Position Paper

Insurance Europe's contribution to the Article 29 Working Party consultation on draft guidelines on consent

Our reference:	COB-DAT-18-014	Date:	23 January 2018
Referring to:	Article 29 Working Party public consultation on draft guidelines on consent		
Contact persons:	Georgia Bakatsia, Policy Advisor, Conduct of Business William Vidonja, Head of Conduct of Business	E-mail:	bakatsia@insuranceeurope.eu vidonja@insuranceeurope.eu
Pages:	5	Transparency Register ID no.:	33213703459-54

Introduction

Insurance Europe welcomes the Article 29 Working Party's (WP) draft guidelines on consent under the General Data Protection Regulation (GDPR). However, since, in the absence of a derogation at national level, explicit consent is **the only legal basis under the GDPR for insurers to process sensitive data when entering into an insurance contract**, it is essential that these guidelines provide legal certainty to insurers when carrying out their business.

Thus, Insurance Europe invites the WP to provide the necessary clarifications of the issues outlined below.

Health data processing in insurance and why consent matters

Processing of health data is a prerequisite for providing a number of types of insurance policies, such as health, long-term care, disability and life. For these policies, insurers need to process health data in order to assess and price ("underwrite") the risks that consumers wish to protect themselves against, provide the corresponding insurance coverage, and perform their contractual obligations, such as the evaluation and payment of claims.

The special categories of data (sensitive data) specified in Art. 9 (1) of the GDPR include health data. Although Art. 9(2) lists 10 legal grounds to process special categories of data, **the only appropriate legal basis under the GDPR for insurers to process health data when entering into the insurance contract, eg for underwriting purposes at the pre-contractual stage, is explicit consent (Art. 9 (2(a))**.

Thus, in the absence of the introduction of any legal basis at national level for processing health data, underwriting activities that require the processing of health data are dependent on the insured's consent. Insurers cannot process health data to assess and price risks, make an insurance offer and provide the related insurance services without such consent.

Insurance Europe aisbl
Rue Montoyer 51, B-1000 Brussels
Tel: +32 2 894 30 00 • Fax: +32 2 894 30 01
E-mail: info@insuranceeurope.eu
www.insuranceeurope.eu

Freely given consent in the insurance context

The GDPR strengthened the legal basis of consent by establishing, among other things, that consent should be freely given. Art. 7(4) in combination with Recital 43 states that consent shall not be deemed freely given when the performance of a contract is conditional on the data subject's consent, **despite such consent not being necessary for the performance of the contract.**

Following an *a contrario* interpretation, **conditional consent shall be considered as freely given if the processing of the data is necessary for entering into or for the performance of the contract.**

As the draft guidelines correctly mention: "*Article 7(4) seeks to ensure that the purpose of personal data processing is not disguised nor bundled with the provision of a contract or a service for which these personal data are not necessary*" (p.9).

Recommendations

- In order to provide the necessary legal certainty, the guidelines should clarify that consent is deemed freely given, and thus valid, where it is given for the processing of special categories of data that are necessary for entering into or for the performance of the contract in an insurance context.
- Insurance Europe invites the WP29 to include the following example in Section 3.1.2 — Conditionality:

  [Example X] An insurance company asks consumers for consent to use their health data for assessing the risks to be covered and for calculating the related insurance premium of a long-term care insurance policy. This processing of health data is necessary for entering into the insurance contract and thus consent shall be considered freely given. The company also asks for consumers' consent to process their health data for evaluating and paying out claims as provided for in the insurance policy. This processing of health data is necessary for the performance of the long-term care insurance contract and thus consent shall be deemed freely given.

Refusal and withdrawal of consent without detriment

Recital 42 states that consent is not regarded as freely given if the data subject is unable to refuse or withdraw consent without detriment. However, the draft guidelines do not provide the necessary legal certainty regarding what constitutes "detriment" as a result of refusing or withdrawing consent. As an example of detriment, the draft guidelines mention the broad notion of "any negative consequences" (p.11) or "lowering service levels" (p.21), without further analysing how the performance of a service can remain undisrupted when the data controller is not able — in the absence of a legal basis after the refusal or withdrawal of consent — to process the data that is necessary for the performance of the service.

In an insurance context, refusal or withdrawal of consent may have an adverse impact on the entering into and the performance of the insurance contract, according to national insurance contract laws. Insurance Europe believes that such an impact does not constitute a "detriment" for the data subject that renders consent not "freely given" and thus invalid.

For instance, in the context of a disability insurance contract, the insurer needs to process the policyholder's health data to verify if an event covered by the insurance policy has actually occurred in order to process and settle the claim and provide the related services and compensation. If the policyholder withdraws their consent for the processing of health data, the insurer can no longer handle and settle the claim. Since it is necessary to process this health data to handle the claim, the consequences of withdrawal of consent shall not be deemed a detriment.

Recommendations

- The guidelines should clarify that when the performance of a service is conditional on obtaining consent for processing data that is necessary for such performance, the withdrawal of consent might lead to the suspension of the provision of the service, and that such suspension is not deemed as a detriment that renders consent invalid.
- The guidelines should also clarify that any adverse effects on the data subject deriving from insurance contract law as a result of refusal or withdrawal of consent to process special categories of data does not constitute a detriment that renders consent not "freely given" and thus invalid.

Consent on behalf of third parties in the insurance context

It is common industry practice for third-party insurance cover to be arranged by one policyholder on behalf of third parties. For example, travel insurance or health insurance policies are taken out by a parent for the entire family. In these cases, the main policyholder provides the insurer with the health data of all the parties covered by the policy and confirms that the additional parties have provided their consent to the processing of their data.

However, the draft guidelines do not clarify whether this practice would remain possible under the GDPR. In the absence of legal certainty, insurers would have to seek direct consent from all third parties in order to provide them with coverage.

Insurance Europe is concerned about the impact this will have on consumers, since they will no longer be able to obtain insurance coverage for their family in a quick, straightforward way. Moreover, it will be extremely burdensome for insurers to obtain, and demonstrate that they have obtained, direct consent from the third parties, even for existing contracts.

Recommendation The guidelines should provide examples that clarify that insurers can continue to provide third-party insurance without having to obtain direct consent from the third parties.

Obligation to name third-party organisations

The draft guidelines state that in order for consent to be "informed", the data controller should name all the organisations to whom data is to be transferred (p.14). This obligation goes beyond the Level 1 GDPR text as, according to Articles 13 (1(e)) and 14 (1(e)), the data controller shall provide **either the recipients or categories of recipients of the personal data**. Thus, the GDPR does not prioritise providing the recipients over providing the categories of recipients. Mentioning the categories of recipients, rather than naming them, is sufficient under the GDPR.

In practice, when an insurance event occurs, insurance companies might need to send personal data to several service providers and the list of recipients can be very long or even unknown at the moment of collection of the data subjects' data, particularly for long-term insurance contracts. Therefore, in certain cases it is not even feasible to disclose the names of all third parties. For example, a travel insurance company would not be able to provide the names of the foreign medical experts or repatriation service providers to whom it may need to transfer personal data if an insured person has an accident while travelling abroad.

Recommendation The guidelines should treat the provision of the names and categories of recipients equally, and thus clarify that providing the categories of recipients, instead of naming them, is sufficient under the GDPR.

Children's consent and parental responsibility

According to the draft guidelines, consent provided by a holder of parental responsibility will expire once the data subject reaches the age of digital consent and the controller must obtain valid consent from the data subject them self (p.26).

However, Insurance Europe believes that children, as vulnerable subjects, should be protected and consent should not expire immediately upon reaching the age of digital consent. In an insurance context, if a child neglects to provide their consent when reaching the age of digital consent, they might be deprived of core services, such as life insurance, concluded for their benefit.

Recommendation Insurance Europe suggests that the guidelines state that consent provided by a holder of parental responsibility remains valid until the data subject acquires full legal capacity, according to national legislation, and does not expire when the data subject reaches the age of digital consent.

Multiple lawful grounds for processing activities

The draft guidelines state that "*as a general rule, a processing activity for one specific purpose cannot be based on multiple lawful bases*" and that the controller cannot swap between different lawful bases (p.22).

This rule contradicts the GDPR, which explicitly refers to the possibility of using more than one lawful basis for processing activities. In particular, Art. 6 (1), before listing the six legal grounds for processing, mentions that "*processing shall be lawful only if and to the extent that **at least** one of the following (legal bases) applies*". Thus, the GDPR wording grants to data controllers the possibility to base one processing activity on more than one legal basis.

Moreover, Art. 17(1(b)), when establishing the right to erasure, states that this right applies when the data subject withdraws the consent on which the processing is based according to point (a) of Art. 6(1) or point (a) of Art. 9(2), **and where there is no other legal ground for the processing.** This provision clearly implies that it is possible to rely on multiple legal bases and swap between them when the data subject withdraws consent. The reference to both Articles 6(1) and 9(2) in Art. 17 (1(b)) clearly indicates that the processing of special categories of personal data can be based on the multiple legal grounds of Art. 9(2), just as the processing of normal categories of personal data can be based on the multiple legal grounds of Art. 6(1).

Recommendation The sentence "*as a general rule, a processing activity for one specific purpose cannot be based on multiple lawful bases*" should be deleted, as it goes beyond the Level 1 GDPR text Moreover, the guidelines should clarify that it is lawful to base one processing activity on multiple legal bases.

Consent for compatible purposes

According to the draft guidelines, the requirement for consent to be specific entails that "*if a controller processes data based on consent and wishes to process the data for a new purpose, the controller needs to seek a new consent from the data subject for the new processing purpose. The original consent will never legitimise further or new purposes for processing*" (p.12).

This wording does not acknowledge the processing of data on the basis of consent for compatible purposes and runs against Recital 50 and Art. 6(4). Following a strict interpretation of specific consent would overload the data subjects, who would be asked to provide their consent even for purposes that are linked and compatible with the initial purpose.

Recommendation The guidelines should clarify that original consent can legitimise processing activities for purposes that are compatible with the purpose for which consent was initially provided in line with Art. 6(4) and Rec. 50.

Consent through electronic means

The draft guidelines mention that, in the digital context, the data subject receives multiple consent requests that need to be answered through clicks and swipes on a daily basis. This may result in click fatigue and in a situation in which consent questions are no longer read. According to the WP, "*the GDPR places upon controllers the obligation to develop ways to tackle this issue*" (p.17).

Insurance Europe's position is that this wording goes beyond the Level 1 GDPR text as the GDPR does not place any obligation on controllers to ensure that data subjects read the consent questions. It is disproportionate to shift the burden of responsibility for the data subjects' activities to the data controllers. Data controllers should be invited to educate data subjects about their rights and obligations, without issuing any obligations to ensure that data subjects read the consent questions before providing their consent.

Recommendation Insurance Europe suggests replacing the sentence "*The GDPR places upon controllers the obligation to develop ways to tackle this issue*" by "*The GDPR encourages controllers to find solutions to tackle this issue*".

Refreshing of consent

The WP recommends as a best practice that consent should be refreshed at appropriate intervals, since providing all information again helps to ensure that data subject remains well informed about how their data is being used and how to exercise their rights (p.20). Insurance Europe believes that this recommendation goes beyond the Level 1 GDPR text, as the GDPR does not include any provisions that require the refreshing of consent. In fact, Insurance Europe believes that this practice would be burdensome for data controllers and lead to fatigue for data subjects, who would be requested to provide their consent again and again.

Moreover, the refreshing of consent may lead to legal uncertainty, for instance if the data subject neglects to reply to the data controller's request to refresh their consent and does not withdraw their consent either. While the data subject's answer is pending, it is not clear whether the data controller should continue processing the data subject's data, taking into consideration also that the original data subject's consent was not withdrawn and thus remains valid.

Recommendation The guidelines should not include refreshing of consent as a best practice and the relevant paragraph on p.20 should be deleted.