Position Paper

# Insurance Europe's comments on the monitoring of codes of conduct under the GDPR

| | | | |
|---|---|---|---|
| Our reference: | COB-DAT-18-065 | Date: | 11 July 2018 |
| Related documents: | | | |
| Contact person: | William Vidonja, Head of Conduct of Business<br>Georgia Bakatsia, Policy Advisor, Conduct of Business | E-mail: | vidonja@insuranceeurope.eu<br>bakatsia@insuranceeurope.eu |
| Pages: | 2 | Transparency Register ID no.: | 33213703459-54 |

## Executive Summary

Codes of conduct will provide insurers with an important tool to ensure compliance with the General Data Protection Regulation (GDPR) provisions. They provide the possibility to address the specific features of the insurance sector and they could facilitate the understanding and, thus, the application of the GDPR. Several national insurance associations, therefore, already established codes of conduct before the entry into force of the GDPR or are reviewing their existing codes.

Drawing up a code of conduct is, however, a lengthy process that requires significant effort and resources, and close cooperation with supervisory authorities. The industry needs clarity on the preconditions for the approval and implementation of a code of conduct.

Therefore, Insurance Europe urges the European Data Protection Board (EDPB) to issue guidance to clarify as swiftly as possible that the approval and implementation of a code of conduct does not require the establishment of a monitoring body pursuant to Article 41 of the GDPR.

## Importance of codes of conduct for the insurance industry

Codes of conduct bring significant advantages to data controllers and legal certainty to data subjects, as they clarify the application of the GDPR principles to the features and needs of a given sector. The GDPR acknowledges the importance of codes of conduct as it expressly calls on member states, the supervisory authorities, the EDPB and the European Commission to encourage the drawing-up of such codes.

Insurance is a heavily regulated sector at both EU and national level and the GDPR is one of the many pieces of legislation with which insurers have to comply. Thus, codes of conduct could facilitate compliance with the GDPR by providing thorough guidance to insurance companies on how to adapt to the new rules. Several national insurance associations have already established codes of conduct that have been approved by their supervisory authorities, under Directive 95/46/EC and their national data protection legislation. Practical experience has shown that such codes contribute significantly to the understanding and application of the data protection rules by insurance companies.

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

Since the GDPR introduced new obligations and enhanced the protection of personal data, the development of codes of conduct becomes even more important for the industry. Although drawing up a code is a lengthy process and requires intensive effort by the industry, several national insurance associations are now in the process of drafting or revising their already established codes. Adherence to a code of conduct establishes best practice in compliance tailored to the specific characteristics of the insurance industry at national level and ultimately, improve and facilitate the implementation of the GDPR. At the same time, approved codes of conduct bring significant benefits to consumers as they shed light on the processing activities carried out by their insurer.

## GDPR provisions on the monitoring body

The insurance industry is committed to complying with the GDPR rules and to demonstrating that compliance. Since codes of conduct are one of the key instruments for promoting compliance, it is essential that their implementation requirements are not unnecessarily burdensome. Given that, and since Article 40 (1) of the GDPR explicitly states that drawing-up of codes should be encouraged, the EDPB should provide legal certainty to the industry as soon as possible by clarifying the conditions for monitoring codes of conduct.

In particular, the EDPB should clarify that the GDPR does not require the appointment of a monitoring body as a precondition to the approval of or the recognition of adherence to a code of conduct. In contrast, it expressly states that the establishment of an independent body to monitor compliance with a code is **optional**[1].

The appointment of a monitoring body is not listed as a criterion for the approval of a code of conduct. Should an association decide to appoint an accredited monitoring body, the code of conduct should contain mechanisms that enable the body to carry out the mandatory monitoring of compliance with its provisions, pursuant to Article 40(4) of the GDPR. In other words, the provisions of Article 40(4) that refer to the inclusion of mechanisms in the code of conduct that enable the body to carry out the mandatory monitoring of compliance should be read in conjunction with Article 41(1), which establishes the optional appointment of a monitoring body. Hence, Article. 40(4) should apply only if a sector decides to appoint such a body. In line with the GDPR provisions, supervisory authorities should approve the code if they assess that it provides appropriate safeguards, without taking into consideration whether a monitoring body is in place.

Imposing an obligation to appoint a monitoring body would add an extra layer of unnecessary administrative burden and costs for the industry, which would ultimately hinder the development of codes of conduct. This would go against the co-legislators' intention to promote compliance through self-regulation.

Therefore, any interpretation that would make the appointment of a monitoring body mandatory would go beyond the GDPR Level 1 text. Moreover, the obligation to appoint accredited monitoring bodies would create a counter-incentive to drawing up new or revised codes of conduct by the industry.

## Insurance Europe's recommendation

**Insurance Europe invites the EDPB to issue EU-level guidance to clarify as swiftly as possible that the approval of and/or recognition of adherence to a code of conduct does not require the mandatory appointment of a monitoring body.**

[1] Article 41(1) of the GDPR states that "*the monitoring of compliance with a code of conduct pursuant to Article 40* ***may*** *be carried out by a body which has an appropriate level of expertise in relation to the subject-matter of the code and is accredited for that purpose by the competent supervisory authority*".