Inhalt

Self-Regulation and Certification

Current problems with self-regulation: Numerous approaches for self-regulation (binding corporate rules, accountability, data protection officer, codes of conduct, etc.) do already exist. However, there is no systematic development of the instrument of codes of conduct. The current European data protection law provides already a basis for codes of conduct as legal instrument in Article 27 of the Data Protection Directive; however, their approval by data protection authorities has been handled insufficiently and has only been successful in very few cases.

Example: *In Germany we have only two officially recognized codes of conduct so far. This is because the necessary informal alignment processes of the (in Germany 17) supervisory authorities are extremely cost- and time consuming. Additionally, criteria for the recognition of such codes are rather vague and not transparent. It is also unclear whether the recognition of one supervisory authority is binding for the others and which legal consequences a recognition generally causes.*

Not only in Germany but also in other Member States there are very few successful examples of codes of conduct based on Art. 27 of the Directive.

In order to avoid previous insecurities we have had so far, this Regulation should provide explicit rules for the following topics:

- **Legal procedures for the clarification of controversial legal questions:** If the approval is denied or if the supervisory body in charge does not become active, legal procedures for the clarification of controversial legal questions are required. At the same time, the legal means for judicial review of the decision need to be installed. Furthermore, the data protection authority might get a conflict of interest through the exercise of different tasks like certification and its general supervisory role.

- **Monitoring body**: Self-regulation is supposed to concretise the legal framework without necessarily going beyond that. The Regulation should give associations or other professional bodies a right to get a code of conduct approved by the competent supervisory authority in adequate time, if it complies with the provisions of the Regulation. The supervisory authority itself should only publish general criteria regarding the self-regulation process.

Principles:

- **Legal certainty:** More legal certainty and/or reduced risk of sanctions imposed by supervisory bodies by joining a code of conduct. This needs a stringent interpretation of the law by the different supervisory authorities as well as mechanisms for conflict resolution for the clarification of controversial legal issues that do not make specific companies a public example.

- **Reduction of complexity:** Acceptance of (possibly certified) self-regulation by supervisory bodies and customers as proof of correct implementation of necessary data protection measures (in accordance with § 11 II 4 Federal Data Protection Act).

- **Cost control:** Costs for self-regulation have to be in proportion to the benefits gained by the companies by joining the cause of self-regulation.

- **No special option for single nations:** Self-regulation should be recognized within Europe and - ideally - internationally. It is not supposed to come on top of the legal provisions, but to make them more concrete.

- **Right to approval**: Associations and other bodies mentioned in Art. 38a should get a right to obtain the approval of a code of conduct if it corresponds to the legal requirements. The approval should lead to a rebuttable presumption of conformity with the Regulation for those companies which signed the respective code of conduct and are compliant with it.

Article 38 and 38a:

Bitkom supports the Council text in Article 38 GDPR.

Generally, Bitkom would welcome an approach whereby the European Data Protection Board would take binding decisions on the recognition of code of conducts. This would lead to a streamlined process and lead to more harmonization. In contrast, we oppose an approach as laid down in Article 38 IV whereby the Commission may declare a general validity for voluntary codes of conduct. This is likely to discourage associations and other bodies mentioned in Art. 38 1a) to develop or suggest codes of conduct. Instead of discouraging self-regulation processes the EU should introduce incentives for companies and associations to engage in self-regulation. Such an incentive would be the introduction of a rebuttable presumption of conformity with the Regulation for those companies which signed an approved code of conduct and are compliant with it. This mechanism has been introduced for technical standards by the EU and works very well. This proof of concept should be sufficient to apply the same mechanism to codes of conduct.

Arguments and recommendations are laid down in more detail in the attached paper (Braunmühl, Ansätze zur Ko-Regulierung in der Datenschutz-Grundverordnung).

EP Version Article 38	Council Version Article 38	Bitkom Suggestions:
1. The Member States, the supervisory authorities and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various data processing sectors, in particular in relation to:	1. The Member States, the supervisory authorities, *the European Data Protection Board* and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various data processing sectors~~, in particular in relation to:~~ *and the specific needs of micro, small and medium-sized enterprises*.	
2. Associations and other bodies representing categories of controllers or processors in one Member State which intend to draw up codes of conduct or to amend or extend existing codes of conduct may submit them to an opinion of the supervisory authority in that Member State. The supervisory	2. Associations and other bodies *referred to in paragraph 1a* ~~representing categories of controllers or processors in one Member State~~ which intend to ~~draw up~~ *prepare a* code~~s~~ of conduct or to amend or extend an existing code~~s~~, ~~of conduct may~~ *shall* submit the~~m~~ ~~to an opinion of~~ *draft code to* the	**Bitkom strongly suggests that submitting codes of conduct to the competent supervisory authority and asking for their approval should remain voluntary. Codes of conduct may have an added value without any official approval.** **Suggested wording**: *Associations and other bodies referred to in paragraph 1a which intend to prepare a code of conduct or to amend or extend an existing code, **may** submit the draft code to the supervisory authority which is competent pursuant to Article 51. The supervisory authority shall give an opinion on whether the draft code, or amended or extended code is in compliance with this Regulation and shall approve such draft, amended or extended code if it finds that it provides sufficient appropriate safeguards.*
authority may give an opinion whether the draft code of conduct or the amendment is in compliance with this Regulation. The supervisory authority shall seek the views of data subjects or their representatives on these drafts.	supervisory authority ~~in that Member State~~ *which is competent pursuant to Article 51*. The supervisory authority ~~may~~ *shall* give an opinion *on* whether the draft code, *or amended or extended code* ~~of conduct or the amendment~~ is in compliance with this Regulation *and shall approve such draft, amended or extended code if it finds that it provides sufficient appropriate safeguards*. ~~The supervisory authority~~	

	~~shall seek the views of data subjects or their representatives on these drafts.~~	
	2a. Where the opinion referred to in paragraph 2 confirms that the code of conduct, or amended or extended code, is in compliance with this Regulation and the code is approved, and if the code of conduct does not relate to processing activities in several Member States, the supervisory authority shall register the code and publish the details thereof.	
	2b. Where the draft code of conduct relates to processing activities in several Member States, the supervisory authority competent pursuant to Article 51 shall, before approval, submit it in the procedure referred to in Article 57 to the European Data Protection Board which shall give an opinion on whether the draft code, or amended or extended code, is in compliance with this Regulation or, in the situation referred to in paragraph 1ab, provides appropriate safeguards.	**Suggested Wording:** *2b. Where the draft code of conduct relates to processing activities in several Member States, the supervisory authority competent pursuant to Article 51 shall, before approval, submit it in the procedure referred to in Article 57 to the European Data Protection Board which shall* ***take a binding decision*** *on whether the draft code, or amended or extended code, is in compliance with this Regulation or, in the situation referred to in paragraph 1ab, provides appropriate safeguards.*
3. Associations and other bodies representing categories of controllers in several Member States may submit draft codes of conduct and amendments or extensions to existing codes of conduct to the Commission.	3. ~~Associations and other bodies representing categories of controllers in several Member States may submit draft~~ *Where the opinion referred to in paragraph 2b confirms that the* code~~s~~ of conduct, ~~and~~ *or* amend~~ments~~*ed* or extensions*ded*~~ to existing~~ code~~s~~, ~~of conduct to the Commission~~ *is in compliance with this Regulation, or, in the situation referred to in paragraph 1ab, provides appropriate safeguards, the European Data Protection Board shall submit its opinion to the Commission.*	
4. The Commission may adopt implementing acts for deciding that the codes of conduct and amendments or extensions to existing codes of conduct submitted to it pursuant to paragraph 3 have general validity within the Union. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).	4. The Commission may adopt implementing acts for deciding that the *approved* codes of conduct and amendments or extensions to existing *approved* codes of conduct submitted to it pursuant to paragraph 3 have general validity within the Union. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).	**Suggested Wording:** *The Commission may adopt implementing acts for deciding that the approved codes of conduct and amendments or extensions to existing approved codes of conduct submitted to it pursuant to paragraph 3 have general validity within the Union* ***as far as they establish a rebuttable presumption of compliance with this Regulation for economic operators which signed such a code of conduct and are compliant with it.*** *Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).*

5. The Commission shall ensure appropriate publicity for the codes which have been decided as having general validity in accordance with paragraph 4.	5. The Commission shall ensure appropriate publicity for the *approved* codes which have been decided as having general validity in accordance with paragraph 4.	
	5a. The European Data Protection Board shall collect all approved codes of conduct and amendments thereto in a register and shall make them publicly available through any appropriate means, such as through the European E-Justice Portal.	

Council Version Article 38a	**Bitkom Suggestions:**
1. Without prejudice to the tasks and powers of the competent supervisory authority under Articles 52 and 53, the monitoring of compliance with a code of conduct pursuant to Article 38 (1b), 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 this purpose by the competent supervisory authority.	
4. Without prejudice to the provisions of Chapter VIII, a body referred to in paragraph 1 may, subject to adequate safeguards, take appropriate action in cases of infringement of the code by a controller or processor, including suspension or exclusion of the controller or processor concerned from the code. It shall inform the competent supervisory authority of such actions and the reasons for taking them.	**Suggested addition to paragraph 4:** *The competent supervisory authorities will not take action against signees of an approved code to enforce articles of the regulation that are covered by the code of conduct as long as the self-regulatory body enforces the code effectively and does not exceed its scope of judgment.*
	Suggested new paragraph:

Article 39 a

Bitkom supports the Council text due to the above-mentioned problems and opposes the EP approach.

Council Version Article 39 a	Bitkom comments:
1. Without prejudice to the tasks and powers of the competent supervisory authority under Articles 52 and 53, the certification shall be issued and renewed by a certification body which has an appropriate level of expertise in relation to data protection. Each Member State shall provide whether these certification bodies are accredited by:	Bitkom does not support the EP approach which states that certification shall be issued and renewed by a supervisory authority. Supervisory authorities should specify criteria for certification but not certify themselves as this may lead to conflicts of interests on the side of the supervisory authorities. This could e.g. be the case if the authority has to deal with a complaint about a product or company the authority has earlier certified.