Position Paper

Response to the EDPB's draft-guidelines on Codes of Conduct & Monitoring Bodies

Our reference:	COB-DAT-19-029		
Referring to:	Guidelines 1/2009 on Codes of Conduct & Monitoring Bodies under Regulation 20116/679		
Contact person:	Ana-María López-Chicheri Llorente, Policy Advisor, Conduct of Business		
Pages:	5	Transparency Register ID no.:	33213703459-54

Importance of codes of conduct for the insurance industry

Codes of conduct bring significant advantages to data controllers and legal certainty to data subjects. This is because they clarify how the General Data Protection Regulation (GDPR) can be applied given the features of a certain sector. The GDPR acknowledges the importance of codes of conduct and expressly calls on member states, the supervisory authorities, the European Data Protection Board (EDPB) and the European Commission to encourage the drafting of such codes (Article 40, GDPR). Moreover, Chapter IV of the EDPB's proposed draft guidelines on codes of conduct & monitoring bodies (hereafter the draft guidelines) explains the benefits of codes of conduct.

Insurance is a heavily regulated sector at EU and national level, with GDPR being one of the many pieces of legislation which insurers must comply with. Codes of conduct could help insurers comply with the GDPR by providing useful guidance which considers the particularities of the insurance business model and sector in relation to the processing of data. They could also assist in providing clearer guidance and guarantees to consumers on how their data is processed.

This is why many national insurance associations have developed codes of conduct that had been approved by their supervisory authorities under the Data Protection Directive 95/46/EC and their national data protection legislation. Practical experience has shown that these codes contributed significantly to the understanding and application of the data protection rules by insurance companies and contributed to better consumer outcomes.

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 has become even more important. Although drawing up a code is a lengthy process which requires intensive effort and resources, several national insurance associations are now in the process of drafting or updating their codes or are considering doing so.

However, the EDPB's draft guidelines severely jeopardize the adoption of codes of conduct in the insurance industry by imposing a mandatory monitoring body and excessive accreditation requirements for this body. Consequently, Insurance Europe urges the EDPB to consider the industry's comments and recommendations when adopting the final guidelines.

Comments on the draft guidelines 1/2019 on Codes of Conduct & Monitoring Bodies under Regulation 2016/679

- **GDPR provisions on the monitoring body & the draft-guidelines interpretation**

  The EDPB's draft guidelines establish that the appointment of a monitoring body shall be mandatory for the approval of a code of conduct. This is because the EDPB interprets Articles 40 (4) and 41 (1) of the GDPR as calling for the mandatory appointment of such a monitoring body.

  However, the GDPR clearly states that the establishment of a monitoring body is optional since, according to Article 41 (1), "*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*".

  While Article 40 (4) GDPR establishes that if an organisation ***opts****,* according to Article 41 (1), to appoint a monitoring body as the mechanism to guarantee compliance with the code, then this monitoring body shall effectively carry out its duties. In other words, it shall conduct the mandatory monitoring of compliance for which it has been designated to do.

  Moreover, the non-mandatory nature of the monitoring body is also confirmed by Article 40 (2) of the GDPR which contains a minimum list of topics to be covered by codes of conduct. If the legislator's intention was to establish a mandatory monitoring body as a pre-requisite for the approval of codes of conduct, an explicit reference to the monitoring body would have been included in the list of topics in Article 40 (2) of the GDPR.

  Therefore, the GDPR does not contain a mandatory requirement for the appointment of a monitoring body for the approval of a code of conduct. Article 40 (4) should only apply if an association opts to appoint a monitoring body. Consequently, supervisory authorities should be able to approve a code of conduct if they assess that it provides appropriate safeguards, without taking into consideration whether a monitoring body has been appointed.

Recommendation: Insurance Europe urges the EDPB to acknowledge that the proposed draft guidelines go beyond the GDPR's Level text 1 and clarify that the appointment of a monitoring body is optional.

- **The lack of economic viability of mandatory monitoring bodies**

  The appointment of mandatory monitoring bodies would impose excessive burden and costs on national associations across all industry sectors. The heavy organisational and financial burden for developing a code of conduct, appointing a monitoring body and maintaining the required structure, for the sole purpose of obtaining approval of the code and monitoring compliance would significantly outweigh the benefits of having an approved code.

  Moreover, it contradicts the EDPB's description in paragraph 11 of the draft-guidelines of the benefits of codes of conducts as "*a beneficial tool for both SME and micro enterprise business by providing a mechanism which allows them to achieve data protection compliance in a more cost effective manner*".

  Consequently, the risk is high that industries, including the insurance industry, would refrain from creating codes of conduct if the final guidelines retain mandatory monitoring bodies. Making monitoring bodies mandatory would therefore run against Article 40 of the GDPR and defeat any of the benefits described in Chapter IV that the adoption of a code could bring to the insurance sector.

Recommendation: Insurance Europe calls on the EDPB to consider feasible solutions in line with the GDPR for the monitoring of compliance of codes of conduct, keeping in mind that codes of conduct are an instrument of self-regulation.

- **The lack of economic viability to meet the accreditation requirements for monitoring bodies**

  Where a national association opts to develop a code of conduct and chooses as the main safeguard mechanism the appointment of a monitoring body, the association would then face the recurring costs that meeting certain of the accreditation requirements for monitoring bodies requires. These costs would be in addition to the organisational and financial burden that the drafting process entails in itself. For example, the requirements for independence, conflict of interest and expertise are disproportionate:

  - To meet the criteria on independence the draft guidelines suggest the appointment of an external or an internal monitoring body (pages 20-21). Both types of appointment would imply a burdensome recurring cost for national associations. Moreover, the criteria proposed to demonstrate the independence of internal monitoring bodies is financially excessive (eg, separate staff and management, separate budget and accountability).
  - The requirement to hire separate staff for the monitoring body so to avoid conflicts of interest is also economically excessive.
  - The criteria to fulfil the requirement of expertise of the monitoring body is also unachievable at this stage. This is because: firstly, there is no prior experience with a body of this nature, therefore it is not possible to "*point to previous experience of acting in a monitoring capacity*", as required in paragraph 69 of the draft guidelines. Secondly, there is currently a shortage in the market of data protection experts due to the recent implementation of the GDPR. Therefore, at this stage it is challenging to find data protection experts in the market to fulfil the "expertise" criteria and at a reasonable hiring cost, which national associations could bear.

Recommendation: Insurance Europe urges the EDPB to reconsider the criteria proposed to meet the accreditation requirements for monitoring bodies. The requirements should provide strong safeguards; however, the guidelines should not prevent the adoption of codes of conduct in practice by imposing disproportionate or excessive requirements.

- **The lack of consultation or the possibility to present amendments to a draft code during the approval phase**

  In chapter 7 the draft guidelines describe a three-step approach for the approval of a national code of conduct: (i) *submission* of the draft code to the data protection authority (DPA), (ii) *acceptance* by the DPA; and (iii) approval of the code (after the DPA's assessment of the draft code's content). Throughout this process, the EDBP has not considered the possibility to consult code owners during the approval phase or to facilitate the introduction of amendments if needed, before rejecting a draft code.

  Insurance Europe understands that once a draft code has been *accepted*, and therefore its contents admitted for assessment at the *approval* phase, it is implied that the draft code does not present fundamental flaws. However, it could be the case were the DPA considers that certain amendments may be needed to grant the approval of the code. However, according to the draft guidelines, if this were to be the case, the draft code would be automatically rejected, and the code owner forced to reinitiate the whole process and "*re-submit an updated draft code*".

  The assessment process for the approval of a code should be more dynamic and effective. In this regard, the dialogue between the DPA and the drafting code owners should be permitted and encouraged during the approval phase, allowing consultations or questionnaires from the DPA to the code owners when further clarifications are needed. Moreover, the possibility to amend the draft code during the approval phase under the DPA's guidance should be allowed. Finally, if the provided clarifications or amendments do not satisfy the DPA's criteria, then the approval of the draft code would be rejected.

Recommendation: The draft guidelines should introduce the possibility of consultations between the DPA and the code owners to provide clarifications on the contents of the draft code, when needed. Moreover, the approval phase should allow the possibility for code owners to amend the draft code at the approval phase. This would allow a more effective and balanced process, avoiding the administrative burden and costs of repeating draft code submissions.

- **The lack of a concrete timeframe to approve a code of conduct**

  The draft guidelines establish in paragraph 45 (page 16) that, during the approval process, and in the absence of a national law prescribing the timeline, the DPA shall "*draft an opinion within a reasonable period of time and keep the draft owners regularly updated on the process and indicative timelines"*.

  However, in order to guarantee legal certainty and reduce administrative burden for the code owners, the guidelines should establish the maximum timeframe in which a DPA shall adopt a decision. For example, from the submission of the code to its approval, the timeframe for the DPA to adopt a decision could be of a maximum of three months.

Recommendation: The EDPB should consider establishing a concrete timeframe in which DPAs shall adopt a decision regarding the adoption of a code of conduct. This would ensure a harmonised practice throughout Europe, provide legal certainty and reduce administrative burden by avoiding infinite delays.

- **Comments regarding Appendix 4 (Flow Chart)**

  In Articles 64 (1) (b) and 40 (7), the GDPR establishes that in the case of transnational codes the competent supervisory authority shall, before approving the draft code, submit it to the Board (EDPB), which shall provide an opinion on whether the draft code complies with the GDPR. In other words, in the event of a **transnational code,** the EDPB shall issue an opinion before the approval of the code by the competent DPA.

  The chart in Appendix 4 of the draft guidelines is misleading since it suggests that the EDPB shall issue opinions on the adequacy of both national and transnational codes. Moreover, the draft guidelines do not clarify in any footnote or section that the chart in Appendix 4 only refers to transnational codes. As explained above, and according to Level text 1, the EDPB shall issue an opinion only in the event of a transnational code.

Recommendation: The EDBP should clarify in the final guidelines that the chart in Appendix 4 refers to the approval process of transnational codes, and that an opinion from the EDPB is not required for the approval of national codes by the competent DPA.