Stellungnahme

Verankerung von Selbstregulierung im Datenschutz in der EU-Datenschutz-Grundverordnung
13. März 2013

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. vertritt mehr als 1.700 Unternehmen, davon über 1.100 Direktmitglieder mit etwa 135 Milliarden Euro Umsatz und 700.000 Beschäftigten. Hierzu zählen Anbieter von Software & IT-Services, Telekommunikations- und Internetdiensten, Hersteller von Hardware und Consumer Electronics sowie Unternehmen der digitalen Medien. Der BITKOM setzt sich insbesondere für eine Modernisierung des Bildungssystems, eine innovative Wirtschaftspolitik und eine zukunftsorientierte Netzpolitik ein.

Der Verband Selbstregulierung Informationswirtschaft e.V. wurde im August 2011 von Unternehmen der Internetbranche und dem ITK-Verband BITKOM gegründet, um den Verbraucher- und Datenschutz im Internet durch Instrumente der Selbstregulierung zu fördern und damit der gesellschaftlichen Verantwortung der informationsverarbeitenden Wirtschaft gerecht zu werden. Die Einhaltung eingebrachter Verhaltenskodizes wird kontinuierlich überwacht und ein unabhängiger Beschwerdeausschuss kann bei Verstößen Sanktionen festlegen.

Zusammenfassung

Selbstregulierung innerhalb eines geeigneten gesetzlichen Rahmens ist ein gutes Instrument, um das Vertrauen von Kunden und Nutzern in den Schutz ihrer Persönlichkeitsrechte in einem Geschäftsfeld hoher Heterogenität und Dynamik dauerhaft zu erhalten. Sie soll die ordnungsgemäße Anwendung datenschutzrechtlicher Regelungen fördern, indem sie sie konkretisiert, erläutert oder auf andere Weise ihre Um- und Durchsetzung erleichtert. Die momentan in Arbeit befindliche EU-Datenschutz-Grundverordnung enthält bereits erste Ansätze, die Selbstregulierung im Datenschutz vorsehen. Diese Möglichkeit sollte genutzt und in den nächsten Monaten über die mögliche Weiterentwicklung und Ausgestaltung der im Entwurf angelegten Regelungen nachgedacht werden. Dabei sollten die folgenden Aspekte berücksichtigt werden:

- Vor dem Hintergrund grenzüberschreitender Kommunikation und international ausgerichteter Geschäftsmodelle sollten gerade im Datenschutz europäische Standards geschaffen werden, die möglichst mit Selbstregulierungs-Ansätzen in Drittstaaten kompatibel sind. Denn in vielen Bereichen wären globale Selbstregulierungsansätze wünschenswert, um einen fairen Wettbewerb und effektive Datenschutzstandards zu erreichen.

- Selbstregulierung muss das Vertrauen der Beteiligten fördern. Die Verfahren zur Festlegung von Kodizes und ihrer Durchsetzung müssen so gestaltet werden, dass den Beteiligten die eingegangenen Verpflichtungen mit hoher Transparenz dargelegt werden und dass sie zuverlässig durchgesetzt werden können. Für Unternehmen sollte die Umsetzung der Selbstverpflichtungen und deren Nachweis mit angemessenem Aufwand möglich sein.

- Selbstregulierung muss flexibel auf die sich in der Informationsgesellschaft dynamisch weiterentwickelnden Gegebenheiten reagieren können. Sie muss branchenspezifische Regelungen unterstützen und Unternehmen Anreize bieten, sich zu beteiligen.

- Selbstregulierung muss wachstumsfördernd wirken, indem sie die Rechtssicherheit für die Beteiligten erhöht und die Anwendung internationale Standards unterstützt.

1 Ziele:

Selbstregulierung dient der Erreichung gesellschafts- und wirtschaftspolitischer Ziele. Eine klare Definition dieser Ziele für die Entwicklung eines gesetzlichen Rahmens ist unabdingbar. BITKOM und SRIW definieren drei Ziele für eine Selbstregulierung im Datenschutz:

- **Schutz und Vertrauen**: Vertrauen ist Voraussetzung für Datenverarbeitung. Selbstregulatorische Ansätze sind nur dann sinnvoll, wenn sie ein angemessenes Schutzniveau realisieren und Vertrauen schaffen.

- **Flexibilisierung**: Der Datenschutz muss von Spezial- und Detailregelungen absehen und flexible Regelungen ermöglichen, innerhalb derer auf den technischen Wandel in angemessener Zeit reagiert werden kann.

- **Wachstumsförderung durch Rechtssicherheit und internationale Standards**: Datenschutz ist auch Standortpolitik – Rechtssicherheit und europäische bzw. internationale Standards würden insbesondere das Wachstum von mittelständischen IT-Unternehmen fördern.

2 Erfolgsfaktoren:

- **Anreize**
  Das System der Selbstregulierung muss Anreize für Unternehmen bieten, sich an Selbstregulierung zu beteiligen, damit diese bereit sind, den Aufwand der Selbstregulierung zu tragen und sich zu beteiligen. Diese Anreize können z.B. sein: ein substantielles Mehr an Rechtssicherheit, Reduzierung oder Vereinfachung administrativer Pflichten etc.

- **Akzeptanz**
  Das System der Selbstregulierung muss europaweite Akzeptanz durch die Aufsichtsbehörden finden. Ohne konstruktive Zusammenarbeit zwischen Aufsichtsbehörden/Datenschutzausschuss und den beteiligten Unternehmen können keine zügigen Lösungen gefunden werden.

- **Flexibilität**
  Die Verfahren für die Erstellung von Kodizes müssen auf Effektivität und Flexibilität ausgerichtet. Sie müssen dem jeweiligen Sachverhalt angemessen und schlank genug sein, um rechtzeitig auf neue Entwicklungen reagieren zu können.

- **Kompatibilität**
  Das System sollte so ausgestaltet sein, dass es auch für internationale Unternehmen mit Hauptsitz außerhalb Europas interessant ist, sich Selbstverpflichtungen anzuschließen. Die geschaffenen Standards sollten möglichst internationale Standards unterstützen bzw. weiterentwickeln.

3 Vorschläge zur Ausgestaltung von regulierter Selbstregulierung im Datenschutz

3.1 Verfahren bis zur Anerkennung eines Kodex

Aus den Erfahrungen mit § 38a BDSG und dem Ansatz, die Selbstregulierung in die EU-Datenschutz-Grundverordnung einzubeziehen, ergeben sich folgende Vorschläge für das Verfahren der Einrichtung einer neuen Selbstverpflichtung/ eines neuen Kodex:

- Schaffung eines Anspruchs für Unternehmensvereinigungen auf Genehmigung eines den gesetzlichen Vorgaben entsprechenden Kodex in angemessener Frist durch die zuständige Aufsicht.

- Gerichtliches Verfahren bei Ablehnung der Genehmigung oder Untätigkeit der zuständigen Aufsicht zur Klärung der streitigen Rechtsfragen. Rechtsmittel zur rechtlichen Überprüfung der Entscheidung.

3.1.1 Verfahrensgrundsätze

- Europäische oder nationale Vereinigungen erarbeiten (möglichst im Dialog mit der zuständigen Aufsichtsbehörde oder dem Europäischen Datenschutzausschuss) einen Kodex. Es sollten hier nicht zu enge Vorgaben gemacht werden, welche Vereinigungen antragsberechtigt sind. Auch zur Anzahl der beteiligten Unternehmen o.ä. sollte es keine Vorgabe geben, da sonst der Effekt verhindert werden könnte, dass wenige „First Movers“ den Rest des Marktes zu besseren Datenstandards treiben können. Es sollte aber grundsätzlich jedem Unternehmen die Möglichkeit gegeben werde, an der Erstellung einer Selbstverpflichtung mitzuwirken, auch wenn es kein Mitglied der Vereinigung ist. Damit schließt man kartellrechtliche Probleme weitgehend aus und erhöht die Akzeptanz unter den Unternehmen einer Branche. Unternehmen, die nicht von Anfang an die Möglichkeit zur Mitwirkung an der Erstellung einer Selbstverpflichtung hatten, könnten Probleme haben, eine solche Selbstverpflichtung zu akzeptieren.

- Für die Anerkennung sollten grundsätzlich die Aufsichtsbehörden zuständig sein. Bei länderübergreifenden Selbstverpflichtungen sollte in jedem Fall der Europäische Datenschutz-Ausschuss zuständig sein. Bei nationalen Verpflichtungen gibt es zwei Alternativen: Entweder erkennt ebenfalls der Europäische Datenschutz-Ausschuss den Kodex an, sofern er den gesetzlichen Vorgaben entspricht, (Variante 1) oder die für die Vereinigung zuständige Datenschutzaufsicht tut dies und gibt den übrigen europäischen Aufsichtsbehörden Gelegenheit zur Stellungnahme im Rahmen des in der Verordnung festzulegenden Kohärenz-Verfahrens (Variante 2).

- Wenn der Europäische Datenschutz-Ausschuss bzw. die zuständige Aufsicht einen Kodex oder eine Selbstkontrollinstanz anerkannt hat, gelten sie auch von den übrigen Aufsichtsbehörden als anerkannt bzw. werden sie von diesen akzeptiert.

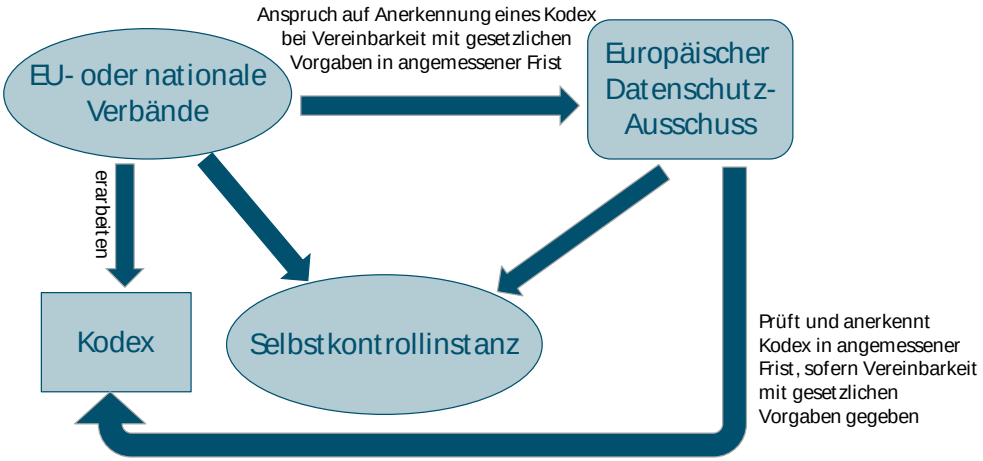
- Die vorlegende Vereinigung hat einen Anspruch auf Anerkennung in angemessener Frist, sofern die Vereinbarkeit mit den gesetzlichen Vorgaben gegeben ist. Ein ähnlicher Anspruch ist im Entwurf der Datenschutz-Grundverordnung in Art. 74 bereits angelegt.

- Um sicher zu stellen, dass auch die Perspektive der Nutzer und anderer möglicherweise von einem Kodex betroffenen Interessengruppen berücksichtigt werden kann, ist zu erwägen, eine Anhörungspflicht bzw. ein Recht zur Stellungnahme für die betroffenen Interessengruppen vorzusehen. Die Ergebnisse einer solchen Anhörung bzw. die eingegangenen Stellungnahmen könnten dann dem Datenschutz-Ausschuss bzw. der zuständigen Aufsichtsbehörde zusammen mit dem Antrag auf Anerkennung zugänglich gemacht werden und von dieser gegebenenfalls berücksichtigt werden. Alternativ könnte dieses Verfahren auch direkt beim Europäischen Datenschutz-Ausschuss bzw. der Aufsicht (wie bereits in Art. 38 Abs. 2 S.2 des Entwurfs angedeutet) angesiedelt werden.

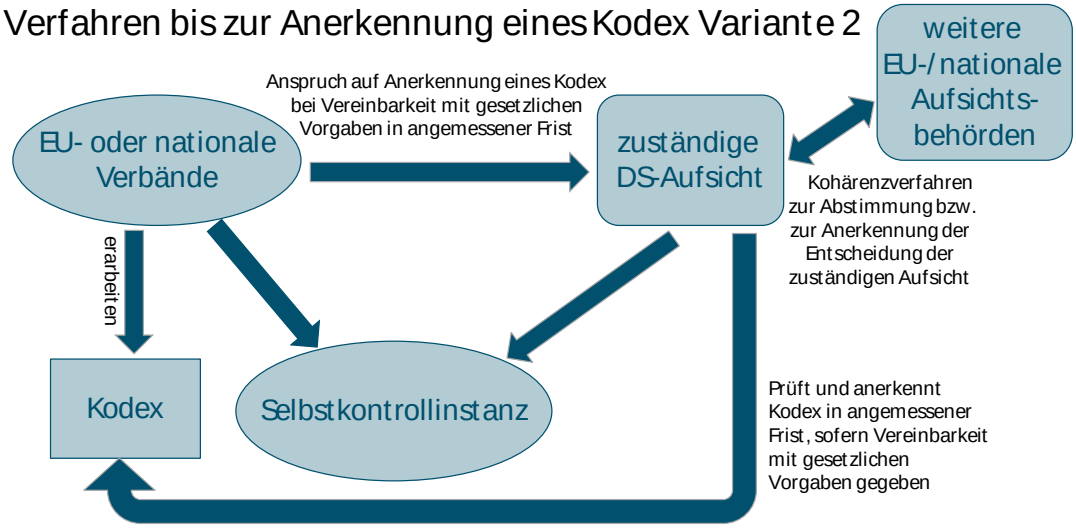
- Wird zum Zweck der Kontrolle und Durchsetzung der Selbstverpflichtung eine Selbstkontrollinstanz eingerichtet, so muss auch diese vom Datenschutz-Ausschuss oder der zuständigen Aufsicht anerkannt werden. Dafür sollten im Gesetz bestimmte Kriterien festgelegt werden, die eine solche Selbstkontrollinstanz erfüllen muss, um anerkannt werden zu können. Das könnten zum Beispiel Ansprüche an eine bestimmte Ausstattung, Sachkompetenz, Neutralität, Verfahren etc. sein. Liegen diese Voraussetzungen vor, muss die zuständige Aufsicht auch die Selbstkontrollinstanz in angemessener Frist anerkennen.

- Selbstverpflichtungen sollten grundsätzlich befristet sein und gegebenenfalls eine regelmäßige Evaluation vorsehen, um sicher zu stellen, dass die Regelungen immer noch den möglicherweise geänderten Gegebenheiten entsprechen.

Verfahren bis zur Anerkennung eines Kodex Variante 1



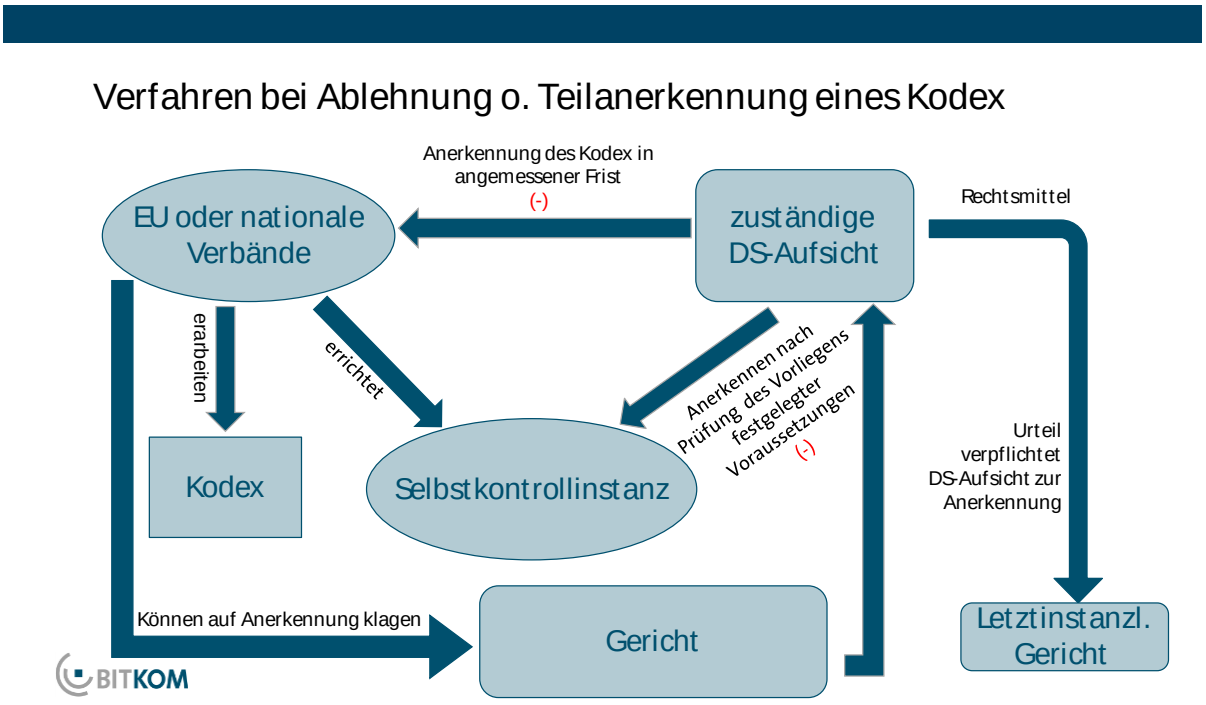
Verfahren bis zur Anerkennung eines Kodex Variante 2



3.1.2 Verfahren bei Ablehnung oder Teilanerkennung eines Kodex

- Ist die zuständige Aufsichtsbehörde der Meinung dass ein zur Anerkennung vorgelegter Kodex oder ein Teil davon nicht den gesetzlichen Vorgaben entspricht, lehnt sie die Anerkennung des Kodex mit einer entsprechenden Begründung ab oder erkennt ihn (sofern das sinnvoll möglich ist) nur teilweise an.

- Die vorlegende Vereinigung kann nun ihren Anspruch auf Anerkennung des Kodex in einem (evtl. beschleunigten) gerichtlichen Verfahren geltend machen. Sieht das Gericht den Anspruch als gegeben an, bindet das Urteil die Aufsichtsbehörde. Sie kann jedoch Rechtsmittel gegen das Urteil einlegen.



3.2 Kontrolle und Durchsetzung eines Kodex

Ist ein Kodex anerkannt, gibt es verschiedene Möglichkeiten zur Kontrolle im Rahmen der Selbstverpflichtung, welche bereits im Kodex selbst festgelegt und im gesetzlichen Rahmen vorgesehen sein sollten. Je nach zu regelndem Sachverhalt und gewünschter Verbindlichkeit gibt es verschieden geeignete und unterschiedlich aufwändige Instrumente zur Kontrolle und Durchsetzung der vereinbarten Regelungen. Hier braucht es einen Spielraum, um die Sensibilität und Bedeutung der Regelungsmaterie sowie ihren Charakter (z.B. eher technisch oder eher ethisch) angemessen berücksichtigen zu können. Die Verordnung sollte daher verschiedene Modelle der Kontrolle und Durchsetzung zulassen und lediglich vorschreiben, welchen Anforderungen diese genügen sollen.

Denkbar sind z.B. die im Folgenden skizzierten Modelle, welche unterschiedliche Vor- und Nachteile aufweisen, aber alle einen relativ hohen Verbindlichkeitsgrad erfüllen und gleichzeitig Anreize für die beteiligten Unternehmen setzen.

- **Modell I**: Kontrolle und Durchsetzung der Selbstverpflichtung durch eine anerkannte Selbstkontrollinstanz, die auch ein Beschwerdeverfahren anbietet. Aufsicht greift nur bei Versagen der Selbstkontrolle.

- **Modell II**: Kontrolle durch Prüfungen unabhängiger Dritte und Durchsetzung durch Aufsichtsbehörde. Die Prüfung von Verstößen und die Durchsetzung von Sanktionen bei Verstößen obliegt den Aufsichtsbehörden. Unternehmen können die Einhaltung technischer Anforderungen oder vorgeschriebener Prozesse von anerkannten Prüfinstituten zertifizieren lassen. Bei Vorliegen einer aktuellen Zertifizierung ist nicht von einem Verschulden des Unternehmens auszugehen, sofern ein Verstoß festgestellt wird, der in den Prüfungsrahmen dieser Zertifizierung fällt.

- **Modell III**: Kontrolle durch Prüfung unabhängiger Dritte im Auftrag einer anerkannten Selbstkontrollinstanz, die auch durchsetzt. Aufsicht greift nur bei Versagen der Selbstkontrolle.

Der zu setzende Rechtsrahmen sollte Spielraum für das zum jeweiligen Sachverhalt passende Instrumentarium lassen.

4 Verankerung von Selbstregulierung und Zertifizierung in der EU-Datenschutz-Grundverordnung

Damit die aufgezeigten Selbstregulierungsmechanismen funktionieren, benötigen sie eine gesetzliche Verankerung in der Datenschutz-Grundverordnung. Dazu schlagen wir die im Folgenden dargestellten Änderungen am vorgelegten Verordnungsentwurf vor. Die Formulierungsvorschläge setzen die oben genannte Variante 1 mit dem Europäischen Datenschutz-Ausschuss als anerkennende Stelle um.

4.1 Verfahren

Art. 38 Codes of Conduct

Commission Proposal	**BITKOM and SRIW Proposal**
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: (a) fair and transparent data processing; (b) the collection of data; (c) the information of the public and of data subjects; (d) requests of data subjects in exercise of their rights; (e) information and protection of children; (f) transfer of data to third countries or international organizations; (g) mechanisms for monitoring and ensuring compliance with the code by the controllers adherent to it; (h) 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.	…

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 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.	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 ***can ask*** ~~may submit them to an opinion of~~ ***the European Data Protection Board*** ~~the supervisory authority in that Member State~~ ***to confirm the compliance with this Regulation***. The European Data Protection Board or supervisory authority ~~may give an opinion~~ ***shall declare in reasonable time*** 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.
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~~ ***can ask the European Data Protection Board to confirm the compliance of*** draft codes of conduct and amendments or extensions to existing codes of conduct to the Commission ***with this Regulation***. ***The European Data Protection Board shall declare in reasonable time whether the draft code of conduct or the amendment is in compliance with this Regulation. The European Data Protection Board shall seek the views of data subjects or their representatives on these drafts.***
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).	
5. The Commission shall ensure appropriate publicity for the codes which have been decided as having general validity in accordance with paragraph 4.	

Art. 38a new Self-regulatory Bodies

1. If a code of conduct sets up a self-regulatory body in order to enforce the provisions of this code with the signees, the Associations or other bodies representing categories of controllers or processors who set up the code may ask the European Data Protection Board to approve this self-regulatory body as competent self-regulatory body.
2. Conditions for approval are:
    a. Proof of sufficient expertise,
    b. Sufficient financial means for the time of planned validity of the code,
    c. Transparent processes that ensure fair and neutral decisions in cases of breach,
    d. Hearing right for signees before a decision.
    e. Erection of a body where complaints can be filed.

3. Self-regulatory bodies that have not been approved by the competent supervisory authority or the European Data Protection Board can appeal against the decision at the competent court.
4. Self-regulatory bodies that have been approved by the competent supervisory authority are competent to enforce all regulations laid down in the code with the signees. 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..

Art. 39 Certification

1. The Member States and the Commission shall encourage, in particular at European level, the establishment of data protection certification mechanisms and of data protection seals and marks, allowing data subjects to quickly assess the level of data protection provided by controllers and processors. The data protection certifications mechanisms shall contribute to the proper application of this Regulation, taking account of the specific features of the various sectors and different processing operations.	1. The Member States and the Commission shall encourage, in particular at European level, the establishment of data protection certification mechanisms**, including self-certification mechanisms,** and of data protection seals and marks**, which shall be capable of global application, affordable and technology neutral,** allowing data subjects to quickly assess the level of data protection provided by controllers and processors. The data protection certifications mechanisms shall contribute to the proper application of this Regulation, taking account of the specific features of the various sectors and different processing operations. **They shall be elaborated based on industry-led efforts and in consultation with the supervisory authorities.**

2. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the data protection certification mechanisms referred to in paragraph 1, including conditions for granting and withdrawal, and requirements for recognition within the Union and in third countries.	
3. The Commission may lay down technical standards for certification mechanisms and data protection seals and marks and mechanisms to promote and recognize certification mechanisms and data protection seals and marks. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).	

4.2 Änderungsvorschläge, die den Zusammenhang Auftragsdatenverarbeitung und Zertifizierung/Selbstverpflichtung betreffen:

Recital 61, Art. 22 und Art. 26

Recital 61 The protection of the rights and freedoms of data subjects with regard to the processing of personal data require that appropriate technical and organizational measures are taken, both at the time of the design of the processing and at the time of the processing itself, to ensure that the requirements of this Regulation are met. In order to ensure and demonstrate compliance with this Regulation, the controller should adopt internal policies and implement appropriate measures, which meet in particular the principles of data protection by design and data protection by default.	***Recital 61*** The protection of the rights and freedoms of data subjects with regard to the processing of personal data require that appropriate technical and organizational measures are taken, both at the time of the design of the processing and at the time of the processing itself, to ensure that the requirements of this Regulation are met. In order to ensure and demonstrate compliance with this Regulation, the controller should adopt internal policies and implement appropriate measures, which meet in particular the principles of data protection by design and data protection by default***. The controller is deemed to have implemented such appropriate technical and organizational measures when employing a processor who has voluntarily self-certified or voluntarily obtained a third party certification, seal or mark showing the implemen-***

	tation of appropriate standard technical and organizational measures in response to the requirements set out in this Regulation.
Article 22 1. The controller shall adopt policies and implement appropriate measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation. 2. The measures provided for in paragraph 1 shall in particular include: (a) keeping the documentation pursuant to Article 28; (b) implementing the data security requirements laid down in Article 30; (c) performing a data protection impact assessment pursuant to Article 33; (d) complying with the requirements for prior authorisation or prior consultation of the supervisory authority pursuant to Article 34(1) and (2); (e) designating a data protection officer pursuant to Article 35(1). 3. The controller shall implement mechanisms to ensure the verification of the effectiveness of the measures referred to in paragraphs 1 and 2. If proportionate, this verification shall be carried out by independent internal or external auditors. 4. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures referred to in paragraph 1 other than those already referred to in paragraph 2, the conditions for the verification and auditing mechanisms referred to in paragraph 3 and as regards the criteria for proportionality under paragraph 3, and considering specific measures for micro, small and medium-sized-enterprises.	***Article 22*** 1. The controller shall adopt policies and implement appropriate measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation. 2. The measures provided for in paragraph 1 shall in particular include: (a) keeping the documentation pursuant to Article 28; (b) implementing the data security requirements laid down in Article 30; (c) performing a data protection impact assessment pursuant to Article 33; (d) complying with the requirements for prior authorisation or prior consultation of the supervisory authority pursuant to Article 34(1) and (2); (e) designating a data protection officer pursuant to Article 35(1). 3. The controller shall implement mechanisms to ensure the verification of the effectiveness of the measures referred to in paragraphs 1 and 2. If proportionate, this verification shall be carried out by independent internal or external auditors. **Measures adhered to by the controller pursuant to Articles 38 and 39 shall be accepted as valid tool to prove compliance with the respective requirements of this Regulation.** 4. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures referred to in paragraph 1 other than those already referred to in paragraph 2, the conditions for the verification and auditing mechanisms referred to in paragraph 3 and as regards the criteria for proportionality under paragraph 3, and considering specific measures for micro, small and medium-sized-enterprises.
Article 26	***Art. 26***

1. Where a processing operation is to be carried out on behalf of a controller, the controller shall choose a processor providing sufficient guarantees to implement appropriate technical and organizational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject, in particular in respect of the technical security measures and organizational measures governing the processing to be carried out and shall ensure compliance with those measures.	1. Where a processing operation is to be carried out on behalf of a controller and would involve personal data that would permit the processor to reasonably identify the data subject, the controller shall choose a processor providing sufficient guarantees assurances to implement appropriate technical and organizational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject, in particular in respect of the technical security measures and organizational measures governing the processing to be carried out and shall ensure compliance with those measures.
2. The carrying out of processing by a processor shall be governed by a contract or other legal act binding the processor to the controller and stipulating in particular that the processor shall: (a) act only on instructions from the controller, in particular, where the transfer of the personal data used is prohibited; (b) employ only staff who have committed themselves to confidentiality or are under a statutory obligation of confidentiality; (c) take all required measures pursuant to Article 30; (d) enlist another processor only with the prior permission of the controller; (e) insofar as this is possible given the nature of the processing, create in agreement with the controller the necessary technical and organizational requirements for the fulfillment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III; (f) assist the controller in ensuring compliance with the obligations pursuant to Articles 30 to 34; (g) hand over all results to the controller after the end of the processing and not process the personal data otherwise;	2. The carrying out of processing shall be governed by a contract or other legal act binding the processor to the controller. **The controller and processor shall be free to determine respective roles and responsibilities with respect to the requirements of this Regulation, and shall provide for the following** ~~and stipulating in particular that the processor shall~~: (a) **the processor shall** act only on instructions from the controller, in particular, where the transfer of the personal data used is prohibited; (b) ~~employ only~~ staff **employed by the processor shall commit** to confidentiality ~~or are under a statutory obligation of confidentiality~~; (c) **agreement with respect to the** ~~take all~~ required measures pursuant to Article 30; ~~(d) enlist another processor only with the prior permission of the controller;~~ (e) insofar as this is possible given the nature of the processing **and the processor's ability to assist with reasonable effort**, ~~create in~~ **an** agreement **as to** ~~with the controller~~ the ~~necessary~~ **appropriate and relevant** technical and organizational requirements ~~for the fulfillment of~~ **which support the ability**

(h) make available to the controller and the supervisory authority all information necessary to control compliance with the obligations laid down in this Article.	**of the controller**~~'s obligation~~ to respond to requests for exercising the data subject's rights laid down in Chapter III; (**f) insofar as this is possible given the nature of the processing, the information available to the processor and his ability to assist with reasonable effort, an agreement on how compliance will be ensured** ~~assist the controller in ensuring compliance~~ with the obligations pursuant to Articles ~~30~~ **28** to 34; (g) ~~hand over all results to the controller after the end of the processing and~~ **assurance from the processor that he will** not process the personal data ~~otherwise~~ **further after the end of the agreed processing**; (h) **agreement that, upon request, the processor will** make available to the controller ~~and the supervisory authority~~ all **available, relevant and permissible** information necessary to control compliance with the obligations laid down in this Article.
3. The controller and the processor shall document in writing the controller's instructions and the processor's obligations referred to in paragraph 2.	3. The controller and the processor shall document in **text** form ~~writing~~ the **arrangements** ~~controller's instructions and the processor's obligations~~ referred to in paragraph 2. **3a – NEW - The controller is deemed to have fulfilled the obligations set out in paragraph 1 when employing a processor who has voluntarily self-certified or voluntarily obtained a third party certification, seal or mark showing the implementation of appropriate standard technical and organizational measures in response to the requirements set out in this Regulation.**
4. If a processor processes personal data other than as instructed by the controller, the processor shall be considered to be a controller in respect of that processing and shall be subject to the rules on joint controllers laid down in Article 24.	4. If a processor processes personal data ***for purposes*** other than as instructed by the controller, the processor shall be considered to be a controller in respect of that processing ~~***and shall be subject to the rules on joint controllers laid down in Article 24***~~.

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the responsibilities, duties and tasks in relation to a processor in line with paragraph 1, and conditions which allow facilitating the processing of personal data within a group of undertakings, in particular for the purposes of control and reporting.	

-