

VERHALTENSREGELN UND ZERTIFIZIERUNG

Artikel 38 Verhaltensregeln	EG 76.
<p>1. Die Mitgliedstaaten, die Aufsichtsbehörden und die Kommission fördern die Ausarbeitung von Verhaltensregeln, die nach Maßgabe der Besonderheiten der einzelnen Datenverarbeitungsbereiche zur ordnungsgemäßen Anwendung dieser Verordnung beitragen sollen und sich <u>insbesondere</u> auf folgende Aspekte beziehen:</p>	<p>Die in Absatz 1 a) bis h) dargelegten Anforderungen sollten nicht als Mindestinhalt verstanden werden. Artikel 27 der EU-Datenschutzrichtlinie und die Umsetzungsnorm des § 38a BDSG kommen ohne diese Konkretisierung aus. Bislang gab es keine schlechten Erfahrungen, vielmehr ermöglichte die offene Formulierung den erforderlichen Gestaltungsspielraum zur Abdeckung der branchenspezifischen Besonderheiten. Gerade f) und h) betreffen nicht jedes Unternehmen oder jede Unternehmensbranche und sollten daher nicht zwingend bzw. künstlich geregelt werden. Auch wenn die Formulierung „insbesondere“ eine nicht abschließende Aufzählung impliziert, kann nicht ausgeschlossen werden, dass Absatz 1 a) bis h) in der Anwendung als Mindestmaß für Verhaltensregeln verstanden wird.</p> <p>GDV-Vorschlag:</p> <p>„Die Mitgliedstaaten, die Aufsichtsbehörden und die Kommission fördern die Ausarbeitung von Verhaltensregeln, die nach Maßgabe der Besonderheiten der einzelnen Datenverarbeitungsbereiche zur ordnungsgemäßen Anwendung dieser Verordnung beitragen sollen und sich insbesondere auf folgende Aspekte beziehen können:“</p>
a) faire und transparente Datenverarbeitung,	
b) Datenerhebung,	
c) Unterrichtung der Öffentlichkeit und der betroffenen Personen;	
d) von betroffenen Personen in Ausübung ihrer Rechte gestellte Anträge;	
e) Unterrichtung und Schutz von Kindern;	
f) Datenübermittlung in Drittländer oder an internationale Organisationen;	
g) Mechanismen zur Überwachung und zur Sicherstellung der Einhaltung der Verhaltensregeln durch die diesen unterliegenden für die Verarbeitung Verantwortlichen;	
h) außergerichtliche Verfahren und sonstige Streitschlichtungsverfahren zur Beilegung von Streitigkeiten zwischen für die Verarbeitung Verantwortlichen und betroffenen Personen im Zusammenhang mit der Verarbeitung personenbezogener Daten unbeschadet der den	

betroffenen Personen aus den Artikeln 73 und 75 erwachsenden Rechte.	
<p>2. Verbände und andere Einrichtungen, die Kategorien von für die Verarbeitung Verantwortlichen oder Auftragsverarbeitern in einem Mitgliedstaat vertreten und beabsichtigen, eigene Verhaltensregeln aufzustellen oder bestehende Verhaltensregeln zu ändern oder zu erweitern, können diesbezügliche Vorschläge der Aufsichtsbehörde in dem betreffenden Mitgliedstaat zur Stellungnahme vorlegen. Die Aufsichtsbehörde <u>kann</u> zu der Frage Stellung nehmen, ob der betreffende Entwurf von Verhaltensregeln beziehungsweise der Änderungsvorschlag mit dieser Verordnung vereinbar ist. Die Aufsichtsbehörde hört die betroffenen Personen oder ihre Vertreter zu diesen Vorschlägen an.</p>	<p>Es sollte nicht in das Ermessen der Aufsichtsbehörden gestellt werden, ob sie zur Frage der Vereinbarkeit Stellung nehmen möchten. Der Verordnungsvorschlag impliziert durch die Wortwahl „kann“ in Satz 2 jedoch gerade einen Entscheidungsspielraum der Behörden, der vor dem Hintergrund der zunehmenden Bedeutung von Verhaltensregeln nicht gerechtfertigt ist.</p> <p>GDV-Vorschlag:</p> <p>Satz 2 wird wie folgt formuliert.</p> <p>„Die Aufsichtsbehörde <u>nimmt</u> zu der Frage Stellung, ob der betreffende Entwurf von Verhaltensregeln beziehungsweise der Änderungsvorschlag mit dieser Verordnung vereinbar ist.“</p> <p>Im Übrigen entspricht die Regelung im Wesentlichen Artikel 27 Absatz 2 der EU-Datenschutzrichtlinie bzw. § 38 a Absatz 1 und 2 BDSG, die sich in der Praxis bewährt haben. Es fehlt jedoch an einer Übergangsregelung. Es ist sicherzustellen, dass ein einmal positiv ergangener Bescheid einer Datenschutzaufsichtsbehörde, wie z.B. in Deutschland nach § 38a Absatz 2 BDSG auch nach Anwendungsbeginn dieser Verordnung gem. Artikel 91 Absatz 2 der Verordnung weitergilt, soweit die ihm zugrunde gelegten Verhaltensregeln mit dieser Verordnung vereinbar sind. Der für die Versicherungswirtschaft eingeführte Code of Conduct sieht eine Evaluierungspflicht nach Änderung der Rechtslage vor. Ergibt diese Evaluierung, dass der Code of Conduct der Verordnung entspricht, sollte die Bestandskraft des Bescheides uneingeschränkt gelten.</p> <p>GDV-Vorschlag:</p> <p>Absatz 2 wird um einen Satz 4 und 5 ergänzt:</p> <p>„Mit Beginn der Anwendung nach Artikel 91 Absatz 2 dieser Verordnung legen Verbände und andere Einrichtungen den zuständigen Aufsichtsbehörden einen Bericht zur Evaluierung ihrer bestehenden Verhaltensregeln im Hinblick auf die Vereinbarkeit mit dieser Verordnung vor. Soweit die Aufsichtsbehörden auf Grundlage des Evaluierungsberichts von der Vereinbarkeit mit dieser Verordnung ausgehen, gelten die nach bisheriger Rechtslage erteilten verbindlichen Vereinbarkeitserklärungen fort“.</p>
<p>3. Verbände und andere Einrichtungen, die Kategorien von für die Verarbeitung Verantwortlichen oder Auftragsverarbeitern in mehreren Mitgliedstaaten vertreten, können der Kommission Entwürfe von <u>Verhaltensregeln</u> sowie Vorschläge zur Änderung oder Ausweitung bestehender Verhaltensregeln</p>	<p>Die Vorschrift bewirkt eine zweifache Prüfung der Verhaltensregeln auf ihre Vereinbarkeit mit der Verordnung. Absatz 2 gilt für die nationalen Aufsichtsbehörden, Absatz 3 für die EU-Kommission. Der Prüfungsgegenstand ist bei beiden Verfahren derselbe, da anders als in Artikel 27 der EU-Datenschutzrichtlinie nicht zwischen</p>

vorlegen.	<p>„einzelstaatlichen“ und „gemeinschaftlichen“ Verhaltensregeln unterschieden wird.</p> <p>GDV-Vorschlag:</p> <p>„Verbände und andere Einrichtungen, die Kategorien von für die Verarbeitung Verantwortlichen oder Auftragsverarbeitern in mehreren Mitgliedstaaten vertreten, können der Kommission Entwürfe von <u>gemeinschaftlichen Verhaltensregeln</u> sowie Vorschläge zur Änderung oder Ausweitung bestehender <u>gemeinschaftlicher Verhaltensregeln</u> vorlegen.“</p>
<p>4. Die Kommission kann im Wege einschlägiger Durchführungsrechtsakte beschließen, dass die ihr gemäß Absatz 3 vorgeschlagenen Verhaltensregeln beziehungsweise Änderungen und Erweiterungen bestehender Verhaltensregeln <u>allgemeine Gültigkeit</u> in der Union besitzen. Die genannten Durchführungsrechtsakte werden in Übereinstimmung mit dem Prüfverfahren gemäß Artikel 87 Absatz 2 erlassen.</p>	<p>Die von der EU-Kommission auf ihre Vereinbarkeit mit der Verordnung nach Absatz 3 geprüften Verhaltensregeln können für allgemein gültig erklärt werden. Anders als bisher bewirkt damit nicht mehr der selbstbestimmte Beitritt eines Unternehmens die rechtliche Verbindlichkeit der Verhaltensregeln. Die Selbstverpflichtung erfolgt in diesen Fällen nicht mehr freiwillig. Darüber hinaus bestehen massive Bedenken gegen diese Kompetenz der Kommission, da diese mit weitreichenden Folgen für die Unternehmen bei eingeschränkter Beteiligungs- und Prüfkompetenzen der Mitgliedstaaten einhergeht.</p> <p>GDV-Vorschlag:</p> <p>Absatz 4 wird gestrichen.</p>
<p>5. Die Kommission trägt dafür Sorge, dass die Verhaltensregeln, denen gemäß Absatz 4 allgemeine Gültigkeit zuerkannt wurde, in geeigneter Weise veröffentlicht werden.</p>	<p>Es wird auf die Ausführungen zu Absatz 4 verwiesen.</p> <p>GDV-Vorschlag:</p> <p>Absatz 5 wird gestrichen.</p>
Artikel 39 Zertifizierung	EG 77.
<p>1. Die Mitgliedstaaten und die Kommission fördern insbesondere auf europäischer Ebene die Einführung von datenschutzspezifischen Zertifizierungsverfahren sowie von Datenschutzsiegeln und –zeichen, anhand deren betroffene Personen rasch das von für die Verarbeitung Verantwortlichen oder von Auftragsverarbeitern gewährleistete Datenschutzniveau in Erfahrung bringen können. Die datenschutzspezifischen Zertifizierungsverfahren dienen der ordnungsgemäßen Anwendung dieser Verordnung und tragen den Besonderheiten der einzelnen Sektoren und Verarbeitungsprozesse Rechnung.</p>	<p>Zertifizierungssysteme sind grundsätzlich zu begrüßen. Aufwand und Kosten einer Zertifizierung sind zu berücksichtigen. Vor diesem Hintergrund sollte an den bereits bestehenden Zertifizierungsverfahren festgehalten werden.</p> <p>Die Zertifizierung Dritter, die für den für die Verarbeitung Verantwortlichen tätig sind und dazu Daten verarbeiten, wäre sehr zu begrüßen. Durch die Zertifizierung von Auftragsdatenverarbeitern (z.B. im Bereich des Cloud Computing) könnten die vertraglichen Pflichten und deren Kontrolle nach Artikel 26 Absatz 2 dieser Verordnung erheblich reduziert werden. Darüber hinaus könnten bestimmte Datenverarbeitungsprozesse des für die Verarbeitung Verantwortlichen zertifiziert werden. Im Gegenzug sollten die Unternehmen von bürokratischen Belastungen wie dem Nachweis einer Datenschutzstrategie (Artikel 22), der Dokumentation (Artikel 28) oder der der Datenschutzfolgenabschätzung (Artikel 33) befreit werden.</p>

<p>2. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Kriterien und Anforderungen für die in Absatz 1 genannten datenschutzspezifischen Zertifizierungsverfahren einschließlich der Bedingungen für die Erteilung und den Entzug der Zertifizierung sowie der Anforderungen für die Anerkennung der Zertifizierung in der Union und in Drittländern festzulegen.</p>	<p>Da es sich bei den Kriterien und Anforderungen für die in Absatz 1 genannten datenschutzspezifischen Zertifizierungsverfahren um eine „wesentliche“ Regelung handelt, sollte diese Verordnungen selbst diesbezügliche Vorgaben machen und entsprechende Kriterien und Anforderungen für das Zertifizierungsverfahren an dieser Stelle regeln.</p> <p>GDV-Vorschlag: Absatz 2 wird gestrichen.</p>
--	---