5.5 Umsetzungsoptionen der Ko-Regulierung im Datenschutz

[Dr. Susanne Dehmel | BITKOM][1]

5.5.1 Einleitung

In der Informationsgesellschaft gibt es ständig neue datenverarbeitende Anwendungen, die Interessenskonflikte auslösen können (und werden). Legislative Prozesse im Bereich Datenschutz sind oft politisch schwierig und sehr langwierig. Die Durchsetzbarkeit nationaler Gesetzgebung ist beschränkt, was insbesondere bei digitalen, ortsunabhängigen Diensten zu berücksichtigen ist. Immer wieder aufkommende politische Forderungen nach Einzelgesetzen widersprechen dem grundsätzlichen Ziel der Schaffung einer übersichtlichen, technikneutralen Rahmengesetzgebung.
Zahlreiche Ansätze zur Selbstregulierung in der IT (Geodatendienste-Kodex, Social Media Kodex, OBA, Binding Corporate Rules, Accountability) sind bereits vorhanden. Es fehlt bislang aber eine systematische Entwicklung des Instruments Selbstregulierung, welche einen nachhaltigen Einsatz ermöglichen würde. Bis auf § 38a BDSG verfügen wir bislang über keinen klaren Rahmen für Selbstverpflichtungen im Datenschutz.
Im aktuellen deutschen Datenschutzrecht ist mit § 38a BDSG die Selbstregulierung als Rechtsinstrument angelegt, bislang aber praktisch nicht angewandt worden. Dafür gibt es vermutlich mehrere Gründe. So ist umstritten, inwieweit die Entscheidung der zuständigen Aufsichtsbehörde auch für die anderen Datenschutzbehörden bindend ist. In der Regel werden sich die Datenschutzbehörden zwar zuvor abstimmen, jedoch nicht in einem formellen Verfahren. Außerdem ist ungeklärt, inwieweit Regelungen über die gesetzlichen Anforderungen hinausgehen müssen bzw. diese konkretisieren müssen. Insgesamt lässt sich feststellen, dass sich § 38a BDSG in der Praxis noch nicht so bewährt hat wie erhofft.
Die Datenschutz-Grundverordnung bietet nun die Chance das Instrument der Selbstregulierung im europäischen Kontext neu zu justieren. Daher lohnt es sich, noch einmal nachzudenken, welche Gründe im Datenschutz für Selbstregulierung sprechen und welche Voraussetzungen für eine erfolgreiche Selbstregulierung gegeben sein sollten.
Selbstregulierung ist ein Instrument zur Erreichung von gesellschafts- und wirtschaftspolitischen Zielen. Eine klare Definition dieser Ziele ist unabdingbar für die Entwicklung eines gesetzlichen Rahmens. BITKOM definiert drei Ziele für die Selbstregulierung im Datenschutz:

- **Vertrauen**: In einer sich schnell wandelnden technischen Umgebung soll das Vertrauen aller Beteiligten in Datensicherheit und datenschutzkonformes Verhalten bei Datenverarbeitungen gestärkt werden.
- **Flexibilisierung**: Datenschutzrecht von (branchenspezifischen) Spezial- und Detailregelungen entlasten und flexible Regelungen ermöglichen, innerhalb derer auf den technischen Wandel in angemessener Zeit reagiert werden kann.
- **Wachstumsförderung durch Rechtssicherheit und internationale Standards**: Unter Beibehaltung eines hohen Datenschutzniveaus sollten europäische Unternehmen durch ein effizienteres Datenschutzregime in ihrer internationalen Wettbewerbsfähigkeit gestärkt werden.

Der vorliegende Aufsatz analysiert die Perspektiven der Beteiligten, stellt die wichtigsten Eckpunkte seitens der deutschen ITK-Wirtschaft vor und skizziert konkrete Umsetzungsvorschläge.

5.5.2 Anforderungen der Beteiligten

Nachfolgend werden einige Anforderungen bzw. Vorteile dargestellt, die sich aus der Sicht der unterschiedlichen Akteure bei der Gestaltung von Selbstregulierung im Datenschutz berücksichtigt werden sollten:

1. Perspektive des Gesetzgebers

Der Gesetzgeber könnte sich bei einem parallelen System der Selbstregulierung auf die Festlegung abstrakter grundsätzlicher Normen beschränken und so die Komplexität der Gesetze sowie die Zahl der Gesetzesänderungen reduzieren.

2. Perspektive der Unternehmen

- Unternehmen sollten einen Anspruch auf Genehmigung einer Selbstverpflichtung in angemessener Frist bekommen, wenn sie den gesetzlichen Vorgaben entspricht.
- Kosten für die Selbstregulierung müssen im Verhältnis zu den Vorteilen stehen, die sich für Unternehmen daraus ergeben, sich freiwillig zu verpflichten. Selbstregulierung sollte europaweit und möglichst international anerkannt werden können.
- **Anforderungen von Unternehmen als Kunde:** Die Inhalte der Selbstverpflichtung des Anbieters müssen transparent sein. Durch Selbstverpflichtungen sollte Einschätzung und Überwachung der datenschutzkonformen Arbeit von Dienstleistern erleichtert werden (zum Beispiel durch Anerkennung von durch Dritte bestätigte Selbstverpflichtung von Auftragsverarbeitern zu technisch-organisatorischen Maßnahmen anstelle individueller Kontrollen durch den Auftraggeber nach § 11 II 4 BDSG). Die Unterzeichnung einer Selbstverpflichtung durch ein Unternehmen muss über eine bloße Selbstauskunft hinaus nachvollziehbar sein.
- **Anforderungen von Unternehmen als Dienstleister:** Es müssen Anreize für die Eingehung von Selbstverpflichtungen geschaffen werden. Diese können zum Beispiel sein: Mehr Rechtssicherheit bzw. Reduktion des Risikos von Sanktionen durch die Aufsichtsbehörden durch Beitritt zu einer Selbstverpflichtung; oder die einheitliche Rechtsauslegung durch die unterschiedlichen Datenschutzbehörden, die zuständig sind. Ein weiterer Vorteil wäre die schnellere Schaffung von Rechtssicherheit sowie die Reduktion von Verwaltungsaufwand durch Schaffung einer zentralen Anlaufstelle. Eine (ggf. zertifizierte) Selbstverpflichtung sollte durch Aufsichtsbehörden und Kunden als Nachweis für datenschutzkonformes Verhalten nach § 11 II 4 BDSG anerkannt werden.

3. Perspektive der Aufsichtsbehörden

- Selbstregulierung kann den Datenschutz fördern, indem sie Unternehmen zwingt, sich mit internen Prozessen bewusst auseinander zu setzen, bevor sie sich verpflichten.
- Selbstregulierung kann den sachlichen Dialog mit Unternehmen/Branchen befördern und Branchenstandards schaffen.
- Selbstregulierung ermöglicht u. U. eine schnellere Reaktion auf Missstände.

- Wenn durch Selbstverpflichtung Standards geschaffen werden, die durch die Aufsichtsbehörden anerkannt sind, können diese Ressourcen bei den Behörden sparen.
- Der Kontrollaufwand durch die Aufsichtsbehörden kann sich verringern.
- Durch Beschwerdeverfahren im Rahmen der Selbstregulierung kann sich die Zahl der individuellen Beschwerden bei den Aufsichtsbehörden verringern.
- Selbstregulierung kann effektiver sein als nicht durchsetzbare Gesetze, denn sie kann auch Nichteuropäer binden.
- Selbstregulierung kann Druck durch den Markt auf Nichteuropäer erzeugen, bestimmte Standards einzuhalten.
- Selbstregulierung muss vertrauenswürdig sein – welche Anforderungen an Erarbeitung, Durchsetzung, Sanktionierung stellen sich?
- Vereinbarkeit mit Unabhängigkeit der Aufsichtsbehörden (und deren Auftrag, die Einhaltung der Gesetze zu prüfen, nicht die von Selbstregulierung).

4. Perspektive der Betroffenen

- Selbstverpflichtungen müssen transparent und durchsetzbar sein.
- Einheitliche Branchenstandards durch Selbstverpflichtungen können es dem Betroffenen erleichtern, zu entscheiden, ob ein Angebot vertrauenswürdig ist oder nicht.
- Der Betroffene muss sich darauf verlassen können, dass die freiwilligen Standards der Unternehmen auf gesetzlicher Grundlage basieren.
- Betroffene sollten bei Erarbeitung und Durchsetzung von Selbstverpflichtungen einbezogen werden.

5. Justiz

- Für die Justiz könnte mehr Selbstregulierung weniger Verfahren bedeuten, da effizientere Vorprüfungen durch die Aufsichtsbehörden möglich wären.
- Konzentration auf wirklich strittige Rechtsfragen, unter Umständen Bündelung, weil solche Fragen auch im Rahmen der Erarbeitung von Selbstverpflichtungen auftauchen und ein Urteil Breitenwirkung entfalten kann.
- Gerichte können sich an durch Selbstverpflichtungen geschaffenen Standards orientieren, wenn sie über Datenschutzverstöße Einzelner entscheiden müssen (zum Beispiel Anhaltspunkte für Verschulden).

5.5.3 Erfolgskriterien

Aus den Anforderungen der unterschiedlichen Beteiligten ergeben sich folgende Erfolgskriterien für Selbstregulierung im Datenschutz:

- **Europäischer Rahmen: Datenverarbeitung erfolgt grenzüberschreitend und Selbstregulierung dafür bedarf daher mindestens eines europäischen Rahmens.** 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. Vor dem Hintergrund grenzüberschreitender Kommunikation und international ausgerichteter Geschäftsmodelle sollten gerade im Datenschutz mindestens europäische Standards

geschaffen werden. Ein System der Selbstregulierung sollte daher bereits auf europäischer Ebene verankert werden. Ein europäisches Selbstregulierungssystem ist dabei im Idealfall kompatibel mit Selbstregulierungsansätzen in Drittstaaten. Ein europäischer Rahmen schließt nicht aus, dass es innerhalb dieses Rahmens auch nationale Selbstverpflichtungen geben kann.

- **Freiwilligkeit: Unternehmen sollten durch Anreize, nicht durch Zwang zu Selbstverpflichtungen motiviert werden.**
  Die Freiwilligkeit von Selbstverpflichtungen ist Voraussetzung für ihre Akzeptanz bei und in Unternehmen. Für eine breite Beteiligung müssen Anreizen gesetzt werden, welche eine Beteiligung für die Unternehmen attraktiv machen. Solche Anreize können beispielsweise durch eine bestimmte Privilegierungswirkung bei Beitritt zu einer Selbstverpflichtung erreicht werden. Wenn sich einzelne Standards branchenweit durchsetzen, gibt es einen faktischen Zwang für Unternehmen, diese ebenfalls einzuhalten. Dabei ist auch zu berücksichtigen, dass Selbstregulierung die Unternehmen immer Geld kostet. Diese Kosten dürfen nicht so hoch sein, dass Selbstregulierung gerade für kleinere Unternehmen unattraktiv wird.
- **Standard: Selbstregulierung sollte den gesetzlichen Rahmen konkretisieren, nicht verschärfen.**
  Es erscheint sinnvoll, dass Selbstverpflichtungen im Datenschutz ähnlich wie im Jugendmedienschutz im Rahmen und auf Basis der gesetzlichen Vorgaben eingegangen werden, um diese zu konkretisieren. Es sollte dagegen nicht Voraussetzung sein, dass über die gesetzlichen Vorgaben hinausgegangen werden muss, weil sonst die Hürden für eine breite Beteiligung zu hoch liegen könnten. Gegenstand der Selbstregulierung wird in der Regel die Konkretisierung gesetzlicher Vorgaben in Form einer „Übersetzung“ auf die technisch-organisatorische Ebene sein. Weiterhin können Selbstverpflichtungen bei gesetzlichen Vorgaben, deren Auslegung Zweifel aufwirft, ein konkretes Verständnis der Vorschrift festschreiben, auf welches man sich im Vorfeld mit den Aufsichtsbehörden geeinigt hat.
- **Verbindlichkeit, Verfahren, Durchsetzbarkeit: Je verbindlicher die Selbstverpflichtung sein soll und je mehr Rechtsfolgen sich aus ihr ergeben, desto höhere Anforderungen sind an Verfahren und Durchsetzbarkeit zu stellen.**
  Kunden und Aufsichtsbehörden müssen sich auf die Einhaltung der im Rahmen einer Selbstverpflichtung eingegangenen Zusagen verlassen können. Dazu muss nicht unbedingt eine staatliche Stelle eingeschaltet werden. Verlässlichkeit könnte auch durch die Bestätigung einer unabhängigen privaten Stelle - wie zum Beispiel einer Selbstkontrolleinrichtung oder einem Zertifizierungsunternehmen – erreicht werden.
  Welche Anforderungen an das **Verfahren** zur Schaffung einer Selbstverpflichtung zu stellen sind, ergibt sich zum einen aus den Bedürfnissen der Beteiligten und zum anderen aus dem Grad der Verbindlichkeit daran geknüpfter Rechtsfolgen, die die Selbstverpflichtung haben soll. Nicht jede Selbstverpflichtung muss grundsätzlich staatlich genehmigt werden. Je nach Rechtsfolge, die an die Unterzeichnung einer Selbstverpflichtung geknüpft werden soll, kann die Genehmigung durch eine Aufsichtsbehörde oder sonstige staatliche Stelle aber sinnvoll oder gar erforderlich sein – nämlich dann, wenn beispielsweise die Aufsicht einen Teil ihrer Kontrollbefugnisse aufgrund einer solchen Selbstverpflichtung an die Selbstkontrolle überträgt.
  Selbstverpflichtungen, die Vertrauen schaffen sollen, müssen auch **durchsetzbar** sein. Je höher der Grad der Verbindlichkeit und der damit verbundenen Privilegien für die

beteiligten Unternehmen, desto höher sind auch die Anforderungen an eine effektive Kontrolle und Durchsetzung der Pflichten. Diese lassen sich zum Beispiel mit Hilfe der Einrichtung einer Selbstkontrolle oder der Kontrolle durch unabhängige Dritte (Prüfer) umsetzen. Die Zusammenarbeit und das Verhältnis von Aufsichtsbehörden und Selbstkontrolle muss geregelt werden. Bei jeder Selbstverpflichtung sollte grundsätzlich festgelegt werden, wer Verstößen nachgeht, ob ein Beschwerdeverfahren eingerichtet wird und welche Sanktionen Verstöße nach sich ziehen.

5.5.4 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.

Grafik 27: Verfahren bis zur Anerkennung eines Kodex

- Europäische oder nationale Vereinigungen erarbeiten (möglichst im Dialog mit der zuständigen Aufsichtsbehörde) einen Kodex. Es sollten nicht zu enge Vorgaben gemacht werden, welche Vereinigungen vorlageberechtigt sind. Eventuell könnte man darüber nachdenken, eine Mindestanzahl von repräsentierten Unternehmen oder einen Mindestanteil im Markt vorzuschreiben. Das könnte allerdings den Effekt verhindern, dass

wenige „First Movers“ den Rest des Marktes zu besseren Standards treiben können. Es sollte 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 ebenso aus wie die Akzeptanz unter den Unternehmen einer Branche erhöht wird. Unternehmen, die nicht von Anfang an die Möglichkeit zur Mitwirkung an der Erstellung einer Selbstverpflichtung hatten, könnten Probleme haben, eine solche Selbstverpflichtung zu akzeptieren.

- 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 eine Selbstkontrollinstanz zum Zweck der Kontrolle und Durchsetzung der Selbstverpflichtung 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-Verordnung 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.

Grafik 28: 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.

5.5.5 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 müssen.
Je nach zu regelndem Sachverhalt und gewünschter Verbindlichkeit gibt es unterschiedlich geeignete und aufwändige Instrumente zur Kontrolle und Durchsetzung der vereinbarten Regelungen.
Neben den Befugnissen der Aufsichtsbehörden und den zusätzlich freiwillig eingeräumten Befugnissen der Selbstkontrollinstanzen gibt es bei Verstößen eines Unternehmens gegen Aussagen, die es im Rahmen einer Selbstverpflichtung getroffen hat, bereits jetzt wettbewerbsrechtliche Instrumente, um dagegen vorzugehen. Darüber hinaus ist aus unserer Sicht keine Änderung der jetzigen Rechtslage bzw. Schaffung von zusätzlichen Durchsetzungsinstrumenten nötig.

Nachfolgend werden drei mögliche Modelle kurz skizziert und bewertet:

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

Modell I

Grafik 29: Kontrolle und Durchsetzung eines Kodex – Modell I

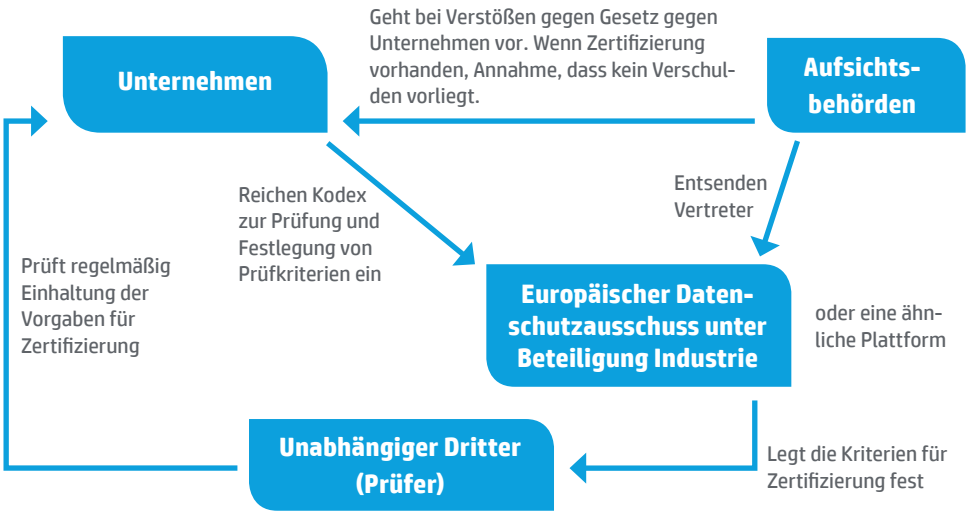
Sofern eine Selbstkontrollinstanz errichtet wird, unterwerfen sich die Unternehmen mit Unterzeichnung des Kodex der Kontrolle und Sanktionierung durch diese Instanz. Die zuständige Aufsichtsbehörde gibt Verdachtsfälle und Meldungen über Verstöße, die den Geltungsbereich der Selbstverpflichtung betreffen, an die Selbstkontrollinstanz weiter und schreitet selbst gegen das Unternehmen nur dann ein, wenn die Selbstkontrollinstanz unbegründet untätig bleibt oder ihren Beurteilungsspielraum überschreitet.

Faktor	Eignung Modell I
Vertrauen Beteiligte	(+) Selbstkontrollinstanz von Aufsicht nach transparenten Kriterien genehmigt (+) Aufsicht kann bei Versagen der Selbstkontrolle eingreifen (+) Betroffene können sich durch Beschwerdeverfahren direkt an Selbstkontrolle wenden (-) Selbstkontrolle wird von den Unternehmen finanziell getragen
Eignung Interessenabwägung im Einzelfall	(+) Selbstkontrollinstanz kann geeignetes Gremium zur Entscheidung in Einzelfällen bereitstellen
Eignung techn.-org. Maßnahmen	(+/-) Prüfung der Unternehmen vor Ort für Selbstkontrollinstanz sehr aufwändig und unter Umständen schwierig zu bewältigen

Rechtssicherheit	(+) für Unternehmen hoch, da von Kodex von Aufsicht anerkannt und grundsätzlich Kontrolle nur durch zentrale Selbstkontrolle
Aufwand/Kosten	(-) Einmalige Kosten für Einrichtung und. laufende Kosten für Unterhalt Selbstkontrollinstanz (+) können angemessen verteilt werden zwischen Großen und kleineren Unternehmen (+) Selbstkontrollinstanz ist zentrale Anlaufstelle für Unternehmen, Aufsichtsbehörden und Betroffene

Grafik 30: Bewertung des Modells I

Modell II



Grafik 31: Kontrolle und Durchsetzung eines Kodex – Modell II

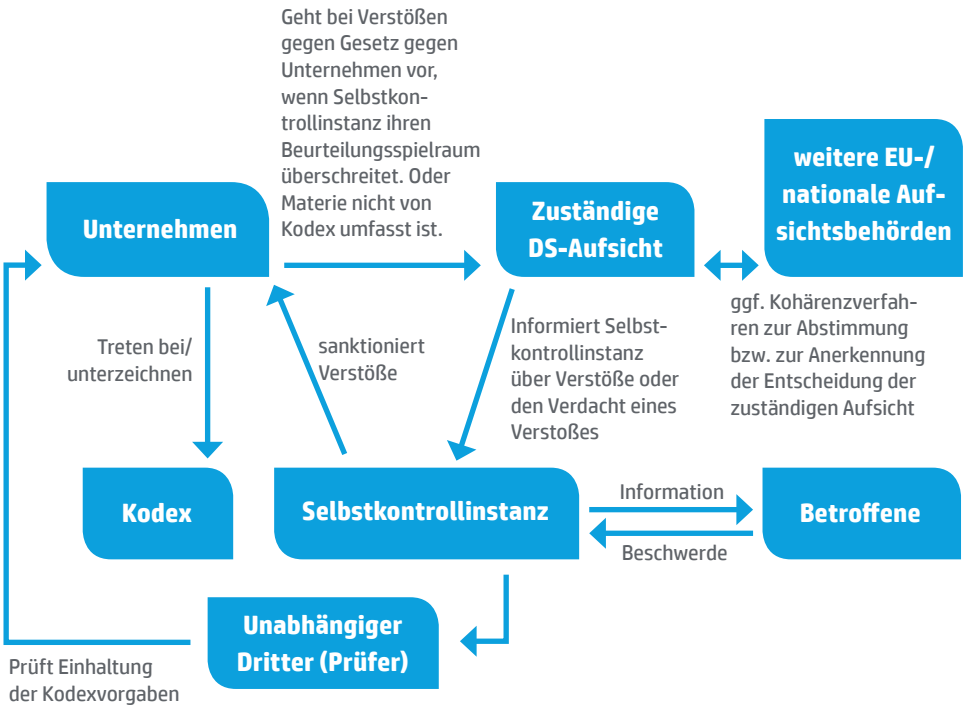
In diesem Modell werden Selbstverpflichtungen so konzipiert, dass sie durch unabhängige Dritte nach festgelegten Kriterien überprüfbar sind. Sie werden bei einer Stelle wie zum Beispiel dem Europäischen Datenschutzausschuss eingereicht.
Im Europäischen Datenschutzausschuss sollten grundsätzlich und insbesondere bei einem solchen Verfahren neben den Vertretern der Aufsichtsbehörden auch Vertreter der Unternehmen vertreten sein, um eine umfassende Berücksichtigung aller relevanten Aspekte und Praxisnähe bei einer Entscheidung sicher zu stellen.
Der Europäische Datenschutzausschuss inklusive Unternehmensvertreter legt entsprechend den Verpflichtungen im Kodex geeignete Prüfkriterien fest. Unabhängige Dritte, welche vorher durch den Datenschutzausschuss anerkannt werden, prüfen (und zertifizieren gegebenenfalls) die Unternehmen, die sich dem Kodex unterwerfen, in regelmäßigen Abständen.

Bei einem Modell, welches eine Zertifizierung beinhaltet, ist zu berücksichtigen, dass die Kosten auch für kleinere Unternehmen tragbar sein müssen, wenn die Verpflichtung sich in der Breite auswirken soll.
Die Prüfung von Verstößen und die Durchsetzung von Sanktionen bei Verstößen obliegt den Aufsichtsbehörden, jedoch ist bei Vorliegen einer aktuellen Zertifizierung nicht von einem Verschulden des Unternehmens auszugehen, sofern ein Verstoß festgestellt wird, der in den Prüfungsrahmen dieser Zertifizierung fällt.

Faktor	**Eignung Modell II**
Vertrauen Beteiligte	(+) Prüfung durch unabhängige Dritte nach Kriterien, die durch Datenschutzausschuss festgelegt wurden (+) Aufsicht kontrolliert und sanktioniert (kein (+) zum Status quo) (-) Betroffene haben außer den Aufsichtsbehörden keine zusätzliche Anlaufstelle für Beschwerden
Eignung Interessenabwägung im Einzelfall	(-) Abwägungen im Einzelfall durch Prüfer teilweise schwierig
Eignung techn.-org. Maßnahmen	(+) Prüfung durch Dritte gut geeignet
Rechtssicherheit	(+) für Unternehmen erhöht: kein Verschulden bei Verstoß), (-) aber nicht grundsätzliches Verfahren bei Aufsichtsbehörde
Aufwand/Kosten	(+/-) Jedes Unternehmen trägt regelmäßig die Kosten für seine Prüfung und ggf. Zertifizierung. Je nach Aufwand könnte das für kleinere Unternehmen zu teuer sein. Allerdings wäre es auch hier vorstellbar, gestaffelte Preise zu vereinbaren. (-) Keine zentrale Anlaufstelle für Unternehmen, Aufsichtsbehörden und Betroffene

Grafik 32: Bewertung des Modells II

Modell III



Grafik 33: Kontrolle und Durchsetzung eines Kodex – Modell III

Denkbar wäre auch eine dritte Variante, bei der es eine Selbstkontrollinstanz gibt, welche nur die Sanktionierung und Beschwerdeverfahren durchführt, während die laufende Kontrolle durch unabhängige Dritte in Audits durchgeführt und ggf. durch Zertifizierungen bestätigt wird.
Generell ist der Kostenaspekt für die Unternehmen zu berücksichtigen. Denn auch eine Selbstkontrollinstanz muss finanziert werden (was in der Regel durch die beteiligten Unternehmen geschieht). Diese Kosten müssen in Relation stehen zu den Vorteilen, die die Unternehmen dadurch haben, dass sie sich freiwillig verpflichten.

Faktor	Eignung Modell II
Vertrauen Beteiligte	(+) Selbstkontrollinstanz von Aufsicht nach transparenten Kriterien genehmigt (+) Prüfung der Kodex-Vorgaben durch unabhängige Dritte (+) Transparenz durch mögliche Zertifikate (+) Kontrolle und Sanktion bei vermuteten Verstößen durch Selbstkontrollinstanz (+) Aufsicht kann bei Versagen der Selbstkontrolle eingreifen (+) Betroffene können sich durch Beschwerdeverfahren direkt an Selbstkontrolle wenden
Eignung Interessenabwägung im Einzelfall	(+) Abwägungen im Einzelfall können bei vermuteten Verstößen durch Selbstkontrollinstanz gewährleistet werden
Eignung techn.-org. Maßnahmen	(+) laufende Prüfung durch Dritte insbesondere für techn.-org. Maßnahmen gut geeignet
Rechtssicherheit	(++) für Unternehmen hoch, da von Kodex von Aufsicht anerkannt und grundsätzlich Kontrolle nur durch zentrale Selbstkontrolle bzw. von dieser beauftragte unabhängige Dritte
Aufwand/Kosten	(-) Einmalige Kosten für Einrichtung und. laufende Kosten für Unterhalt Selbstkontrollinstanz (+) können angemessen verteilt werden zwischen Großen und kleineren Unternehmen (+) Selbstkontrollinstanz ist zentrale Anlaufstelle für Unternehmen, Aufsichtsbehörden und Betroffene (-) Jedes Unternehmen trägt zusätzlich regelmäßig die Kosten für seine Prüfung und ggf. Zertifizierung – auch hier vorstellbar, gestaffelte Preise zu vereinbaren.

Grafik 34: Bewertung des Modells III

5.5.6 Ausblick

Es bleibt abzuwarten, ob zumindest einige dieser Ansätze tatsächlich Eingang in die Datenschutz-Grundverordnung der EU finden werden. Vorstöße, einen besseren Selbstregulierungsrahmen zu schaffen, hat es in der laufenden Diskussion (unter anderem von der Bundesregierung) bereits gegeben. Ob sie sich durchsetzen werden, ist noch nicht abzusehen.
Ein robuster europäischer Selbstregulierungs-Rahmen wäre auch für die internationale Datenverarbeitung hilfreich. Die global bestehenden unterschiedlichen Datenschutzsysteme werden in absehbarer Zeit nicht vereinheitlicht werden können. Aber vielleicht gelingt der Bau von „Selbstregulierungsbrücken", die die unterschiedlichen Systeme auf einem angemessenen Niveau verbinden.

1 Das Thesenpapier wurde unter Einbindung von Mitgliedern des AK Datenschutzes des BITKOM erstellt.