

MUTTER, DER MANN MIT DEN COCS IST DA

Heidi Scheichenbauer / Christof Tschohl / Walter Hötzendorfer /
Markus Kastelitz

Senior Researcher, Research Institute AG & Co KG
Amundsenstraße 9, 1170 Wien, AT
heidi.scheichenbauer@researchinstitute.at; <https://www.researchinstitute.at>

Wissenschaftlicher Leiter, Research Institute AG & Co KG
christof.tschohl@researchinstitute.at; <http://www.researchinstitute.at>

Senior Researcher, Research Institute AG & Co KG
walter.hoetendorfer@researchinstitute.at; <https://researchinstitute.at>

Senior Researcher, Research Institute AG & Co KG
markus.kastelitz@researchinstitute.at; <https://researchinstitute.at>

Schlagworte: *DSGVO, Verhaltensregeln, CoC, Selbstregulierung, Verbände, Überwachungsstelle*

Abstract: *Art. 40 DSGVO bietet Verbänden und anderen Vereinigungen, die Kategorien von Verantwortlichen oder Auftragsverarbeitern vertreten, die Möglichkeit, Verhaltensregeln (Codes of Conduct, CoC) auszuarbeiten. Die AutorInnen sind seit Anfang 2018 in der Praxis mit der Ausarbeitung von CoC befasst und setzen sich in diesem Beitrag mit offenen Rechtsfragen zu Art. 40 und 41 DSGVO auseinander. Darüber hinaus berichten sie von ihren Erfahrungen in der Ausarbeitung von CoC und im Genehmigungsverfahren bei der DSB nach Art. 40 Abs. 5 DSGVO.*

1. Verhaltensregeln nach der DSGVO als Instrument der Selbstregulierung

Die Anwendung der DSGVO¹ erweist sich für viele Rechtsunterworfenen als Herausforderung. Die Vielzahl an unbestimmten Rechtsbegriffen der DSGVO eröffnet große Interpretationsspielräume und führt oftmals zu Rechtsunsicherheit. Hier versucht Art. 40 DSGVO Abhilfe zu schaffen.

Nach Art. 40 Abs. 2 DSGVO können Verbände und andere Vereinigungen, die Kategorien von Verantwortlichen oder Auftragsverarbeitern vertreten, Verhaltensregeln ausarbeiten, die die Anwendung der DSGVO präzisieren. Verhaltensregeln sind somit eine Möglichkeit, um die zahlreichen Regelungslücken der DSGVO im Wege der Selbstregulierung zu schließen. Sie können damit Verantwortlichen und Auftragsverarbeitern die Anwendung der DSGVO erleichtern² und so zur Erhöhung der Rechtssicherheit für Verantwortliche und Auftragsverarbeiter beitragen.³

2. Verhaltensregeln unter der Datenschutz-Richtlinie

Die Möglichkeit Verhaltensregeln auszuarbeiten, war bereits in Art. 27 der Datenschutz-Richtlinie⁴ vorgesehen.⁵ Die entsprechende innerstaatliche Umsetzung erfolgte in § 6 Abs 4 DSG 2000, wonach zur näheren Fest-

¹ Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABI L 2016/119, 1.

² Vgl. ErwGr. 98 DSGVO.

³ Vgl. PAAL in Paal/Pauly (Hrsg.), Datenschutz-Grundverordnung, 2017, Art. 40 Rz 3.

⁴ Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABI L 1995/281, 31.

⁵ Vgl. Art. 27 Abs. 1, RL 95/46/EG: Die Mitgliedstaaten und die Kommission fördern die Ausarbeitung von Verhaltensregeln, die nach Maßgabe der Besonderheiten der einzelnen Bereiche zur ordnungsgemäßen Durchführung der einzelstaatlichen Vorschriften beitragen sollen, die die Mitgliedstaaten zur Umsetzung dieser Richtlinie erlassen.

legung dessen, was in einzelnen Bereichen als Verwendung von Daten nach Treu und Glauben anzusehen ist, für den privaten Bereich die gesetzlichen Interessenvertretungen, sonstige Berufsverbände und vergleichbare Einrichtungen Verhaltensregeln ausarbeiten konnten. Die Genehmigung erfolgte durch den Bundeskanzler (Verfassungsdienst), wobei es jedoch unter dem Regime des DSGVO 2000 insgesamt nur zwei Genehmigungen von Verhaltensregeln kam, sodass sich die rechtliche Bedeutung dieses Instruments bislang in Grenzen gehalten hat.⁶ In Einzelfällen ist Verhaltensregeln dennoch rechtliche Bedeutung zugekommen. So resultierte die Diskussion bei der Abfassung der Verhaltensregeln des Dialog Marketing Verbandes Österreich in einem wesentlichen Beitrag zum Abänderungsantrag zu § 151 GewO 1994 (neu) in welchem aufgrund der strengen Zweckbindung für Marketingzwecke und des damit einhergehenden geringen Gefährdungspotentials für nicht sensible Daten ein Opt-out-System vorgesehen⁷ und für sensible Daten eine relativ generell gehaltene Einwilligung zur Verwendung sensibler Daten für Marketingzwecke als ausreichend erachtet wurde.

3. Rechtswirkungen von Verhaltensregeln

Durch die DSGVO wurde das Instrument der Verhaltensregeln deutlich gestärkt. Die Verhaltensregeln gem. Art. 40 DSGVO sind nun nicht mehr – wie bisher gem. § 6 Abs. 4 DSGVO 2000 – lediglich auf den Aspekt von «Treu und Glauben» begrenzt. Einerseits dienen Verhaltensregeln dazu, die Vorgaben der DSGVO branchenspezifisch zu präzisieren, andererseits kann die Einhaltung dieses Instruments der Selbstregulierung als Faktor bzw. Gesichtspunkt herangezogen werden, um die Einhaltung der DSGVO nachzuweisen.⁸ Die Einhaltung genehmigter Verhaltensregeln ist bei der Verhängung einer etwaigen Geldbuße gebührend zu berücksichtigen (Art. 83 Abs. 2 lit. j DSGVO).⁹ Davon zu unterscheiden ist freilich die Tatsachenfrage, ob die Verhaltensregeln im Einzelfall tatsächlich eingehalten wurden. Verhaltensregeln können darüber hinaus «geeignete Garantien» zur Datenübermittlung in ein Drittland oder an eine internationale Organisation darstellen (Art. 46 Abs. 2 lit. e DSGVO) und sind bei der Beurteilung der Auswirkungen eines beabsichtigten Verarbeitungsvorganges im Rahmen einer Datenschutz-Folgeabschätzung zu berücksichtigen (Art. 35 Abs. 8 DSGVO).

Für die Aufsichtsbehörde bewirken einmal genehmigte Verhaltensregeln (ungeachtet der konkurrierenden Zuständigkeit zwischen Überwachungsstelle und Aufsichtsbehörde für deren Einhaltung) eine (faktische) Selbstbindung,¹⁰ wodurch ein Maß an Rechtssicherheit erlangt wird, wie es für die DSGVO bemerkenswert ist.¹¹

4. Wer kann Verhaltensregeln ausarbeiten?

Gemäß dem Wortlaut der DSGVO können Verbände oder andere «Vereinigungen» die Kategorien von Verantwortlichen oder Auftragsverarbeitern vertreten, Verhaltensregeln ausarbeiten, was darauf hinweist, dass die vertretenen Verantwortlichen oder Auftragsverarbeiter entsprechende Gemeinsamkeiten aufweisen müssen. Hier ist in erster Linie an Branchenvereinigungen zu denken. Vereine die sich zu Verbänden zusammenschließen, sind ebenfalls vorlageberechtigt.¹²

Die DSB gibt dazu an, dass als Antragsteller insbesondere gesetzliche Interessenvertretungen (etwa Kammern oder Berufsverbände) oder private Verbände und Vereinigungen (etwa freiwillige Zusammenschlüsse)

⁶ Vgl. HÖTZENDORFER in Gantschacher/Jelinek/Schmidl/Spanberger, DSGVO, 2017, Art. 40 Rz 2 m.w.N.

⁷ Vgl. SPOHN/NÖDL/MARKOWSKI in Feiler/Raschhofer (Hrsg.), Innovation und internationale Rechtspraxis, Praxisschrift für Wolfgang Zankl, 2009, S. 546.

⁸ Vgl. FEILER/FORGÓ, EU-DSGVO, 2017, Art. 40, Rz 1.

⁹ Vgl. auch Informationsschreiben der DSB zum Thema Verhaltensregeln <https://www.dsb.gv.at/documents/22758/844171/Verhaltensregeln.pdf/fb4e8d2d-6cbc-43fc-80b6-d91318b24874> (alle in diesem Beitrag zitierten Internetquellen wurden am 7. Januar 2019 zuletzt aufgerufen).

¹⁰ Vgl. LEPPERHOFF in Gola (Hrsg.), DS-GVO, 2018, Art. 40 Rz 23; zur Frage der Rechtswirkungen und Selbstbindung siehe (für Deutschland) BERGT in Kühling/Buchner (Hrsg.), Datenschutz-Grundverordnung, 2018, Art. 40 Rz 40 ff.

¹¹ Vgl. BERGT in Kühling/Buchner (Hrsg.), Datenschutz-Grundverordnung, 2018, Art. 40 Rz 1. Zur österreichischen Rechtslage siehe BERKA Grundrechte – Grundfreiheiten und Menschenrechte in Österreich, Springer, 1999, Rz 986; VfGH, VfSlg. 8375/1978.

¹² Vgl. BERGT in Kühling/Buchner (Hrsg.), Datenschutz-Grundverordnung, 2018, Art. 40 Rz 14.

legitimiert sind, die bescheinigen können, dass sie eine relevante Anzahl von Verantwortlichen oder Auftragsverarbeitern vertreten. Im Umkehrschluss bedeutet dies, dass einzelne oder bloß wenige Verantwortliche oder Auftragsverarbeiter keine ausreichende Vertretungsrelevanz besitzen, um einen Antrag auf Genehmigung von Verhaltensregeln stellen zu können. Damit soll auch verhindert werden, dass unterschiedliche Verhaltensregeln innerhalb derselben Branche entworfen werden.¹³ Denkbar ist auch, Vereinigungen zum Zweck der Ausarbeitung von Verhaltensregeln zu gründen, wenn die Vereinigung (weiterhin) Beständigkeit aufweist.¹⁴

In der Literatur wird auch die Möglichkeit der Ausarbeitung von Verhaltensregeln für Konzerne bzw. Unternehmensgruppen befürwortet, sofern entsprechende Gemeinsamkeiten existieren,¹⁵ rein Unternehmensinterne Verhaltensregeln dürften jedoch nicht vorlagefähig sein.¹⁶

5. Zulässiger Inhalt von Verhaltensregeln

Inhaltlich setzt die DSGVO den Verhaltensregeln grundsätzlich keine Grenzen, solange diese Präzisierungen enthalten. Die Verhaltensregeln können einen breiten oder aber auch einen eingeschränkten Bereich regeln, je nachdem, wo Präzisierungsbedarf gegeben ist. Präzisierungen können etwa zu folgenden Aspekten erfolgen (Art 40 Abs 2 DSGVO):

- faire und transparente Verarbeitung
- berechnigte Interessen des Verantwortlichen in bestimmten Zusammenhängen
- Erhebung personenbezogener Daten
- Pseudonymisierung personenbezogener Daten
- Unterrichtung der Öffentlichkeit und der betroffenen Personen
- Ausübung der Rechte betroffener Personen
- Unterrichtung und Schutz von Kindern und Art und Weise, in der die Einwilligung des Trägers der elterlichen Verantwortung für das Kind einzuholen ist
- Maßnahmen und Verfahren gem. den Art. 24 und 25 DSGVO und die Maßnahmen für die Sicherheit der Verarbeitung gem. Art. 32 DSGVO
- Meldung von Verletzungen des Schutzes personenbezogener Daten an Aufsichtsbehörden und die Benachrichtigung der Betroffenen
- Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen oder
- außergerichtliche Verfahren und sonstige Streitbeilegungsverfahren zur Beilegung von Streitigkeiten zwischen Verantwortlichen und Betroffenen

Diese demonstrative¹⁷ Aufzählung enthält für die Praxis bedeutende Punkte, wie etwa die «berechtigten Interessen» des Verantwortlichen in bestimmten Zusammenhängen oder Präzisierungen hinsichtlich der notwendigen Transparenz von Verarbeitungen. Zudem kann auch eine Präzisierung der technischen und organisatorischen Maßnahmen erfolgen.

Verhaltensregeln müssen jedoch ausreichend auf die spezifischen Fragen und Probleme der Branche bzw. Gruppe eingehen und dafür auch ausreichend klare Lösungen vorsehen, wobei es zulässig ist sich auf einzelne

¹³ Informationsschreiben der DSB zum Thema Verhaltensregeln <https://www.dsb.gv.at/documents/22758/844171/Verhaltensregeln.pdf/fb4e8d2d-6cbc-43fc-80b6-d91318b24874>.

¹⁴ Vgl. BERGT in Kühling/Buchner (Hrsg.), Datenschutz-Grundverordnung, 2018, Art. 40 Rz 13.

¹⁵ Vgl. PAAL in Paal/Pauly (Hrsg.), Datenschutz-Grundverordnung, 2017, Art. 40 Rz 11; BERGT in Kühling/Buchner (Hrsg.), Datenschutz-Grundverordnung, 2018, Art. 40. Rz 13 unter Verweis auf BERGT/BERTEMANN in Koreng/Lachenmann (Hrsg.), Formularhandbuch Datenschutzrecht, S. 185.

¹⁶ Vgl. PAAL in Paal/Pauly (Hrsg.), Datenschutz-Grundverordnung, 2017, Art. 40 Rz 9, der die Vorlage von bloß unternehmensintern wirkenden Verhaltensregeln ablehnt.

¹⁷ Vgl. auch Informationsschreiben der DSB zum Thema Verhaltensregeln <https://www.dsb.gv.at/documents/22758/844171/Verhaltensregeln.pdf/fb4e8d2d-6cbc-43fc-80b6-d91318b24874>.

Punkte zu beschränken.¹⁸ Sie müssen somit einen «gewissen»¹⁹ branchenspezifischen Mehrwert bieten²⁰ und sind bei einer bloßen Wiederholung des Wortlautes der DSGVO, nicht genehmigungsfähig.²¹ Allgemeine Verweise («Soweit gemäß Art. 6 DSGVO zulässig») oder unpräzise Vorgaben («Die Speicherfristen richten sich nach der BAO») schaffen auch Sicht der DSB keinen relevanten Mehrwert.²² Unterschreitungen des Schutzniveaus der DSGVO sind ebenfalls nicht genehmigungsfähig.²³

Hier ist auch zu berücksichtigen, dass ein Verfahren zur Genehmigung von Verhaltensregeln keine Einzelfallprüfung zum Gegenstand hat, sondern genehmigte Verhaltensregeln generell abstrakte Wirkung besitzen. Daher ist es nicht möglich, durch Verhaltensregeln bestimmte Verarbeitungsvorgänge/bestimmte Geschäftsmodelle allgemein für zulässig zu erklären («Die berechtigten Interessen des Verantwortlichen überwiegen»). Es muss stets genug Spielraum für die Beurteilung im Einzelfall übrigbleiben.²⁴

6. Der Genehmigungsprozess

Die Verhaltensregeln müssen ein mehrstufiges Verfahren bis zu ihrer Genehmigung durchlaufen. Nach Erarbeitung in Zusammenarbeit mit den relevanten Stakeholdern («maßgebliche Interessenträger») und nach erfolgter Einreichung gibt die zuständige Aufsichtsbehörde eine Stellungnahme dahingehend ab, ob sie den Entwurf für mit der DSGVO vereinbar hält und ausreichende Garantien geboten werden.²⁵

Der ErwGr. 99 DSGVO weist darauf hin, dass während des Ausarbeitungsprozesses (oder bei der Änderung oder Erweiterung solcher Verhaltensregeln) Verbände und oder andere Vereinigungen die maßgeblichen Interessenträger und möglichst auch die betroffenen Personen konsultieren und die Eingaben und Stellungnahmen, die sie dabei erhalten, berücksichtigt werden sollen. Erfolgt diese Konsultation nicht, hat dies jedoch keine Rechtswidrigkeit zur Folge,²⁶ kann jedoch das Genehmigungsverfahren erschweren.²⁷

Sämtliche genehmigte Verhaltensregeln werden in ein Verzeichnis aufgenommen und veröffentlicht.²⁸ Die DSB veröffentlicht genehmigte Verhaltensregeln auf ihrer Homepage sowie im Rechtsinformationssystem (RIS).²⁹ Zudem nimmt der Europäische Datenschutzausschuss alle genehmigten Verhaltensregeln in ein Register auf und veröffentlicht diese.³⁰ Sofern sich Verantwortliche und Auftragsverarbeiter genehmigten Verhaltensregeln unterwerfen, kann diese Außenwirkung jedenfalls werbewirksame Effekte mit sich bringen.³¹

Bei Antragstellung muss der Behörde ausdrücklich mitgeteilt werden, ob entworfene Verhaltensregeln auf Verarbeitungstätigkeiten in mehreren Mitgliedstaaten abzielen («internationale Verhaltensregeln») oder ob die

¹⁸ Vgl. BERGT in Kühling/Buchner (Hrsg.), Datenschutz-Grundverordnung, 2018, Art. 40 Rz 18.

¹⁹ Siehe dazu auch Informationsschreiben der DSB zum Thema Verhaltensregeln <https://www.dsb.gv.at/documents/22758/844171/Verhaltensregeln.pdf/fb4e8d2d-6cbc-43fc-80b6-d91318b24874>.

²⁰ Vgl. PAAL in Paal/Pauly (Hrsg.), Datenschutz-Grundverordnung, 2017, Art. 40 Rz 15. Ebenso LEPPERHOFF, in: Gola, DS-GVO (Hrsg.), Art. 40 Rz 13.

²¹ Vgl. BERGT in Kühling/Buchner (Hrsg.), 2018, Art. 40 Rz 18.

²² Informationsschreiben der DSB zum Thema Verhaltensregeln <https://www.dsb.gv.at/documents/22758/844171/Verhaltensregeln.pdf/fb4e8d2d-6cbc-43fc-80b6-d91318b24874>.

²³ Vgl. BERGT in Kühling/Buchner (Hrsg.), 2018, Rz 17. Vgl. auch Informationsschreiben der DSB zum Thema Verhaltensregeln <https://www.dsb.gv.at/documents/22758/844171/Verhaltensregeln.pdf/fb4e8d2d-6cbc-43fc-80b6-d91318b24874>.

²⁴ Vgl. Informationsschreiben der DSB zum Thema Verhaltensregeln <https://www.dsb.gv.at/documents/22758/844171/Verhaltensregeln.pdf/fb4e8d2d-6cbc-43fc-80b6-d91318b24874>.

²⁵ Vgl. LEPPERHOFF in Gola (Hrsg.), DS-GVO, 2018, Art. 40 Rz 25.

²⁶ Vgl. LEPPERHOFF in Gola (Hrsg.), DS-GVO, 2018, Art. 40 Rz 12 m.w.N.; BERGT in Kühling/Buchner (Hrsg.), Datenschutz-Grundverordnung, 2018, Art. 40 Rz 24.

²⁷ Vgl. PAAL in Paal/Pauly (Hrsg.), DS-GVO, 2017, Art. 40 Rz 16.

²⁸ Vgl. Art. 40 Abs. 6 DSGVO.

²⁹ Informationsschreiben der DSB zum Thema Verhaltensregeln <https://www.dsb.gv.at/documents/22758/844171/Verhaltensregeln.pdf/fb4e8d2d-6cbc-43fc-80b6-d91318b24874>.

³⁰ Siehe Website des Europäischen Datenschutzausschusses: https://edpb.europa.eu/our-work-tools/consistency-findings/register-for-decisions_de.

³¹ Vgl. BERGT in Kühling/Buchner (Hrsg.), Datenschutz-Grundverordnung, 2018, Art. 40 Rz 2.

Verhaltensregeln sich in der Erfassung von inländischen Verarbeitungstätigkeiten erschöpfen («nationale Verhaltensregeln»). Dies ist insofern wichtig, als die DSB nationale Verhaltensregeln selbst genehmigen kann.³² Wenn sich die Verhaltensregeln auf Verarbeitungstätigkeiten in mehreren Mitgliedstaaten beziehen, hat die angerufene Aufsichtsbehörde den Entwurf der Verhaltensregeln zusammen mit ihrer Stellungnahme zum Entwurf dem Europäischen Datenschutzausschuss vorzulegen, der ein Kohärenzverfahren durchführt (Art. 40 Art. 7 DSGVO).³³

7. Bindung an die Verhaltensregeln

Verhaltensregeln werden nicht mit ihrer Genehmigung verbindlich, sondern erst, wenn ihre Einhaltung etwa durch eine Satzung vorgeschrieben wird oder wenn eine freiwillige Selbstverpflichtung durch den Verantwortlichen oder Auftragsverarbeiter erfolgt.³⁴ Die Teilnahme ist grundsätzlich fakultativ, weshalb sich Verantwortliche und Auftragsverarbeiter proaktiv den genehmigten Verhaltensregeln unterwerfen müssen. Nur die Unterwerfung unter genehmigte Verhaltensregeln, die durch eine akkreditierte Stelle überwacht werden, löst die oben genannten Wirkungen aus.³⁵

Unklar ist, ob sich auch Nichtmitglieder den Verhaltensregeln eines Verbandes unterwerfen können.³⁶ Als Auslegungshilfe befolgt werden können Verhaltensregeln jedoch jedenfalls stets auch von Nichtmitgliedern. Die DSB hat die Möglichkeit einer Unterwerfung unter Verhaltensregeln durch Nichtmitglieder, die der betreffende Branchenverband jedoch ablehnen kann, genehmigt.³⁷ Problematisch kann dies in Bezug auf Tätigkeit und Finanzierung der Überwachungsstelle erscheinen.

8. Überwachungsstelle und Sanktionen

Obwohl der Wortlaut von Art. 41 DSGVO das Gegenteil vermuten lässt, ist eine Stelle, welche die Einhaltung der Verhaltensregeln zu überwachen hat, zwingend vorgeschrieben.³⁸ Überwachungsstellen sind in Art. 40 und 41 DSGVO geregelt. Diese legen fest, dass die Überwachung der Verhaltensregeln von einer Stelle durchgeführt werden kann, die über das geeignete Fachwissen verfügt und von der Aufsichtsbehörde akkreditiert worden ist.³⁹ Eine Überwachungsstelle ist eine private Stelle, die mit der obligatorischen Überwachung der Verhaltensregeln betraut wird.⁴⁰ Trotz des Bestehens einer Überwachungsstelle und der Möglichkeit alternative Streitbeilegungsverfahren durch Verhaltensregeln zu schaffen, bleiben die Befugnisse der Aufsichtsbehörde stets unangetastet.

³² Vgl. auch Informationsschreiben der DSB zum Thema Verhaltensregeln <https://www.dsb.gv.at/documents/22758/844171/Verhaltensregeln.pdf/fb4e8d2d-6cbc-43fc-80b6-d91318b24874>.

³³ Vgl. BERGT in Kühling/Buchner (Hrsg.), Datenschutz-Grundverordnung, 2018, Art. 40 Rz 30; Informationsschreiben der DSB zum Thema Verhaltensregeln <https://www.dsb.gv.at/documents/22758/844171/Verhaltensregeln.pdf/fb4e8d2d-6cbc-43fc-80b6-d91318b24874>.

³⁴ Vgl. BERGT in Kühling/Buchner (Hrsg.), Datenschutz-Grundverordnung, 2018, Art. 40 Rz 8. So auch WOLFF in Schantz/Wolff, (Hrsg.), Das neue Datenschutzrecht, 2017, S. 389 Rz 1283.

³⁵ Informationsschreiben der DSB zum Thema Verhaltensregeln <https://www.dsb.gv.at/documents/22758/844171/Verhaltensregeln.pdf/fb4e8d2d-6cbc-43fc-80b6-d91318b24874>.

³⁶ Vgl. LEPPERHOFF in Gola (Hrsg.), DS-GVO, 2018, Art. 40 Rz 17, der die Öffnung an Nichtmitglieder befürwortet.

³⁷ ISPA – Internet Service Providers Austria, Datenschutzgrundverordnung – Code of Conduct für Internet Service Provider Version 1.0. v. 26.11.2018: Geltungsbereich: Diesen Verhaltensregeln können sich Internet Service Provider, welche öffentliche Kommunikationsnetze oder -dienste bereitstellen und über eine Allgemeinenehmigung im Sinne von § 15 TKG verfügen, unterwerfen.

³⁸ Vgl. BERGT in Kühling/Buchner (Hrsg.), Datenschutz-Grundverordnung, 2018, Art. 40 Rz 20. Siehe auch Informationsschreiben der DSB: <https://www.dsb.gv.at/documents/22758/844171/Verhaltensregeln.pdf/fb4e8d2d-6cbc-43fc-80b6-d91318b24874>.

³⁹ Vgl. LEPPERHOFF in Gola (Hrsg.), DS-GVO, 2018, Art. 41 Rz 5.

⁴⁰ Informationsschreiben der DSB zum Thema Verhaltensregeln <https://www.dsb.gv.at/documents/22758/844171/Verhaltensregeln.pdf/fb4e8d2d-6cbc-43fc-80b6-d91318b24874>.

8.1. Stellung und Tätigkeit der Überwachungsstelle

Umstritten ist, ob eine Überwachungsstelle i.S.v. Art. 41 DSGVO gesondert einzurichten ist⁴¹ oder ob eine Überwachung auch durch eine andere externe Stelle, wie eine Aufsichtsbehörde⁴² oder den Verband selbst erfolgen kann.⁴³ Hier ist u.E. nach dem Schutzzweck der Norm darauf zu achten, dass eine Einrichtung der Überwachungsstelle im Verband so erfolgt, dass durch die Gestaltung der Verfahren und begleitende Sicherheitsmechanismen die Objektivität der Überwachungsstelle nicht durch Interessenskonflikte kompromittiert ist.

Verhaltensregeln müssen geeignete Sanktionsregelungen für jene Fälle vorsehen, in denen Überwachungsstellen Verstöße gegen Verhaltensregeln feststellen. Dabei kann es sich etwa um vorläufige oder endgültige Ausschlüsse von den Verhaltensregeln handeln. Die Aufsichtsbehörde muss zusätzlich über solche Maßnahmen informiert werden.⁴⁴

Unklar ist, ob zur Begründung der Rechte einer Überwachungsstelle bereits eine einseitige Verpflichtungserklärung ausreicht, oder ob eine vertragliche Konstruktion erforderlich ist.⁴⁵

Die Überwachung durch die Überwachungsstelle muss geeignet sein, Verstöße gegen die Selbstverpflichtung aufzudecken, so kann etwa eine stichprobenartige Kontrolle vorgesehen werden. Eine Vor-Ort-Kontrolle ist nicht zwingend erforderlich und der Einsatz von qualifizierten Dritten, wie etwa Auditoren, zulässig.⁴⁶

Die Überwachungsstelle muss unabhängig sein, worunter eine personelle, rechtliche oder wirtschaftliche Unabhängigkeit zu verstehen ist. Dies soll auch sicherstellen, dass kein «race-to-the-bottom», erfolgen kann.⁴⁷ Gesellschaftsrechtliche, personelle oder sonstige wirtschaftliche Verbindungen zu den zu kontrollierenden Einrichtungen schaden dann nicht, wenn sichergestellt wird, dass keine Interessenkonflikte vorliegen.⁴⁸ Eine erforderliche Finanzierung sollte dabei durch alle überwachten Verantwortlichen bzw. Auftragsverarbeiter erfolgen. Zudem muss die Überwachungsstelle das erforderliche datenschutzrechtliche und branchenspezifische Fachwissen aufweisen und ein gewisses technisches und organisatorisches Verständnis vorhanden sein.⁴⁹

Es müssen Verfahren festgelegt sein, nach denen die Stelle die Konformität erheben und die Überwachung durchführen wird.⁵⁰ Prüfschemata müssen dabei so detailliert sein, dass überprüfte Unternehmen erkennen können, welche Erfordernisse sie erfüllen müssen.⁵¹ Dabei könnten etwa umfangreiche detaillierte Checklisten erstellt und verwendet werden. Darüber hinaus müssen Kriterien festgelegt sein, nach denen die Auswahl der Verantwortlichen oder Auftragsverarbeiter bei der Durchführung der Prüf- und Überwachungskompetenz erfolgt.⁵² Die Überwachungsstelle muss zudem Strukturen und Verfahren festgelegt haben, mit denen sie Beschwerden in Zusammenhang mit den Verhaltensregeln nachgehen kann, wobei diese für betroffene Personen und die Öffentlichkeit transparent gemacht werden.

Sofern die Überwachungsstelle die gebotenen Maßnahmen gegen ein Unternehmen nicht ergreift oder die Aufsichtsbehörde nicht über ergriffene Maßnahmen in Kenntnis setzt, ist dies – gemäß Art. 83 Abs. 4 lit. c DSGVO mit einer Geldbuße bis zu €10. Mio oder zwei Prozent des weltweiten Vorjahresumsatzes bedroht.

⁴¹ Vgl. BERGT in Kühling/Buchner, DS-GVO (Hrsg.), Datenschutz-Grundverordnung, 2018, Art. 40 Rz 22.

⁴² Vgl. BRAUNMÜHL in Plath (Hrsg.), BDSG/DS-GVO, 2016, Art. 40 Rz 13.

⁴³ Vgl. LEPPERHOFF in Gola (Hrsg.), DS-GVO, 2018, Art. 41 Rz 5.

⁴⁴ Vgl. LEPPERHOFF in Gola (Hrsg.), DS-GVO, 2018, Art. 41 Rz 8.

⁴⁵ Vgl. BERGT in Kühling/Buchner (Hrsg.), Datenschutz-Grundverordnung, 2018, Art. 40 Rz 22.

⁴⁶ Vgl. LEPPERHOFF in Gola (Hrsg.), DS-GVO, 2018, Art. 41, Rz 9.f.

⁴⁷ Vgl. BERGT in Kühling/Buchner (Hrsg.), Datenschutz-Grundverordnung, 2018, Rz 22.

⁴⁸ Vgl. LEPPERHOFF in Gola (Hrsg.), DS-GVO, 2018, Art. 41, Rz 16.

⁴⁹ Vgl. KRÖPFL, Datenschutzrechtliche Verhaltensregeln in Jähnel (Hrsg.), Datenschutzrecht, Jahrbuch 2018, S. 138.

⁵⁰ Vgl. KRÖPFL, Datenschutzrechtliche Verhaltensregeln in Jähnel (Hrsg.), Datenschutzrecht, Jahrbuch 2018, S. 138.

⁵¹ Vgl. KRÖPFL, Datenschutzrechtliche Verhaltensregeln in Jähnel (Hrsg.), Datenschutzrecht, Jahrbuch 2018, S. 138.

⁵² Vgl. RASCHAUER in Sydow (Hrsg.), Europäische Datenschutzgrundverordnung, 2017, Art. 41 Rz 18.

8.2. Akkreditierung der Überwachungsstelle

Bei der Schaffung von Verhaltensregeln, kann nur eine durch die DSB akkreditierte Stelle als Überwachungsstelle ausgewählt werden. Künftige Überwachungsstellen müssen einen Antrag auf Akkreditierung stellen.⁵³ Der Antrag muss die konkrete Bezeichnung der Verhaltensregeln oder des Bereichs von genehmigten Verhaltensregeln, für den die Akkreditierung erfolgen soll, beinhalten.⁵⁴ Die genaueren Voraussetzungen dieser Akkreditierung werden nach Information der DSB voraussichtlich in der ersten Jahreshälfte 2019 mittels einer eigenen Akkreditierungs-Verordnung durch die DSB kundgemacht.⁵⁵ Die Akkreditierungsvoraussetzungen müssen von der nationalen Aufsichtsbehörde dem Datenschutzausschuss übermittelt werden.⁵⁶ Im Wege des Kohärenzverfahrens gemäß Art. 63 DSGVO hat der Europäische Datenschutz-Ausschuss Stellung zu beziehen. Umstritten ist, ob die Überwachungsstelle einen Sitz im entsprechenden Mitgliedstaat haben muss.⁵⁷

Bereits vor Erlass der nationalen Akkreditierungs-Verordnung können Anträge auf die Genehmigung von Verhaltensregeln gestellt werden. Die DSB genehmigt Verhaltensregeln bis zu diesem Zeitpunkt nur unter der aufschiebenden Bedingung, dass die jeweilige Verhaltensstelle nachfolgend akkreditiert wird.⁵⁸

Sofern eine Überwachungsstelle die Voraussetzungen für ihre Akkreditierung nicht oder nicht mehr erfüllt, oder wenn die Stelle Maßnahmen ergreift, die nicht mit der DSGVO vereinbar sind, hat die Aufsichtsbehörde die Akkreditierung zu widerrufen.

9. Förderungspflicht

Gemäß Art. 40 DSGVO sollen die Mitgliedstaaten, die Aufsichtsbehörden, der Ausschuss und die Kommission die Ausarbeitung von Verhaltensregeln fördern, die nach Maßgabe der Besonderheiten der einzelnen Verarbeitungsbereiche und der besonderen Bedürfnisse von Kleinstunternehmen sowie kleinen und mittleren Unternehmen zur ordnungsgemäßen Anwendung dieser Verordnung beitragen sollen.⁵⁹ Diese Förderpflicht war bereits in der Datenschutz-Richtlinie vorgesehen.⁶⁰ In Art. 57 Abs. 1 lit. m DSGVO wird den Aufsichtsbehörden explizit die Pflicht auferlegt, die Ausarbeitung von Verhaltensregeln zu fördern. Die Aufsichtsbehörden haben dabei Stellungnahmen abzugeben und Verhaltensregeln die ausreichende Garantien gemäß Art. 40 Abs. 5 DSGVO bieten, zu genehmigen.

In welcher Form die Aufsichtsbehörden bzw. die anderen in Art. 40 Abs. 1 DSGVO genannten Stellen, die Ausarbeitung von Verhaltensregeln zu fördern haben, legt die DSGVO jedoch nicht fest. Darunter wird die Schaffung eines Umfeldes zu verstehen sein, welches dafür sorgt, dass sich selbstregulatorische Verhaltensregeln zu einem wirksamen Instrument datenschutzrechtlicher Selbstkontrolle entwickeln können.⁶¹

Die Förderung der Ausarbeitung könnte grundsätzlich durch eine Vielzahl an Maßnahmen, wie etwa Beratungen⁶² oder eine vermehrte Öffentlichkeitsarbeit für die Erstellung von Verhaltensregeln durch die Aufsichtsbehörden, erfolgen. Auch sind finanzielle Unterstützungen,⁶³ etwa in Form von Förderungen, denkbar. In der Literatur wurde diesbezüglich angeregt, dass von Seiten des Europäischen Datenschutzausschusses und der

⁵³ Vgl. KRÖPFL, Datenschutzrechtliche Verhaltensregeln in Jähnel (Hrsg.), Datenschutzrecht, Jahrbuch 2018, S. 137.

⁵⁴ Vgl. KRÖPFL, Datenschutzrechtliche Verhaltensregeln in Jähnel (Hrsg.), Datenschutzrecht, Jahrbuch 2018, S. 140.

⁵⁵ Informationsschreiben der DSB zum Thema Verhaltensregeln <https://www.dsb.gv.at/documents/22758/844171/Verhaltensregeln.pdf/fb4e8d2d-6cbc-43fc-80b6-d91318b24874>.

⁵⁶ Vgl. Art. 41 Abs. 3 DSGVO.

⁵⁷ Verneinend KRÖPFL, Datenschutzrechtliche Verhaltensregeln in Jähnel (Hrsg.), Datenschutzrecht, Jahrbuch 2018, S. 137.; aA RASCHAUER in Sydow (Hrsg.), Europäische Datenschutzgrundverordnung, 2017, Art. 41 Rz 20.

⁵⁸ Informationsschreiben der DSB zum Thema Verhaltensregeln <https://www.dsb.gv.at/documents/22758/844171/Verhaltensregeln.pdf/fb4e8d2d-6cbc-43fc-80b6-d91318b24874>.

⁵⁹ Vgl. dazu auch die Empfehlung 2003/361/EG der Kommission.

⁶⁰ Vgl. ErWG 61 zu RL 1995/46/EG.

⁶¹ Vgl. PAAL in Paal/Pauly (Hrsg.), DSGVO, 2017, Art. 40 Rz 5.

⁶² Vgl. LEPPERHOFF in Gola, DS-GVO, 2018, Art. 40 Rz 7.

⁶³ RASCHAUER in Sydow (Hrsg.), Europäische Datenschutzgrundverordnung, 2017, Art. 41 Rz 20.

öster. DSB eine detailliertere Klarstellung erfolgen sollte, was von Entwürfen zu Verhaltensregeln erwartet werde und wie die Ausgestaltung zu erfolgen habe.⁶⁴

10. Aktueller Stand und Ausblick

Bislang⁶⁵ wurden – nach Kenntnis der AutorInnen – sechs Verhaltensregeln bei der DSB eingereicht und ein Antrag – jener der ISPA (Internet Service Providers Austria) – «aufschiebend bedingt» genehmigt. Die bisherigen Praxiserfahrungen mit der österreichischen DSB zeigen auf, dass die DSB bislang unterschiedliche Vorgehensweisen gewählt hat und die Bandbreite von nicht näher begründeten Untersagungen einzelner Bestimmungen von Verhaltensregeln bis zu detaillierten Ausführungen inklusive der Erteilung Verbesserungsvorschlägen hinsichtlich von Inhalten in Verhaltensregeln reicht. Eine Problematik ist dabei, dass nicht nur die Einreichung von Verhaltensregeln,⁶⁶ sondern vor allem der Erstellungsprozess von Verhaltensregeln in der Regel mit Kosten durch den Zukauf von Beratungsleistungen verbunden ist und daher (durchaus unpräjudizielle) Vorabgespräche bzw. Vorabbegegnungen von Entwürfen sinnvoll wären, um unnötige Aufwendungen zu vermeiden.

Da Verfahren zur Genehmigung von Verhaltensregeln – anders als Beschwerdeverfahren – keine Einzelfallprüfung zum Gegenstand haben, sondern diese generell abstrakte Wirkung besitzen (und gerade keine allgemeine Genehmigung von Geschäftsmodellen in Form von Verhaltensregeln erfolgen kann),⁶⁷ wären solche Vorgehensweisen uE von der Förderpflicht in Art. 40 und Art. 57 Abs. 1 lit. m DSGVO gedeckt.

Die bisherigen Erfahrungen zeigen auch, dass nicht nur auf der rechtlichen Ebene viele Aspekte zu berücksichtigen sind, sondern auch ausreichend viele Abstimmungsrunden und Feedbackschleifen durchzuführen sind, um die Meinung der Verbandsmitglieder im Zuge der Ausarbeitung ausreichend zu berücksichtigen. Verhaltensregeln können sich nur dann zu einem erfolgreichen Instrument der datenschutzrechtlichen Selbstregulierung entwickeln, wenn sie von der Zustimmung möglichst vieler Branchenmitglieder getragen werden. Dabei ist die gemeinsame Erarbeitung jener Verarbeitungskonstellationen wesentlich, die Präzisionsbedarf aufweisen. Hier können Konstellationen zu Tage treten, in denen in manchen Bereichen bestimmte Regulierungen mangels ausreichender Homogenität von Verbandsmitgliedern nicht erarbeitet werden können.

⁶⁴ Vgl. KRÖPFL, Datenschutzrechtliche Verhaltensregeln, in Janel (Hrsg.), Datenschutzrecht, Jahrbuch 2018, S. 140.

⁶⁵ Stand, Jänner 2019.

⁶⁶ Ein Antrag auf Genehmigung von Verhaltensregeln an die DSB löst eine Gebührenpflicht aus. Siehe dazu Informationsschreiben der DSB zum Thema Verhaltensregeln <https://www.dsb.gv.at/documents/22758/844171/Verhaltensregeln.pdf/fb4e8d2d-6cbc-43fc-80b6-d91318b24874>.

⁶⁷ Informationsschreiben der DSB zum Thema Verhaltensregeln <https://www.dsb.gv.at/documents/22758/844171/Verhaltensregeln.pdf/fb4e8d2d-6cbc-43fc-80b6-d91318b24874>.