**Verankerung von Selbstregulierung im Datenschutz in der EU-Datenschutz-Grundverordnung**

< TT. Monat JJJJ >

Seite 1

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medi-en 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 zukunftsorien-tierte Netzpolitik ein.

Zusammenfassung

Selbstregulierung innerhalb eines geeigneten gesetzlichen Rahmens ist ein geeignetes Instrument, um das Vertrauen von Kunden und Nutzern in den Schutz ihrer Persönlichkeitsrechte in einem Geschäftsfeld hoher Heterogenität und Dynamik dauerhaft zu erhalten. 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.

# Ziele:

Selbstregulierung dient der Erreichung gesellschafts- und wirtschaftspolitischer Ziele. Eine klare Definition dieser Ziele für die Entwicklung eines gesetzlichen Rahmens ist unabdingbar. BITKOM definiert 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.

# 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.

# Vorschläge zur Ausgestaltung von regulierter Selbstregulierung im Datenschutz

## 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.

### Verfahrensgrundsätze



* Europäische oder nationale Vereinigungen erarbeiten (möglichst im Dialog mit der zuständigen Aufsichtsbehörde) 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.
* 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 der Aufsichtsbehörde zusammen mit dem Antrag auf Anerkennung zugänglich gemacht werden und von dieser gegebenenfalls berücksichtigt werden. Alternativ könnte dieses Verfahren auch direkt bei der Aufsicht angesiedelt werden (wie bereits in Art. 38 Abs. 2 S.2 des Entwurfs angedeutet).
* Die für die Vereinigung zuständige Datenschutzaufsicht erkennt den Kodex an, sofern er den gesetzlichen Vorgaben entspricht. Dabei hat die Vereini­gung 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.
* Wird zum Zweck der Kontrolle und Durchsetzung der Selbstverpflichtung eine Selbstkontrollinstanz eingerichtet, so muss auch diese von 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.
* Vor der Anerkennung informiert die zuständige Aufsicht die weiteren europäi­schen und nationalen Aufsichtsbehörden und gibt diesen Gelegenheit zur Stellungnahme. Sofern aufgrund eines grenzüberschreitenden Sachverhalts nötig, erfolgt eine Abstimmung nach einem in der Datenschutz-VO bestimm­ten Kohärenzverfahren. Wenn 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

.

* 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 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.

## 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. Nähere Ausführungen dazu finden sich in dem beigefügten Thesenpapier ab Seite 9.

* **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. Privilegierung der Unternehmen im Falle von Verstößen bei regelmäßiger Prüfung durch Dritte.
* **Modell III**: Kontrolle durch Prüfung unabhängiger Dritte im Auftrag einer anerkannten Selbstkontrollinstanz, die auch durchsetzt. Aufsicht greift nur bei Versagen der Selbstkontrolle.

# 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 folgende Änderungen am vorgelegten Verordnungsentwurf vor:

**Art. 38 Codes of Conduct**

| **Commission Proposal** | **BITKOM 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 organisations;  (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 supervisory authority in that Member State ***to confirm the compliance with this Regulation***. The 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.*** |
|  |  |
| 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. 39 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 supervisory authority of their Member State or in the case of an international code the European Data Protection Board to approve this self-regulatory body as competent self-regulatory body. 2. Conditions for approval are:    1. Proof of sufficient expertise    2. Sufficient financial means for the time of planned validity of the code    3. Transparent processes that ensure fair and neutral decisions in cases of breach    4. … 3. Self-regulatory bodies that have been approved by the competent supervisory authority or the European Data Protection Board - gerichtliche Überprüfung der Entscheidung beantragen… 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 act only if the self-regulatory body doesn’t act at all in reasonable time or exceeds its scope of judgement evaluation. |

**Art. 40 new (former 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. |  |
| 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). |  |
|  |  |

To Do:

-Welche delegierten Rechtsakte lassen sich ggf. durch Selbstverpflichtungen ersetzen?

- Rechtsfolgen regeln, z.B. dass aktuelle Zertifizierungen als Nachweis bzw. Ersatz für Kontrollpflicht anerkannt sind. Wo wäre das am besten klarzustellen?

-