

Concerns about EC proposal for an ePrivacy Regulation

| | | | |
|-----------------|--|-------------------------------|----------------------------|
| Our reference: | COB-DAT-18-105 | Date: | 14 January 2019 |
| Contact person: | William Vidonja, Head of Conduct of Business | E-mail: | Vidonja@insuranceeurope.eu |
| Pages: | 3 | Transparency Register ID no.: | 33213703459-54 |

Introduction

Insurance Europe welcomes the European Commission's proposal for an ePrivacy Regulation ("the proposal") and its objective to update and harmonise rules that govern electronic communications. Insurance Europe also fully supports the Council's approach of taking the time to scrutinise the proposal in detail and ensure that the adopted framework is not only robust and comprehensive but also fit for purpose.

While Insurance Europe believes that ensuring a high level of protection of electronic communications is essential, it is concerned about the unintended consequences that the proposal would have on the insurance industry and, ultimately, on consumers.

Scope of the ePrivacy proposal

The proposal aims to complement the new General Data Protection Regulation (GDPR), which already regulates personal data processing activities by insurers. Hence, any additional requirements imposed on top of the existing ones should serve a specific, legitimate purpose, bring added value to consumers and establish clear rules that do not hamper innovation.

- Insurance Europe acknowledges the need for additional rules to protect the confidentiality of electronic communications, as they may reveal highly sensitive information about natural persons. However, the scope of the proposal is significantly broader than the existing ePrivacy Directive and goes beyond setting rules that guarantee the right to confidentiality of electronic communications. For example, the rules under the ePrivacy proposal are extended to interpersonal communication services that are ancillary to another service as well as to machine-to-machine communications (M2M). These activities are already adequately covered by the GDPR when they involve the processing of personal data. Yet the proposal includes in its scope all M2M communications, regardless of whether there is an impact on privacy. For instance, it is not clear which privacy concerns the proposal is trying to address when M2M communication does not involve personal data. Privacy rules aim to protect the privacy of individuals. Hence, such rules are unnecessary when no-one's privacy is at stake.

The extremely broad scope of the proposal is not future-proof and would be likely to have an impact on the ability to offer innovative products that involve the processing of non-personal machine-generated data.

- The scope of the proposal is unclear and thus creates legal uncertainty over its impact on the industry. Against this background, Insurance Europe welcomes the clarification by the Council that customer-

care communication channels that solely allow customers to communicate with the company in question (Rec. 11a) do not not fall under the provisions of art. 5-7. This explanation is very important, as insurance undertakings are increasingly communicating with their clients via their own electronic communication services. Therefore, this clarification should be highlighted in the final text of the Regulation.

However, there is still legal uncertainty over the scope of other provisions in the proposal and this hinders assessment of the concrete implications for the insurance industry. For instance, art. 8 regulates the use of the processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment, as well as the collection of information emitted by the terminal equipment of the end-user to enable it to connect to another device. In an increasingly digital era and connected society the scope of this article seems extremely broad, as it is difficult to ascertain which processing activities do not rely on "processing and storage capabilities of terminal equipment". It is therefore not clear which processing activities the co-legislators intend to capture in art. 8.

The uncertainty of the legal framework is detrimental to the insurance industry. If the proposal is not amended, businesses would be forced to operate without clearly knowing the rules with which they must comply.

Recommendations: Insurance Europe invites the Council to:

- carefully examine whether processing activities that are already addressed under the GDPR should also be covered by the proposal; and,
- clarify the scope of the proposal to allow stakeholders to understand which sectors and activities are covered. To this end, it should be clarified which processing activities fall under the scope of art. 8.

Impact of art. 8 on innovative insurance products

Some innovative insurance products, such as telematics policies in motor insurance, are based on processing data from terminal equipment, such as black boxes, applications on mobile phones or other internet of things (IoT) devices.

Example: A policyholder opts for a motor third-party liability insurance policy which includes a clause that grants the policyholder a discount on the premium payment at the end of the year, provided that the analysis of certain data collected from the black box (eg driving speed, acceleration in turns) proves that the policyholder is not a high-risk driver.

In art. 8(1), the proposal prohibits the use of the processing and storage capabilities of terminal equipment, unless one of the exemptions listed under this provision is met. There is no clear exemption allowing insurers to process such data and execute a policy such as the one in the example above.

- Exemption of information society services — art. 8(1)(c): There is currently no explicit reference to the effect that the provision of services based on telematics constitutes an "information society service". Insurers would therefore not be able to rely on the "information society services" exception under art. 8(1)(c). It is not clear whether the Council aims to broaden the definition of an "information society service" when it mentions that "the provision of information society services, such as those used by IoT (for instance connected devices, such as connected thermostats), requested by the end-user" does not require consent (Rec. 21 of 19 October Council [text](#)).
- Exemption of consent — art. 8(1)(b): In the absence of clarity in art. 8(1)(c), insurers may only be able to rely on the exemption of consent. Nevertheless, it would be difficult to obtain valid consent when processing data from the terminal equipment is necessary for the performance of a telematics insurance contract. To be valid, consent must be freely given. As explained in the European Data Protection Board (EDPB) guidelines on consent, "consent can only be an appropriate lawful basis if a data subject is offered control and is offered a genuine choice with regard to accepting or declining the terms offered or declining them without detriment". Likewise, the individual should have the right to withdraw consent

without detriment. However, in the event that a policyholder refuses or withdraws their consent to the processing of data from the terminal equipment, the insurer would not be able to execute the policy, to the detriment of the consumer. An authorisation to process data is absolutely necessary for the performance of the insurance contract.

As a result, insurers cannot rely safely on any of the exemptions under art. 8(1), as currently drafted, for processing data from terminal equipment. The absence of a solid exemption on which insurers can rely in the final text would prevent insurers from providing innovative insurance products, such as telematics insurance, despite their benefits for consumers.

Hindering the development and offering of innovative products would ultimately reduce consumer choice and possibly increase the cost of insurance in the long term. In the black box example, for instance, the effective use of telematics is expected to lead to a reduction in the cost of motor insurance. Moreover, it should make insurance more widely available to some societal groups, such as young drivers who typically pay a higher premium for standard insurance products that are not adapted to their needs.

The ePrivacy proposal should therefore be aligned with the GDPR, which provides several legal bases for processing data, such as contract, legitimate interest, etc. As the EDPB expressly stated in its guidelines on consent, consent is not an appropriate legal basis when processing involves personal data that is necessary for the performance of a contract ("If a controller seeks to process personal data that are in fact necessary for the performance of a contract, then consent is not the appropriate lawful basis", p. 8 of the guidelines). Processing data from terminal equipment is necessary for the execution of a telematics insurance policy and, hence, consent is not fit for purpose. Under the GDPR, insurers would process such data relying on the legal basis of the performance of a contract (art. 6(1)(b)).

Recommendation: In line with the GDPR, Insurance Europe urges the Council to include a provision under art. 8 of the proposal that allows processing of data from terminal equipment when such data is necessary for the performance of a contract.