

**Handlungs-
empfehlungen**

- **Rechtssicherheit durch europaweit einheitliche Rechtsanwendung:** keine neuen Auslegungsfragen schaffen
- **Bürokratieabbau:** nicht datenintensive Verarbeitungen – v.a. im B2B-Bereich – von unnötigen Informations- und Dokumentationspflichten entlasten
- **Auftragverarbeiter sind keine „Empfänger“:** Informations- und Auskunftspflichten auf echte Dritte beschränken
- **EU-weite Standards:** einheitliche Vorgaben zu Datenschutz-Folgenabschätzungen und Datenpannen etablieren
- **Innovationsfähiger Datenschutz:** klare, praktikable Regeln für KI, Pseudonymisierung und biometrische Verfahren sind Voraussetzung

EWE begrüßt die Bemühungen der EU-Kommission, die DSGVO durch die Vorschläge in **Art. 3 des Digital Omnibusses COM (2025) 837** v. 19.11.2025 für die Wirtschaft praktikabler zu gestalten und dennoch ein hohes Datenschutzniveau zu gewährleisten. Dennoch sieht EWE bei vielen Änderungen weiteren Anpassungs- beziehungsweise Konkretisierungsbedarf. Mit den aktuellen Änderungen wird das Risiko erhöht, neue Rechtsunsicherheiten zu schaffen, die nur schwer abzusehen sind. Folgenden Anpassungsbedarf sehen wir bei den aktuellen Vorschlägen:

1. Artikel 4 Nummer 1 DSGVO-neu

Im Artikel 4 Nummer 1 DSGVO sollen folgende Sätze angefügt werden:

“Information relating to a natural person is not necessarily personal data for every other person or entity, merely because another entity can identify that natural person. Information shall not be personal for a given entity where that entity cannot identify the natural person to whom the information relates, taking into account the means reasonably likely to be used by that entity. Such information does not become personal for that entity merely because a potential subsequent recipient has means reasonably likely to be used to identify the natural person to whom the information relates.”

Generell begrüßen wir den Ansatz und halten es grundsätzlich für notwendig, dass Informationen einer natürlichen Person, die für andere Personen oder Stellen keinen Personenbezug mehr enthalten, nicht mehr unter den Anwendungsbereich der DSGVO fallen. Die aktuelle Formulierung hat jedoch viel Auslegungsspielraum und sorgt insofern für Rechtsunsicherheit in der praktischen Anwendung.

Es ist nach der aktuellen Formulierung unklar, bei wem die Verantwortung zur Prüfung liegt, ob der Empfänger bei Daten im Sinne dieser Neuregelung wieder einen Personenbezug herstellen kann. Es stellt sich zudem die Frage, ob ein Empfänger in einer Verarbeitungskette noch erkennen kann, ob es lediglich Daten im Sinne der Neuregelung des Artikel Nummer 1 DSGVO-neu sind, schon anonymisierte Daten oder Daten, die nie einen Personenbezug hatten. Weitere Unklarheiten ergeben sich auch, wenn die Verarbeitungskette das EU-Ausland betrifft.

Sollte Artikel 4 Nummer 1 DSGVO-neu so bestehen bleiben, möchten wir darauf hinweisen, dass sich durch diese Neuregelung absehbare Auswirkungen ergeben werden, welche zumindest hinsichtlich derjenigen Konstellationen betrachtet und unmittelbar gesetzlich geregelt werden sollten, welche in der DSGVO vorgesehen sind.

Dem Gedanken aus Artikel 4 Nummer 1 DSGVO-neu folgend würde in Artikel 26 und Artikel 28 DSGVO weiterer Anpassungsbedarf bestehen, da für diese Daten keine weitreichenden Vereinbarungen notwendig erscheinen. So sollten für Daten nach Artikel 4 Nummer 1 Satz 2- neu klargestellt werden, welche Regelungen nach Artikel 26 oder Art 28 DSGVO auf diese anwendbar sein sollen. Sollte weiterhin der ganze Artikel 28 DSGVO anwendbar sein, bringt die Anpassung in Artikel 4 Nummer 1 DSGVO-neu nicht die notwendige und begrüßenswerte Entlastung für die Wirtschaft.

Daher schlagen wir vor, dass **Artikel 28 DSGVO nur eingeschränkt gilt** (z.B. nur Artikel 28 Absatz 1 und 2 DSGVO) und das **Artikel 26 DSGVO für Daten nach Artikel 4 Nummer 1 DSGVO-neu nicht anwendbar** ist, soweit der Artikel 26 DSGVO entsprechend unseres Vorschlags (siehe "Weitere Vorschläge" unter Punkt 13) nicht abgeschafft wird.

2. Artikel 9 Absatz 2 DSGVO-neu

Im Artikel 9 Absatz 2 DSGVO sollen folgende Buchstaben angehängt werden:

"[...]

l) processing of biometric data is necessary for the purpose of confirming the identity of a data subject (verification), where the biometric data or the means needed for the verification is under the sole control of the data subject."

Der beabsichtigte Artikel 9 Absatz 2 Buchstabe l DSGVO-neu wird von EWE begrüßt. Wir sehen jedoch dahingehende Probleme, dass die biometrischen Daten oder die für die Verifikation erforderlichen Mittel unter der ausschließlichen Kontrolle ("sole control") der betroffenen Personen stehen müssen. Auf Grund dieses Vorbehalts ist es nicht möglich, biometrische Verfahren selbst für den Zugang von sensiblen/kritischen Bereichen, z. B. Rechenzentren, zu verwenden. Die Regelung sollte dahingehend geändert werden, dass **eine Verarbeitung von biometrischen Daten durch Verantwortliche auch zur Identifizierung von Personen beim Betreten sensibler/kritischer Bereiche möglich** ist.

3. Artikel 12 Absatz 5 DSGVO-neu

Artikel 12 Absatz 5 DSGVO soll folgende Fassung erhalten:

"(5) Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character or also, for requests under Article 15 because the data subject abuses the rights conferred by this regulation for purposes other than the protection of their data, the controller may either:

(a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or

(b) refuse to act on the request. The controller shall bear the burden of demonstrating that the request is manifestly unfounded or that there are reasonable grounds to believe that it is excessive."

EWE begrüßt den Ansatz, die Betroffenenrechte auf die datenschutzrechtlich relevanten Bedürfnisse der betroffenen Personen zu reduzieren und eine missbräuchliche Nutzung der Regelungen auszuschließen. EWE hat jedoch erhebliche Zweifel daran, dass durch den Verantwortlichen die

Beweislast einer missbräuchlichen Nutzung durch eine betroffene Person erbracht werden kann, da das Auskunftsrecht ohne Begründung ausgeübt werden kann.

Ferner wäre es wünschenswert, **dass sowohl bei den Informationspflichten gem. Artikel 13 und 14 DSGVO, als auch bei den Auskunftspflichten gemäß Artikel 15 DSGVO, wie auch unter Artikel 19 DSGVO unter dem Begriff der „Empfänger der Daten“ keine Auftragsverarbeiter zu verstehen sind**, sondern Dritte gem. Artikel 4 Nummer 10 DSGVO.

Nach unserer Auffassung dienen die Regelungen als Information bzw. Auskunft für die betroffene Person, um die ordnungsgemäße Datenverarbeitung überprüfen zu können. Auftragsverarbeiter haben in diesem Zusammenhang jedoch keine eigenständige Tätigkeit, sondern verarbeiten die Daten im Rahmen von Weisungen des Verantwortlichen. Eine eigenständige Verarbeitung der Daten bei dem Empfänger (Auftragsverarbeiter) findet nicht statt. Auch bleibt der Verantwortliche für die Verarbeitung beim Auftragsverarbeiter gegenüber der betroffenen Person verantwortlich. Zur Vereinfachung des Verfahrens und ohne das Risiko für die betroffene Person zu erhöhen, regen wir an, die Auftragsverarbeiter aus dem Kreis der Empfänger herauszunehmen.

Anlässlich der geplanten Änderungen des Artikel 12, regen wir darüberhinausgehend auch eine Änderung des Artikel 15 DSGVO an, welche sich eben in diesen Kontext der Verhinderung rechtsmissbräuchlicher Ausnutzung stellt. Die Praxis hat gezeigt, dass während sich die sogenannte First-Level-Auskunft als weitestgehend unproblematisch und für betroffene Personen stets ausreichend erwies, die tieferegreifende Beauskunftung, unter Berücksichtigung einer Kopie der Daten, im Lichte der zahlreichen, teilweise widersprüchlichen Rechtsprechung als missbrauchsanfällig bestätigt hat. Wir regen daher an, eine **Staffelung des Auskunftsanspruches vorzunehmen, bzw. die Kopie an weitere Erfordernisse zu koppeln** und hierbei der betroffenen Person nur die personenbezogenen Daten zur Verfügung zu stellen, die für eine Überprüfung der Rechtmäßigkeit der Datenverarbeitung erforderlich sind (vgl. Erwägungsgrund 63).

4. Artikel 13 Absatz 4 und 5 DSGVO-neu

Im Artikel 13 DSGVO sollen die Absatz 4 und 5 angefügt werden:

“(4) Paragraphs 1, 2 and 3 shall not apply where the personal data have been collected in the context of a clear and circumscribed relationship between data subjects and a controller exercising an activity that is not data-intensive and there are reasonable grounds to assume that the data subject already has the information referred to in points (a) and (c) of paragraph 1, unless the controller transmits the data to other recipients or categories of recipients, transfers the data to a third country, carries out automated decision-making, including profiling, referred to in Article 22(1), or the processing is likely to result in a high risk to the rights and freedoms of data subjects within the meaning of Article 35.

(5) When the processing takes place for scientific research purposes and the provision of information referred to under paragraphs 1, 2 and 3 proves impossible or would involve a disproportionate effort subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing, the controller does not need to provide the information referred to under paragraphs 1, 2 and 3. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available.”

EWE begrüßt es, nicht datenintensive Verarbeitungen von der Informationspflicht auszunehmen. Allerdings führt diese Regelung in dieser Form in der Praxis zu keiner Erleichterung, da unter

“Empfänger” auch Auftragsverarbeiter umfasst sind. Es ist für eine betroffene Person bei nicht datenintensiven Tätigkeiten entscheidend, ob die Weitergabe der Daten an Dritte im Sinne des Artikel 4 Nr. 10 DSGVO erfolgt ist und nicht welcher Auftragsverarbeiter die Daten erhalten hat. Diese verarbeiten die Daten lediglich im Rahmen von Weisungen des Verantwortlichen. Zur Vereinfachung des Verfahrens und ohne das Risiko für die betroffene Person zu erhöhen, regen wir hier ebenfalls an, die **Auftragsverarbeiter aus dem Kreis der Empfänger herauszunehmen**.

Es wird zudem angeregt, die **nicht datenintensiven Tätigkeiten zu konkretisieren**. So kann insbesondere im B2B-Bereich eine Entbürokratisierung durchgeführt werden, die die Unternehmen entlasten und keine wesentlichen Auswirkungen auf das Gesamtdatenschutzniveau haben. Genannt sei hier **beispielsweise der Verzicht auf den Austausch von Datenschutzinformationen für Mitarbeiterkontaktdaten im geschäftlichen Verkehr zweier Unternehmen**.

5. Artikels 33 Absatz 1 DSGVO-neu

Artikel 33 Absatz 1 DSGVO soll folgendermaßen geändert werden:

“(1) In the case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall without undue delay and, where feasible, not later than 96 hours after having become aware of it, notify the personal data breach via the single-entry point established pursuant to Article 23a of Directive (EU) 2022/2555 to the supervisory authority competent in accordance with Article 55 and Article 56. Where the notification to the supervisory authority is not made within 96 hours, it shall be accompanied by reasons for the delay.”

Insgesamt wird die Änderung des Artikel 33 Absatz 1 DSGVO sehr positiv gesehen. Wir schlagen darüber hinaus eine **Anpassung der Frist zur Meldung bei der Aufsichtsbehörde** vor. Diese sollte **4 Werktage statt 96 Stunden** betragen. Um für Rechtssicherheit zu sorgen schlagen wir vor, dass sich die Frist auf die “Verordnung (EWG, Euratom) Nummer 1182/71 des Rates vom 3. Juni 1971 zur Festlegung der Regeln für die Fristen, Daten und Termine” bezieht. Hiernach werden gemäß Artikel 3 Absatz 3 bei der Fristberechnung keine Feiertage, Sonntage und die Sonnabende berücksichtigt.

6. Artikel 33 Absatz 6 DSGVO-neu

Im Artikel 33 DSGVO der folgende Absatz 6 angefügt werden:

“(6) The Board shall prepare and transmit to the Commission a proposal for a common template for notifying a personal data breach to the competent supervisory authority referred to in paragraph 1 as well as for a list of the circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of a natural person. The proposals shall be submitted to the Commission within [OP date = nine months of the entry into application of this Regulation]. The Commission after due consideration reviews it, as necessary, and is empowered to adopt it by way of an implementing act in accordance with the examination procedure set out in Article 93(2).”

Generell ist der Artikel 33 Absatz 6 DSGVO-neu zu begrüßen. Aus unserer Sicht schafft er Rechtssicherheit bezüglich der Meldung von Verletzungen des Schutzes personenbezogener Daten. Zu diesem Zweck würden wir ergänzend anregen, dass die **Fristen für die Umsetzung durch die Kommission verkürzt** werden.

7. Artikel 35 Absatz 4-6 DSGVO-neu

In Artikel 35 DSGVO sollen die Absätze 4, 5 und 6 folgendermaßen verfasst werden:

“(4) The Board shall prepare and transmit to the Commission a proposal for a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1.

(5) The Board shall prepare and transmit to the Commission a proposal for a list of the kind of processing operations for which no data protection impact assessment is required.

(6) The Board shall prepare and transmit to the Commission a proposal for a common template and a common methodology for conducting data protection impact assessments.”

Grundsätzlich begrüßt EWE eine Standardisierung bezüglich der Umsetzung der Datenschutz-Folgenabschätzung. Wir sehen hierin eine Vereinfachung, soweit die Standardisierung sich umsetzungsfreundlich anwenden lässt. Hierzu gehört auch, dass es **keine zusätzlichen Anforderungen auf nationaler Ebene** geben darf, die zu Mehraufwänden bei der Umsetzung führen.

8. Artikel 35 Absatz 6a - 6c DSGVO-neu

In Artikel 35 sollen die Absätze 6a – 6c eingefügt werden:

“(6a) The proposals for the lists referred to in paragraphs 4 and 5 and for the template and methodology referred to in paragraph 6 shall be submitted to the Commission within [OP date = 9 months of the entry into application of this Regulation]. The Commission after due consideration reviews them, as

necessary, and is empowered to adopt them by way of an implementing act in accordance with the examination procedure set out in Article 93(2).

(6b) The lists and the template and methodology referred to in paragraph 6a shall be reviewed at least every three years and updated where necessary. The Board shall submit its assessment and possible proposals for updates to the Commission in due time. The Commission after due consideration of the proposals reviews them and is empowered to adopt any updates following the procedure in paragraph 6a.

(6c) Lists of the kind of processing operations which are subject to the requirement for a data protection impact assessment and of the kind of processing operations for which no data protection impact assessment is required established and made public by supervisory authorities remain valid until the Commission adopts the implementing act referred to in paragraph 6a.”

Grundsätzlich begrüßt EWE die Ergänzungen. Es muss jedoch, wie oben bereits beschrieben, sichergestellt werden, dass **weitere Kriterienkataloge nicht mehr gelten beziehungsweise in der neuen Liste aufgehen (z.B. Artikel 29-Gruppe, nationaler Katalog der Datenschutzkonferenz)**.

EWE-Formulierungsvorschlag Artikel 35 Absatz 6c DSGVO-neu:

(6c) Lists of the kind of processing operations which are subject to the requirement for a data protection impact assessment and of the kind of processing operations for which no data protection impact assessment is required established and made public by supervisory authorities remain valid only until the Commission adopts the implementing act referred to in paragraph 6a.”

9. Artikel 41a DSGVO-neu

Der Artikel 41a soll in der DSGVO hinzugefügt werden:

“(1) The Commission may adopt implementing acts to specify means and criteria to determine whether data resulting from pseudonymisation no longer constitutes personal data for certain entities.

(2) For the purpose of paragraph 1 the Commission shall:

(a) assess the state of the art of available techniques;

(b) develop criteria and or categories for controllers and recipients to assess the risk of re-identification in relation to typical recipients of data.

(3) The implementation of the means and criteria outlined in an implementing act may be used as an element to demonstrate that data cannot lead to reidentification of the data subjects.

(4) The Commission shall closely involve the EDPB in the preparations of the implementing acts. The EPDB shall issue an opinion on the draft implementing acts within a deadline of 8 weeks as of the receipt of the draft from the Commission.

(5) The Implementing Acts shall be adopted in accordance with the examination procedure referred to in Article 93(3).”

Vor dem Hintergrund der fortschreitenden Digitalisierung wäre ein starres Vorgehen über einmalige Durchführungsrechtsakte nicht zielführend. EWE schlägt vor, dass ein Verfahren gewählt wird, dass eine **Überprüfung und Anpassung der Mittel und Kriterien regelmäßig (jährlich) nach dem Stand der Technik** ermöglicht.

10. Artikel 88a DSGVO-neu

Nach Artikel 88 soll ein neuer Artikel 88a eingefügt werden:

“Processing of personal data in the terminal equipment of natural persons

(1) Storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person is only allowed when that person has given his or her consent, in accordance with this Regulation.

(2) Paragraph 1 does not preclude storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person, based on Union or Member State law within the meaning of, and subject to the conditions of Article 6, to safeguard the objectives referred to in Article 23(1).

(3) Storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person without consent, and subsequent processing, shall be lawful to the extent it is necessary for any of the following:

(a) carrying out the transmission of an electronic communication over an electronic communications network;

(b) providing a service explicitly requested by the data subject;

(c) creating aggregated information about the usage of an online service to measure the audience of such a service, where it is carried out by the controller of that online service solely for its own use;

(d) maintaining or restoring the security of a service provided by the controller and requested by the data subject or the terminal equipment used for the provision of such service.

(4) Where storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person is based on consent, the following shall apply:

(a) the data subject shall be able to refuse requests for consent in an easy and intelligible manner with a single-click button or equivalent means;

(b) if the data subject gives consent, the controller shall not make a new request for consent for the same purpose for the period during which the controller can lawfully rely on the consent of the data subject;

(c) if the data subject declines a request for consent, the controller shall not make a new request for consent for the same purpose for a period of at least six months.

This paragraph also applies to the subsequent processing of personal data based on consent.

(5) This Article shall apply from [OP: please insert the date = 6 months following the date of entry into force of this Regulation]"

EWE begrüßt die Ausnahmeregelungen des 88a Absatz 3 DSGVO-neu. Jedoch kann dieser Artikel innerhalb der DSGVO nur den Umgang mit personenbezogenen Daten regeln. Endgerätezugriffe, bei denen keine personenbezogenen Daten betroffen sind, sind nach unserem Verständnis demnach nicht im originären Anwendungsbereich der DSGVO, insbesondere unter dem neuen Verständnis des Begriffes "personenbezogene Daten" gemäß Artikel 4 Absatz 1 DSGVO-neu, erfasst. Als Folge würde der **Endgerätezugriff ohne personenbezogene Daten in den definierten Ausnahmetatbeständen gemäß Artikel 88a Absatz 3 DSGVO-neu weiterhin einwilligungspflichtig bleiben**. Aus diesem Grund muss vor dem Hintergrund des Aufgehens der ePrivacy-Richtlinie (2002/58) in der DSGVO hier eine Nachbesserung erfolgen.

11. Artikel 88b DSGVO-neu

Nach Artikel 88a soll ein neuer Artikel 88b eingefügt werden:

"Automated and machine-readable indications of data subject's choices with respect to processing of personal data in the terminal equipment of natural persons

(1) Controllers shall ensure that their online interfaces allow data subjects to:

(a) Give consent through automated and machine-readable means, provided that the conditions for consent laid down in this Regulation are fulfilled;

(b) decline a request for consent and exercise the right to object pursuant to Article 21(2) through automated and machine-readable means.

(2) Controllers shall respect the choices made by data subjects in accordance with paragraph 1.

(3) Paragraphs 1 and 2 shall not apply to controllers that are media service providers when providing a media service.

(4) The Commission shall, in accordance with Article 10(1) of Regulation (EU) 1025/2012, request one or more European standardisation organisations to draft standards for the interpretation of machine-readable indications of data subjects' choices.

Online interfaces of controllers which are in conformity with harmonised standards or parts thereof the references of which have been published in the Official Journal of the European Union shall be presumed to be in conformity with the requirements covered by those standards or parts thereof, set out in paragraph 1.

(5) Paragraphs 1 and 2 shall apply from [OP: please insert the date = 24 months following the date of entry into force of this Regulation].

(6) Providers of web browsers, which are not SMEs, shall provide the technical means to allow data subjects to give their consent and to refuse a request for consent and exercise the right to object pursuant to Article 21(2) through the automated and machine-readable means referred to in paragraph 1 of this Article, as applied pursuant to paragraphs 2 to 5 of this Article.

(7) Paragraph 6 shall apply from [OP: please insert the date = 48 months following the date of entry into force of this Regulation]."

Nach Auffassung von EWE trägt der Vorstoß des Artikel 88b DSGVO-neu in dieser Form weder dazu bei, eine wahrgenommene "Cookiebanner-Flut" oder auch "Consent-Fatigue" in der Bevölkerung einzudämmen, noch für eine bürokratische Entlastung der Wirtschaft zu sorgen. Im Gegenteil: Es ergeben sich **neben den zusätzlichen Aufwänden für die Wirtschaft auch neue Fragestellungen, wie zum Beispiel mit Informationen umgegangen werden soll, die nicht personenbezogen sind.** Auch hier regen wir vor dem Hintergrund des Aufgehens der ePrivacy-Richtlinie (2002/58) in der DSGVO eine Nachbesserung an.

12. Artikel 88c DSGVO-neu

Nach Artikel 88b wird Artikel 88c eingefügt:

"Processing in the context of the development and operation of AI

Where the processing of personal data is necessary for the interests of the controller in the context of the development and operation of an AI system as defined in Article 3, point (1), of Regulation (EU) 2024/1689 or an AI model, such processing may be pursued for legitimate interests within the meaning of Article 6(1)(f) of Regulation (EU) 2016/679, where appropriate, except where other Union or national laws explicitly require consent, and where such interests are overridden by the interests, or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Any such processing shall be subject to appropriate organisational, technical measures and safeguards for the rights and freedoms of the data subject, such as to ensure respect of data minimisation during the stage of selection of sources and the training and testing of AI an system or AI model, to protect against non-disclosure of residually retained data in the AI system or AI model to ensure enhanced transparency to data subjects and providing data subjects with an unconditional right to object to the processing of their personal data."

Grundsätzlich befürwortet EWE die Regelungen im Zusammenhang mit der Entwicklung und dem Betrieb von KI. Es sind jedoch einige **unbestimmte Rechtsbegriffe ("erforderlich", "kann ...**

erfolgen" "sofern dies angebracht ist") enthalten, die für den Verantwortlichen keine Rechtssicherheit herstellen. Für eine bessere Förderung von Innovation sollte der Artikel weiter konkretisiert werden.

In der Praxis ist es in der Regel nicht möglich, aus einem trainierten KI-Modell personenbezogene Daten nach dem Widerspruch wieder zu löschen bzw. die Verarbeitung zu unterbinden. Es sollte klargestellt werden, dass sich das bedingungslose Widerspruchsrecht nur auf die Entwicklung (Training) und nicht auf den Betrieb des KI-Systems/Modell bezieht.

13. Weitere Vorschläge

Des Weiteren schlagen wir folgende Anpassungen vor, die einen positiven gesamtwirtschaftlichen Effekt erzielen würde, ohne das hohe Schutzgut des Datenschutzes zu schwächen.

a. Einführung einer Herstellerhaftung

EWE begrüßt den Vorstoß der deutschen Datenschutzkonferenz (DSK) sowie des des Bundeskanzlers und der Regierungschefinnen und Regierungschefs der Länder, die Hersteller und Anbieter von Standardlösungen künftig in die Verantwortung zu nehmen. Dies würde die Rechtssicherheit beim Einsatz von Standardlösungen erhöhen und zudem Aufwände für die Verantwortlichen (Anwender) reduzieren.

b. Abschaffung des Artikel 26 DS-GVO (Joint Control)

Die Erstellung und Aktualisierung solcher Vereinbarungen ist mit erheblichem Aufwand verbunden, insbesondere im Mehr-Parteienverhältnis. Auch der Anwendungsbereich ist unklar und in der Praxis schwer handhabbar. Die Auslegungen auf EU-Ebene und Aufsichtsbehörden sind sehr weit gefasst und konturlos. In der Praxis kann das Anschließen an von Dritten festgelegten Mitteln und Zwecken zu einer gemeinsamen Verantwortlichkeit führen, auch bei extern beauftragten Dienstleistungen. Daher soll dieser Artikel bestenfalls gelöscht werden, insbesondere angesichts der ohnehin bestehenden Datenschutzpflichten jedes Beteiligten. Ein JCA bietet hier keinen Mehrwert.

EWE AG EWE ist ein Versorgungskonzern im Bereich Strom, Erdgas, Telekommunikation und Informationstechnologie. Die EWE AG ist registrierte Interessenvertreterin spwphl nach dem EU Transparency Register (Nr. 237768853046-23) sowie nach dem Lobbyregistergesetz (Registernummer R001058) und folgt dem vom Deutschen Bundestag und von der Bundesregierung beschlossenen Verhaltenskodex.

Kontakt EWE Aktiengesellschaft
Tirpitzstraße 39
D-26122 Oldenburg
ww.ewe.com

Ansprechpartner/ in
Abteilung Politische Angelegenheiten
Fabiane Buchheister
fabiane.buchheister@ewe.de

Tjark Melchert
tjark.melchert@ewe.de
+49 162 962 4720