



ABI response to DCMS Call for views on GDPR

The ABI

The Association of British Insurers 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 £1.6trillion.

Introduction

Establishing certainty for the future grounds of data processing under GDPR, and doing so quickly, is going to be essential for the uninterrupted provision of insurance products to UK consumers. We therefore appreciate the opportunity from DCMS to provide our views on the GDPR derogations.

As will be clear from the ABI's previous representations and position papers on GDPR, the ability to process data, including personal data and sensitive personal data, is of fundamental importance to the provision of a competitively priced insurance. The resultant ability for individuals to transfer their risks to an insurer is to the benefit of individuals ('data subjects' in the context of GDPR) and wider society. The provisions contained within the GDPR text create challenges for insurers, which will necessitate the use of some of the available derogations. Please find a summary of the key concerns of the insurance industry.

Theme 5 – Archiving and Research

Article 89: Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

Data retained by insurers and reinsurers under Article 89 should not be subject to Article 21 (right to object to processing). Automated decision-making and profiling are necessary for insurers to accurately calculate the level of risk posed by an individual before entering into a contract by using historical behaviours and data to predict future risk (please see points under Theme 9 – Rights and Remedies (Article 22: Automated individual decision-making, including profiling)).

Theme 6 – Third Country Transfers

Article 49: Derogations for specific situations

We have outlined in Theme 13 – Restrictions (Article 23: Restrictions) the need for a derogation for transfers which are required to comply with a legal obligation to which the controller is subject outside of the EU (e.g. The Office of Foreign Assets Control ("OFAC"), for checking against sanctions and any related reporting.

Theme 7 – Sensitive personal data and exceptions

Article 9: Processing of special categories of personal data

It is crucial that insurers can continue to process special categories of data so that they can provide individuals with cover that is proportionate to the risk they present, at a risk reflective price.

Insurers need to process special categories of data, in particular health data and criminal convictions data, for a wide range of insurance lines including, but not limited to, private medical insurance, travel insurance, motor insurance, and life insurance.

The data is used to inform key parts of the insurance contract, including underwriting, pricing, and claims handling (see also our points under Theme 9 (Article 22: Automated individual decision-making, including profiling)).

Under GDPR, insurers do not have a legal basis to continue to process special categories of personal data. Special categories of data includes 'data concerning health' (Article 9) and could, if legislation were passed, include data 'relating to criminal convictions and offences or related security measures based on Article 6(1) (Article 10)), under Article 6(b) 'necessary for performance of a contract' (unlike other types of personal data).

In order for insurers to process special categories of data listed under Article 9, the only processing ground available under GDPR is "explicit consent" (Article 9.2 (a)). However, processing special categories of data on the grounds of explicit consent is inappropriate, for a number of reasons, for example:

- The data processing is a precondition of accessing a service, meaning the data subject has no real choice to the processing of their data (ICO consent guidance makes clear that if people are not offered a genuine choice over how their data is used, consent is not an appropriate basis for processing).
- One of the conditions for consent (GDPR Article 7.3) is that the "data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent." Where insurance contracts contain special categories of personal data, insurers can only arrange, underwrite and administer and pay claims where the data is available. Therefore if consent is withdrawn, it would not be possible to continue to provide the contract to the data subject.

Relying on explicit consent will also prevent insurance being purchased on behalf of a third party. This includes where one person is taking out the insurance on behalf of others, for both personal lines and group policies offered via employers, e.g. to obtain family health insurance, group travel insurance, third party motor insurance on behalf of others, group protection policies and group insurance policies, and in situations where the data controller has no direct contact with the data subject.

We therefore need clarity on how consent can be provided to process special categories of data on behalf of another individual in the insurance context, and if this would be accepted as valid consent under the GDPR. If this is not addressed, consumers will face lengthier and more difficult journeys to obtain the insurance cover they need, and may lead to lower levels of insurance cover (exposing individuals to expensive costs and delays e.g. to medical treatment, if things go wrong).

Due to the issues outlined with consent as a basis for processing special categories of data, we are of the view that Government should:

- Use UK legislation for a derogation from the GDPR, so that paragraph 1 of Article 9 should not apply where: “the processing is necessary for the arranging, underwriting, and administration of insurance and reinsurance policies and insurance and reinsurance policy claims”.
- Retain the provisions of SI 2000 No. 417 the Data (Processing of Sensitive Personal Data) Order 2000, with extension of the scope within Paragraph 5, to allow individuals to obtain insurance on behalf of family and friends. Paragraph 5 currently 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.
- Retain the provisions within The Consumer Insurance (Disclosure and Representations) Act (CIDRA) 2012. CIDRA 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 party’s health data. This principle is recognised within CIDRA sections 7, 8 and 9.

Theme 8 – Criminal Convictions

Article 10: Processing of personal data relating to criminal convictions and offences

Article 10 requires that processing of criminal convictions and offences based on Article 6(1) can only be processed if authorised by Union or Member State law providing for appropriate safeguards.

If no domestic legislation is introduced, then insurers will not be able to use criminal conviction and offences data to identify risk, underwrite, price accurately, handle claims and to help detect and prevent fraud. The processing of such data by insurers also helps act as a disincentive for criminal behaviour, and contribute to a safer environment and society with less of a burden on public service resources.

We believe that the UK Government can provide appropriate safeguards by treating criminal convictions and records as sensitive/special category personal data under Article 9, with the same derogation for the insurance sector as for health data.

We are therefore seeking UK legislation for a derogation from the GDPR, so that insurers can process criminal conviction data for the purposes of identifying risk and preventing fraud, and ensure that any such authorising legislation provides appropriate safeguards for data subjects. We are seeking that Paragraph 1 of Article 9 should not apply where: “the processing is necessary for the arranging, underwriting, and administration of insurance and reinsurance policies and insurance and reinsurance policy claims”.

Theme 9 – Rights and Remedies

Art 22: Automated individual decision-making, including profiling

Automated decision making and profiling in the form of underwriting, is core to the provision of insurance. In cases where this profiling is 'solely' automated and if it produces 'legal' or 'significant' effect on the data subject it will fall within the scope of Article 22 of GDPR.

In data protection terms, the insurer evaluates historical personal data and behaviours, to predict future risk relating to a natural person. This allows insurers to charge a fair price for insurance that reflects the level of risk being insured. The evaluation can be conducted partially or fully by automated means, with limited or no human intervention from the insurer's side. Fully automated evaluations are expected to increase as, with digitalisation, consumers demand more and more online insurance services that are simple, efficient and quick.

We believe that the following is necessary:

- Legal certainty that insurers can rely on Article 22.2.a "is necessary for entering into, or performance of, a contract between the data subject and a data controller" as a legal basis for processing personal data where processing falls under Article 22 and produces a legal or significant effect.
- Explicit legal processing ground for the processing of special categories of data where profiling involving processing of special categories of data is necessary for performance of a contract. Please also see points at Theme 7 (Article 9: Processing of special categories of personal data).
- Legal certainty that data that insurers retain for underwriting and pricing under Article 89 should not be subject to the restrictions in Article 22. If a derogation is granted under Article 9 to enable the "processing is necessary for the arranging, underwriting and administration of insurance and reinsurance policies and insurance and reinsurance policy claims, then this should also include the ability for insurers and reinsurers to be able to make decisions by automated means (including by profiling) for the arranging and underwriting of insurance and reinsurance policies and insurance and reinsurance policy claims without consent even when special categories of data are involved.
- A corresponding derogation under Article 26 – Joint controllers. Under this Article, joint controllers need to set out in a contract their obligations under Articles 13 and 14. If a derogation is granted under Article 9 to enable the "processing is necessary for the arranging, underwriting, and administration of insurance and reinsurance policies and insurance and reinsurance policy claims", then there should be a corresponding derogation under this Article for insurers and reinsurers relying on such Article 9 derogation.
- Legal clarity that profiling is permitted in relation to the processing of children's data for insurance purposes. A new specific derogation is required to explicitly authorise a child's personal data to be processed via an automated decision, for example as part of a family travel insurance policy or family health insurance policy.

Theme 13 – Restrictions

Article 23: Restrictions

Government should legislate to continue similar restrictions that exist under the current Directive and which were used in the Data Protection Act 1998, to shape appropriate exemptions from the

requirements of the DPA where that was permissible. As noted in Theme 6 - Third Country Transfers (Article 49: Derogations for specific situations), Theme 7 – Sensitive personal data and exceptions (Article 9 Processing of special categories of personal data), Theme 8 – Criminal Convictions (Article 10: Processing of personal data relating to criminal convictions and offences) and Theme 9 – Rights and Remedies (Art 22: Automated individual decision-making, including profiling), we request:

- That UK Government legislates for a derogation from the GDPR so that Paragraph 1 of Article 9 should not apply where “the processing is necessary for the arranging, underwriting, and administration of insurance and reinsurance policies and insurance and reinsurance policy claims”
- A derogation enabling UK controller from complying with a legal obligation originating from outside the EU to which the controller is subject (e.g. the Office of Foreign Assets Control (“OFOA”) for checking against sanctions and any related reporting).
- Use of the wider remit of Article 23 to seek to replicate the exemptions under the DPA firms may currently use to disclose or not disclose personal data, in certain circumstances, for example:
 - s. 8(5) – ability to withhold information about the logic involved in automated decision- taking if, and to the extent that, the information constitutes a trade secret
 - s. 29 – exemption relating to crime and taxation
 - s. 35 exemption relating to disclosures required by law and made in connection with legal proceedings
 - schedule 3 (7A) – condition relating to processing by anti-fraud organisations
 - schedule 7 – various miscellaneous exemptions.

Additionally, in relation to Article 23, Articles 14-21 should not apply in relation to crime prevention and detection.

