



**COUNCIL OF
THE EUROPEAN UNION**

Brussels, 13 February 2013

6413/13

**Interinstitutional File:
2012/0011 (COD)**

LIMITE

**DATAPROTECT 15
JAI 100
MI 107
DRS 24
DAPIX 18
FREMP 11
COMIX 98
CODEC 332**

NOTE

from: German delegation
to: Working Party on Data Protection and Exchange of Information
No. prev. doc.: 5702/13 DATAPROTECT 2 JAI 47 MI 44 DRS 17 DAPIX 6 FREMP 3
COMIX 40 CODEC 155
Subject: Proposal for a new version of Article 38 (Codes of conduct) and for a new Article 38a (Institutions of voluntary self-regulation) of the proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)

1. In an effort firstly to offer controllers and data subjects legal certainty, secondly to respond flexibly to technical developments and specific risks of data processing and thirdly to minimize the number of delegated acts within the Regulation, the German Delegation proposes that the co-regulation instruments already provided for in the General Data Protection Regulation should be strengthened.

2. The German Delegation believes that the proposal for provisions on codes of conduct in Article 38 of the Regulation should be revised with the aim of achieving an appropriate balance between the various interests of stakeholders, enabling the Regulation to be further specified by means of a bottom-up procedure and ensuring the effective implementation of European data protection law based on uniform high standards.
3. Further, the German Delegation believes that codes of conduct should specify, flesh out or supplement the Regulation's provisions for specific sectors, but should not limit them. Due to their function of giving concrete form to legislation, codes of conduct should also be considered as alternatives to delegated or implementing acts of the Commission. However, the essential points must be determined within the Regulation itself.
4. Based on Article 38 of the Regulation, the German Delegation proposes the following new wording:

Article 38

Codes of conduct

- (1) The Member States, the supervisory authorities and the Commission shall encourage the drawing up of codes of conduct in the private sector intended to contribute to the proper application of this Regulation, taking account of the specific features of the various data processing sectors.
- (2) Data controllers, processors or associations thereof may draw up codes of conduct themselves or assign independent bodies to do so for the purpose of framing, specifying or interpreting the provisions of this Regulation with the objective of its uniform implementation. They may refer in particular to the following aspects:
 - a) fair and transparent data processing;
 - b) the collection of data and adherence to purpose;
 - c) the weighing up of interests according to Article 6 (1) (f);

- d) consent according to Article 7;
 - e) information of the public and of data subjects;
 - f) the exercise of the rights of data subjects and their requests made in that regard;
 - g) information and protection of children;
 - h) technical data protection measures according to Article 23 and measures to ensure the security of processing according to Article 30;
 - i) transfer of data to third countries or international organizations;
 - j) mechanisms for monitoring and ensuring compliance with the code by the controllers adherent to it;
 - k) out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with respect to the processing of personal data, without prejudice to the rights of the data subjects pursuant to Articles 73 and 75.
- (3) The procedure for drawing up or amending codes of conduct must conform to general principles of proper procedure and must be published. It must be ensured that the controllers, processors and associations thereof involved represent a majority of the sector in question. Supervisory authorities shall be involved in the procedure. Organizations and associations representing the rights of data subjects and government bodies with responsibility for data security should be given the opportunity to comment if they could be affected by the codes of conduct. National or European standardization bodies may be involved in the procedure.
- (4) Data controllers, processors or associations thereof shall submit proposals for codes of conduct to the European Data Protection Board. The European Data Protection Board shall give an opinion whether the draft code of conduct is in compliance with this Regulation and may recommend the application of the code of conduct. If the European Data Protection Board does not express an opinion within six months of receipt, it shall be deemed to have made such recommendation. Article 58 (8) shall apply *mutatis mutandis*.

- (5) The Commission may adopt implementing acts for deciding that the codes of conduct recommended by the European Data Protection Board pursuant to paragraph 4 and applicable throughout Europe have general validity within the Union.¹ Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87 (2).
- (6) Data controllers, processors or associations thereof shall evaluate the codes of conduct no later than five years after their publication. The results shall be published in a report.
- (7) The European Data Protection Board shall save all codes of conduct in a register and shall publish them in the Official Journal of the European Union and in any other appropriate form. The register shall also indicate which data controllers or processors are bound by the codes of conduct.
- (8) In its supervisory activity, the supervisory authority competent according to Article 51 of this Regulation shall take into account the codes of conduct recommended by the European Data Protection Board pursuant to paragraph 4. Where a data controller or processor has submitted to a code of conduct on which the supervisory authority has based its supervisory activity, the supervisory authority shall only check whether the processing of personal data is in compliance with this code of conduct.
- (9) The rights defined in Articles 73 to 77 of this Regulation shall remain unaffected.

¹ Subject to an exception for codes of conduct for data processing for the purpose of scientific research, which may be anchored in Article 83 or in Article 38 (5) of this Regulation.

Article 38a

Institutions of voluntary self-regulation

- (1) In the private sector, the monitoring of compliance with codes of conduct pursuant to Article 38 may be conducted by institutions of voluntary self-regulation (institution) accredited at the recommendation of the European Data Protection Board by the competent supervisory authority according to Article 51 of this Regulation. An institution may be accredited for this purpose if
 - a) the independence and expertise of its designated auditors is guaranteed and appropriate provision is guaranteed by means of a variety of data controllers, processors or associations thereof,
 - b) the powers referred to in Article 53 have been invested in them,
 - c) rules of procedure have been established which make provision regarding the extent of the review, effective sanctions and the possibility to review decisions,
 - d) it is guaranteed that the data controllers or processors or, in the event of complaints being lodged at least one complainant, are heard before a decision is taken, the decision is taken in writing and those involved are informed thereof, and
 - e) a complaints department has been established.
- (2) Where a data controller or processor submits to an accredited institution, that institution shall investigate violations of the code of conduct. Where there is evidence that a data controller or a processor has violated a code of conduct by which he is bound, the institution shall initiate proceedings.
- (3) Measures taken by the supervisory authority against the data controller or processor shall be permissible if the institution, despite evidence of violations of approved codes of conduct, does not act or oversteps its margin of discretion, or the data controller or processor does not cease the violation despite the measures taken by the institution.
- (4) The rights defined in Articles 73 to 77 of this Regulation shall remain unaffected.

- (5) Where an institution does not fulfil its tasks in a specific instance, the supervisory authority competent according to Article 51 of this Regulation may lodge complaints against the institution. Accreditation may be revoked in full or in part if the conditions for accreditation are no longer met or the institution's decisions do not guarantee that the objectives of this Regulation will be fulfilled.
5. Further explanations regarding the proposed wording:

Re Article 38

Paragraph 1 establishes a general obligation for Member States, supervisory authorities and the Commission to create an environment favourable to sector-specific self-regulation.¹ Especially the consultation procedures with data controllers, processors and associations thereof ensure that they can work to include issues relevant for the proper and coherent application of the Regulation in proposals for codes of conduct. Issues of general relevance should be included in the Regulation itself.

Paragraph 2 first sentence makes clear that codes of conduct give more specific form and elaborate on the more general provisions of the Regulation. They are to be drawn up with the aim of Europe-wide implementation in order to contribute to the harmonized application of the law. The possibility of drawing up national codes of conduct continues to exist. The second sentence lists examples of areas to which codes of conduct may refer.²

¹ Paragraph 1 largely corresponds to Article 38 (1) General Data Protection Regulation (draft).
² Paragraph 2 second sentence is largely based on the proposed list in Article 38 (1) General Data Protection Regulation (draft).

Paragraph 3 specifies the requirements for the procedure to draw up the codes of conduct (Step 1). It must conform to general principles of proper procedure and must, in particular, guarantee that members of the supervisory authorities are involved. The supervisory authorities involved will have no veto during the drafting of codes of conduct. The supervisory authorities involved should be chosen in consultation with the European Data Protection Board and should regularly inform the Board about progress on the drafting of the code. Interested groups, especially organizations and associations representing the interests of data subjects, must be given the opportunity to represent their interests, for example by submitting statements or in the context of hearings.

By involving the national and European standardization institutions, for example the European Committee for Standardization (CEN), tried and tested and transparent procedures can serve as a reference when drafting codes of conduct. In any case, those involved in drafting codes should have suitable discretion when choosing the procedure, as long as it satisfies the requirements listed in this paragraph.

Self-regulation according to Article 38 must not interfere with established national and international procedures for technical standardization.

Paragraph 4 defines the procedure for data protection supervisory authorities to review codes of conduct that have been drawn up (Step 2). To ensure a uniform evaluation of codes of conduct, they are presented to the European Data Protection Board to check whether they are in compliance with the provisions of the Regulation. Members of the European Data Protection Board include the European Data Protection Supervisor and the national supervisory authorities, which in this way are involved in checking the codes of conduct. This gives the data protection supervisory authorities an important role in the procedure.¹

The European Data Protection Board provides an opinion on the codes of conduct presented to it and recommends their application. This procedure applies to codes of conduct applicable both Europe-wide and at national level in order to ensure consistent interpretation of the Regulation.

¹ For codes of conduct, at European level, the Commission's proposal only provides for approval by the Commission and gives no further role to the data protection supervisory authorities.

The reference to Article 58 (8) of the Regulation ensures that the competent supervisory authorities take the opinion of the European Data Protection Board into account.

The procedure has been designed to avoid lengthy examination and the associated lack of legal certainty for stakeholders. If the European Data Protection Board does not issue an opinion within six months, it will be deemed to have recommended the codes of conduct presented to it. Introducing a time-limit and a legal fiction of approval may expedite the procedure and thus establish legal certainty as soon as possible. In this way, the position of the data protection authorities is taken into consideration, as they are involved in the process of drafting the codes of conduct already at an early stage.

Paragraph 5 takes up the possibility provided in the Commission's proposal to declare codes of conduct applicable Europe-wide to have general validity within the Union.¹ This declaration of general validity is made conditional upon the new provision that the codes of conduct have first been examined and recommended by the European Data Protection Board according to paragraph 4.

With regard to the declaration of general validity, it is necessary to ensure in particular that the interests of small and medium-sized enterprises as well as research units which process personal data for purposes of scientific research are sufficiently taken into account.

Paragraph 6 contains the obligation to regularly evaluate codes of conduct in order to be able to take account of subsequent changes. The results of the evaluation will be published.

Paragraph 7 takes account of the requirement that rules which give concrete form to the provisions of the Regulation must be published. This enables all groups concerned to find out which data protection provisions are binding in a specific sector.

¹ Cf. Article 38 (4) General Data Protection Regulation (draft).

Paragraph 8 makes allowance for the fact that a key incentive for data controllers to participate in self-regulation is that by doing so they can give concrete form to the provisions of the Regulation and that this concrete form then applies to the competent national supervisory authorities as well. The wording "take into account" should be put into practice in such a way that the national competent supervisory authorities may determine through a decision whether, in their view, the codes of conduct recommended by the European Data Protection Board according to paragraph 4 satisfy the requirements of data protection law as given in the Regulation.

Paragraph 9 makes clear that the supervisory authorities' being bound to the outcomes of self-regulatory processes is limited by a judicial review of the specification of the provision.

Re Article 38a

Paragraphs 1 through 5 are based on the idea that the incentive to self-regulate is stronger if it is left primarily to the self-regulating enterprises to monitor and ensure compliance with the codes of conduct. That is why data controllers are given the possibility to establish institutions of voluntary self-regulation. These are to be accredited at the recommendation of the European Data Protection Board by the competent supervisory authority according to Article 51 of this Regulation, if the conditions specified in paragraph 1 second sentence are met. There are good experiences with the instrument of voluntary self-regulation in the area of the protection of minors.
