover is commonly arranged by one policyholder on behalf of third parties for a variety of insurance lines, for example:
- Motor insurance, e.g. when adding a named driver to the policy
- Home insurance, e.g. for a policy also covering a family or group of named individuals

We would urge DCMS to extend insurance cover to third parties without the need to obtain direct third party consent. Insurers currently process sensitive personal data to price, underwrite, and administer the insurance policy and process claims. It is common industry practice for the main policy holder to provide an insurance company with personal data and sensitive personal data of all parties named on the policy, on the basis that the main policy holder confirms that the additional parties have given them their consent to do so.

If explicit consent to process personal data has to be collected from each individual, we are concerned that there will be a number of detrimental consequences:

- People who are currently covered by third party insurance are likely to be left without cover (that would have been bought on their behalf and for their benefit), against a range of risks.
- Significantly increased operational costs leading to higher insurance premiums for customers. The potential requirement for insurers to gain explicit consent from each insured person in turn will make purchase calls more complex and many will not be able to be transacted in a single call if the other dependents are not available. These costs (e.g. to build IT systems and greater time and staffing to obtain and process consent) would eventually be passed on to the consumer, increasing the price of insurance.
- Inconvenient and lengthy customer journeys. Customers will endure a difficult process in trying to arrange third party cover if consent is to be provided from each person named on the policy. This would be a backwards-step for the insurance industry's ability to treat customers fairly and provide a competitive, modern and efficient service.
- Fewer people are likely to complete the sales process which will result in lower levels of insurance cover. For example, if a policyholder is a parent of a named driver and wanted to take out that policy it would not be incepted until the named driver had also confirmed their consent. Time delays may risk both the policyholder and named driver being uninsured until the explicit consent of both parties was captured. For another example, customers are currently used to their policies being automatically renewed and the grandfathering of previously given consent. If insurers were required to gain active consent from each individual on that policy, each year, to process personal and sensitive personal data, this could lead to periods of time where the individual is uninsured, and create time-consuming administration to ensure continued cover for both individuals and insurers where there currently is none.

Furthermore, Co-op Insurance would have to provide names and details of all third parties relying on consent (which would relate to health and criminal conviction data under Explicit Consent). This would require us to set out details of all third party organisations that are essential in the provision and administration of the insurance contract. These parties would vary from policy to policy dependant on the available agent, location, commercial arrangement, and type of service. Therefore, having this detailed at a granular level within the Privacy Policy would be unsustainable. No sooner as we have listed the details of hundreds of suppliers, these details could change and the Privacy Policy would become obsolete. Our experience shows that a customer's focus would be principally obtaining the treatment, service and support at claims stage.

Finally, we would also question whether there was a commercial implication to the listing of suppliers and therefore revealing commercial contracts would be considered commercially sensitive.

- **Possible solution**

We would ask DCMS to introduce legislation that:

- allows consent to be provided on behalf of others to set up or amend insurance policies.
- grandfathers consents: if existing consents cannot be grandfathered under the GDPR, this could cause a loss of policy take up. Individuals will be faced with a barrage of consent requests from organisations leading to consumer dissatisfaction and confusion
- clarifies 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. Given that the Consumer Insurance (Disclosure and Representation) Act 2012 (CIDA) makes explicit the duty of the consumer (main policyholder) providing information, including on behalf of a third party or parties that the main policyholder takes "reasonable care not to make a misrepresentation to the insurer" (paragraph 7 (1, 2 and 3), and paragraph 8). The Act has the expectation that the third party provided information to the insurer "directly or indirectly" it is unclear how this accords with GDPR provisions.
- clarifies the extent to which the definition of a child (as anyone under the age of 13) for the purposes of commercial internet services such as social networking, will apply to insurers providing parents or guardians with insurance cover on behalf of children.

Issue 4: Automated individual decision-making, including profiling

- **Issue**

The GDPR introduces new rules for 'profiling'. As the underwriting process involves systematic profiling of individuals so that we 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.

Article 22 relates to underwriting practices where data is analysed through mathematical decision making algorithms to determine the technical price, i.e. the premium to cover the risk. The benefit of this practice has been noted in the recent ICO Big Data paper. For non-sensitive data, an individual can object to Article 22 processing whereby the Data Controller would further explain how this is a legitimate process to establish optimum pricing, forming a contract. However, if an individual withdraws consent for processing sensitive data which forms part of an insurance policy, it would not be possible to continue to provide the contract to the data subject/policy holder.

- **Impact**

The precise opportunity cost for innovation is difficult to quantify; however, opportunities to optimise Big Data sets and the Internet of Things will be restricted, or made more difficult to achieve, as a result of the following:

- Resources that could be used to drive new business ventures may be required to enable compliance with GDPR. For example, making changes to systems to facilitate right to erasure or data portability will deprive business of resource that could be used for more forward thinking activities.
- Restrictions imposed by GDPR on profiling and automated decision making will limit an insurer's ability to reap benefits from advances in field of Data Science and Big Data Sets. Restricting profiling to where it is necessary to perform a contract; authorised by law or consent has been obtained will be challenging operationally and will prove detrimental in preventing and detecting fraud. Marketing campaigns will also be less effective
- Documentation and Website changes will prove costly and challenging to manage within timescales for implementation. This will impact upon General Insurance and Commercial Markets where broker relationships will need to be more closely defined.

Furthermore given the provisions in GDPR, and the inability to make decisions based on special categories of data where an automated decisions takes place, it is very unclear if online insurance can now be offered at all.

- **Possible solution**

We would ask DCMS to introduce legislation that:

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