Praxishelfer Dialogmarketing

BEST PRACTICE GUIDE

EUROPÄISCHE DATENSCHUTZ-GRUNDVERORDNUNG
AUSWIRKUNGEN AUF DAS DIALOGMARKETING

2. überarbeitete Auflage

Zulässigkeit
Transparenz
Dienstleister
Durchsetzung
Grenzüberschreitende Verarbeitung

DDV
Deutscher Dialogmarketing Verband e.V.

Herausgeber
Deutscher Dialogmarketing Verband e.V.
Hahnstraße 70
60528 Frankfurt
Tel. 069 401 276 500
Fax 069 401 276 599
eMail: info@ddv.de
www.ddv.de

Gestaltung
rahlwespietz, Frankfurt/Main

Stand
September 2017

INHALT

VORBEMERKUNG

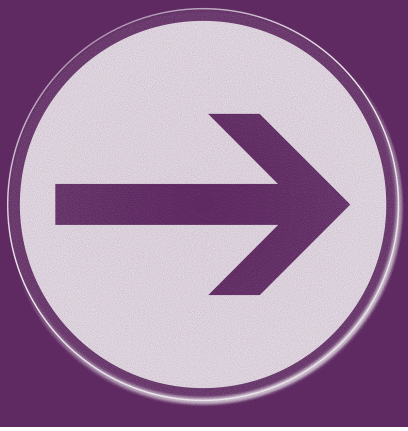
Am 25. Mai 2018 löst die Europäische Datenschutz-Grundverordnung (2016/679/EU) nationale Datenschutzvorschriften in der Europäischen Union weitgehend ab. Die wesentlichen datenschutzrechtlichen Rahmenbedingungen für das Dialogmarketing werden auf diese Weise europaweit harmonisiert. Nur in wenigen Fragen können die Mitgliedstaaten nationale Sonderregelungen treffen. In Deutschland wurde hierzu das Datenschutz-Anpassungs- und Umsetzungsgesetz beschlossen (Bundesgesetzblatt 2017 Teil I, Seite 2097). Der Best Practice Guide beschreibt, wie die neuen Rahmenbedingungen der Datenschutz-Grundverordnung in der Praxis des Dialogmarketings umgesetzt werden können.

Eine der zentralen Fragestellungen im Dialogmarketing ist, ob personenbezogene Daten mit oder ohne Einwilligung der betroffenen Personen zu Werbezwecken verarbeitet werden dürfen. Der europäische Gesetzgeber hat sich für die Beibehaltung des Opt-Out-Prinzips entschieden, bei dem die betroffenen Personen jederzeit und ohne besondere Begründung der Verwendung ihrer Daten für Zwecke des Dialogmarketings widersprechen können. Auf diese Weise bringt die Verordnung den Selbstbestimmungsgrundsatz mit den ökonomischen Zielen der Europäischen Union in Einklang.

Das Opt-Out-Prinzip gilt jedoch nicht ohne Einschränkungen. Die schutzwürdigen Interessen der betroffenen Personen sind angemessen zu berücksichtigen. Ausreichende Transparenz hinsichtlich der Verwendung der Daten ist herzustellen. Für elektronische Werbung gelten Beschränkungen, die sich aus den nationalen Gesetzen zur Umsetzung der Datenschutzrichtlinie für elektronische Kommunikation (ePrivacy Richtlinie - 2002/58/EG) ergeben. Diese Beschränkungen sind - soweit die ePrivacy Richtlinie Anwendung findet - weiterhin einzuhalten.

Die Europäische Kommission hat eine neue ePrivacy Verordnung vorgeschlagen (COM (2017) 10 final). Dieser Vorschlag erweitert die Einwilligungsvorbehalte im Bereich der elektronischen Werbung. Die Europäische Kommission drängt darauf, dass der Vorschlag gleichzeitig mit der Grundverordnung am 25. Mai 2018 wirksam werden soll. Realistisch ist ein Abschluss des Gesetzgebungsverfahrens bis zu diesem Zeitpunkt jedoch nicht mehr.

Im Vergleich zu den geltenden nationalen Datenschutzvorschriften bringt die Datenschutz-Grundverordnung zahlreiche Neuerungen für das Dialogmarketing. Teilweise werden sehr spezifische nationale Sonderregelungen durch generellere Regelungen



abgelöst. Die Verwendung von Daten zu Marketingzwecken unterliegt einer allgemeinen Interessenabwägung. Transparenzanforderungen und die Rechte der Betroffenen werden erweitert. Die Eingriffs- und Sanktionsrechte der Datenschutzaufsichtsbehörden werden wesentlich verschärft.

Die Grundkonzeption der Verordnung räumt dem Dialogmarketing einen angemessenen Spielraum ein. Die Herausforderungen bei der Umsetzung liegen in der Auslegung der Detailregelungen, denn die Artikel der Verordnung und ihre Erwägungsgründe konnten in den langwierigen Verhandlungen in Brüssel und Straßburg leider nicht durchgängig zu einem konsistenten Ergebnis geführt werden. Der Best Practice Guide schlägt – unter Berücksichtigung der Zielsetzungen der Verordnung – praxisgerechte Lösungen für die Anwendung dieser Regelungen vor.

Bei der Auslegung der allgemein gehaltenen Regelungen der Verordnung lassen sich unterschiedliche Ansichten nicht vermeiden. Jeder Mitgliedstaat wird insbesondere dazu tendieren, die Verordnung möglichst nahe an seinen bisherigen nationalen Sonderregelungen umzusetzen und auszulegen. Dies widerspricht aber dem europäischen Harmonisierungsziel der Verordnung. Der Best Practice Guide orientiert sich deshalb bewusst nicht an den Besonderheiten des früheren nationalen Rechts.

Das Wirksamwerden der Verordnung sollte nicht tatenlos abgewartet werden. Schon jetzt besteht aktueller Handlungsbedarf für Unternehmen. Beispielsweise sollten die Transparenzanforderungen möglichst frühzeitig umgesetzt werden. Ebenso sind Verträge zur Auftragsverarbeitung an die Anforderungen der Verordnung anzupassen, wenn sie über den Sommer 2018 hinaus wirksam sein sollen. Zuletzt müssen sich Unternehmen organisatorisch auf die Verordnung vorbereiten, damit die erforderlichen Umstellungen interner Prozesse bis 25. Mai 2018 durchgeführt sind. Außerdem sollten Einwilligungstexte daraufhin überprüft werden, ob sie den Anforderungen der Verordnung entsprechen. Der Best Practice Guide will Unternehmen bei den Umsetzungsmaßnahmen unterstützen.

Der Best Practice Guide wurde vom Arbeitskreis Datenschutz des DDV erarbeitet. Rechtsanwalt Prof. Dr. Ulrich Wuermeling, Latham & Watkins LLP, Frankfurt, ist zur fachlichen Unterstützung in den Arbeitskreis Datenschutz des DDV seit Jahren eingebunden und hat an der Erstellung des Best Practice Guides maßgeblich mitgewirkt. Ihm und dem Arbeitskreis Datenschutz sei an dieser Stelle ausdrücklich gedankt.

1. PRAXIS DES DIALOGMARKETINGS

1.1 VERFÜGBARE DATENQUELLEN

Dialogmarketing setzt auf die interessengerechte Ansprache von potentiellen Neukunden und Bestandskunden. Hierzu bedarf es geeigneter Kommunikationskanäle zu den Adressaten und aussagekräftiger Selektionskriterien. Die Kommunikationskanäle im Dialogmarketing reichen von postalischer Werbung über die Ansprache per elektronischer Nachricht bis hin zum Online Behavioral Advertising. Die Verwendung von Selektionskriterien hat zum Ziel, die Ansprache möglichst auf potentiell interessierte Personen zu beschränken. Die Selektion erspart damit nicht nur dem Unternehmen Kosten, sondern liegt auch im Interesse der Adressaten.

Um potentielle Adressaten, verfügbare Kommunikationskanäle und aussagekräftige Selektionskriterien zu ermitteln, stehen Unternehmen unterschiedliche Datenquellen zur Verfügung. Die Daten stammen zu einem wesentlichen Teil aus Interessenten- und Bestandskundenbeziehungen oder aus öffentlich zugänglichen Quellen. Sie werden direkt vom Adressaten erhoben oder von anderen Marktteilnehmern oder Datendienstleistern zur Verfügung gestellt. Die Selektionskriterien sollen wirtschaftlich die Wahrscheinlichkeit erfolgreichen Dialogmarketings erhöhen.

Zur Bewertung der Aussagekraft von Selektionskriterien gehört deren statistische Analyse. Auf diese Weise können detaillierte personenbezogene Kriterien in generische Gruppen zusammengefasst werden. Die Selektionskriterien enthalten damit weniger konkrete personenbezogene Daten. Sie können teilweise pseudonymisiert oder sogar anonymisiert werden, bevor sie zu Selektionszwecken zur Verfügung gestellt werden. Auf diese Weise wird den schutzwürdigen Interessen der betroffenen Personen besonders entsprochen.

1.2 VORBEREITUNG EINES INDIVIDUELLEN DIALOGS

Ein individueller Dialog erfordert im ersten Schritt eine breite Basis potentieller Adressaten mit Angaben zu den verfügbaren Kommunikationskanälen. Die Basis wird vom werbetreibenden Unternehmen entweder selbst erhoben oder durch andere Markteilnehmer oder Datendienstleister zur Verfügung gestellt.

Im zweiten Schritt erfolgt die Auswahl der Adressaten, die potentiell Interesse an den beworbenen Produkten und Dienstleistungen des Werbetreibenden haben könnten. Die hierzu erforderliche Selektion erfolgt auf der Grundlage von personenbezogenen, pseudonymisierten oder anonymisierten Daten. Der Werbetreibende kann die Selektion teilweise auf Grund seiner selbst erhobenen Daten durchführen. Besonders bei der Ansprache potentieller Neukunden wird der eigene Datenbestand jedoch nicht ausreichen. Dann kann der Werbetreibende auf andere Marktteilnehmer oder Datendienstleister zurückgreifen. Hierfür lassen sich teilweise Verfahren verwenden, bei denen der Werbetreibende die der Selektion zugrundeliegenden Einzeldaten nicht verarbeitet (wie im Lettershop-Verfahren oder beim Online Behavioral Advertising).

Ziel der Selektion ist die Auswahl einer Adressatengruppe, die als gemeinsames Merkmal das potentielle Interesse an bestimmten Produkten oder Dienstleistungen hat. Nach der Selektion wird die ausgewählte Zielgruppe nochmals überprüft. Die Adressen werden zur Verbesserung der Datenqualität berichtigt und aktualisiert. Die Adressaten werden gegen Werbewiderspruchslisten abgeglichen. Soweit die Kommunikationskanäle einer Einwilligung bedürfen, wird der Einwilligungsstatus überprüft. Das Ergebnis ist eine Liste mit potentiell interessierten Adressaten mit Angaben zur Verwendbarkeit der entsprechenden Kommunikationskanäle.

1.3 ANSPRACHE POTENTIELLER INTERESSENTEN

Die Ansprache der potentiellen Interessenten erfolgt über postalische oder elektronische Kanäle. Wegen der bestehenden rechtlichen Hürden bei der Ansprache per E-Mail, Telefon, Telefax oder SMS wird häufig die postalische Ansprache gewählt. Sowohl der Anbieter der beworbenen Produkte oder Dienstleistungen als auch andere Marktteilnehmer können die Absender der Kommunikation sein. Online Behavioral Advertising ist ein Sonderfall, denn es erfolgt keine individuelle Ansprache bestimmter Adressaten. Die auf einer Internetseite eingeblendete Werbung wird jedoch ebenfalls nach potentiellen Zielgruppen priorisiert.

2. DIALOGMARKETING ZULÄSSIG GESTALTEN

2.1 DREI ALTERNATIVEN FÜR RECHTMÄSSIGES DIALOGMARKETING

Jede Verarbeitung personenbezogener Daten bedarf unter der Datenschutz-Grundverordnung einer konkreten Erlaubnis. Als Rechtsgrundlagen für die Verarbeitung von personenbezogenen Daten zu Zwecken des Dialogmarketings kommen drei Alternativen in Betracht: Interessenabwägung, Einwilligung und Zweckänderung. Die Verarbeitung von anonymisierten Daten unterliegt nicht dem Datenschutzrecht und bedarf deshalb keiner Rechtsgrundlage. Es ist jedoch nicht einfach zu beurteilen, wann Daten als anonym und wann als personenbezogen gelten.

§ Personenbezogene, pseudonyme oder anonyme Daten?

In der Regel werden für das Dialogmarketing personenbezogene Daten verwendet. Hierzu gehören pseudonymisierte Daten. Eine Pseudonymisierung liegt vor, wenn die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können. Diese zusätzlichen Informationen sind gesondert aufzubewahren. Außerdem ist durch technische und organisatorische Maßnahmen zu gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden (Artikel 4 (5)).

Darüber hinaus erfolgen Selektionen auf der Grundlage von anonymisierten Daten. Da die Verordnung auf anonyme Daten keine Anwendung findet, ist die Abgrenzung zwischen personenbezogenen und anonymen Daten von großer praktischer Bedeutung. Für die Verarbeitung von anonymen Daten bedarf es keiner Rechtsgrundlage.

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (Artikel 4 (1)). Diese Definition stammt inhaltlich aus der Europäischen Datenschutzrichtlinie von 1995. Die Verordnung enthält zusätzlich klarstellende Beispiele dafür, wann eine Identifizierbarkeit von Personen gegeben sein soll. Als mögliche Identifizierungsmerkmale werden Kennnummern, Standortdaten oder Online-Kennungen von Personen genannt.

→

Daten sind personenbeziehbar, wenn dem verarbeitenden Unternehmen Mittel verfügbar sind, die nach allgemeinem Ermessen aller Voraussicht nach zur Bestimmung der betroffenen Person genutzt werden (Erwägungsgrund 26). Eine rein theoretische Identifizierbarkeit führt nicht dazu, dass Daten als personenbezogen gelten. Wenn eine Nutzung der Mittel zur Identifizierung aller Voraussicht nach nicht erfolgt, gelten die Daten als anonym. Unbeachtlich ist, ob ein Dritter die theoretische Möglichkeit zur Bestimmung der Person hat. Diese Möglichkeit ist nur zu berücksichtigen, wenn die Daten des Dritten aller Voraussicht nach mit denen des verarbeitenden Unternehmens zusammengeführt werden.

Beispiele für die Abgrenzung zwischen personenbezogenen und anonymen Daten sind IP-Adressen und Cookies. Die Verordnung stellt fest, dass betroffene Personen „unter Umständen“ durch solche Online-Kennungen zugeordnet werden können (Erwägungsgrund 30). Es bleibt offen, unter welchen Umständen dies der Fall sein soll.

Der Europäische Gerichtshof hat festgestellt, dass IP-Adressen in der Hand des Anbieters eines Internetzugangs personenbezogene Daten darstellen (C70/10). Wenn Anbieter von Internet-Diensten personenbezogene Daten zur Verfolgung von Hackerangriffen erheben, stellen diese ebenfalls personenbezogene Daten dar (C-582/14). Der Europäische Gerichtshof sieht hier im Falle eines Angriffs die rechtliche Möglichkeit der Identifizierung durch Sicherheitsbehörden als gegeben.

Im Bereich des Dialogmarketings besteht jedoch in der Regel keine rechtlich zulässige Möglichkeit, anonyme Daten mit Hilfe von Daten Dritter bestimmten Personen wieder zuzuordnen. Dies gilt beispielsweise für so genannte mikrogeographische Daten, die sich auf geographische Segmente und nicht auf konkrete Personen beziehen. Die einzelnen Segmente werden so gewählt, dass die Angaben nicht eindeutig einer bestimmten Person innerhalb des Segmentes zugeordnet werden können. Je spezifischer die Einzelangaben pro Segment sind, desto größer müssen die Segmente gebildet werden, um eine Identifizierbarkeit auszuschließen. Häufig wird hierzu eine Grenze von 5 bis 10 Haushalten verwendet.

§ Profiling für automatisierte Einzelentscheidungen

Die Verordnung stellt besondere Anforderungen an automatisierte Einzelentscheidungen (Artikel 22). Dies gilt insbesondere dann, wenn die automatisierten Entscheidungen auf so genanntem Profiling beruhen. Der Begriff Profiling ist weit definiert (Artikel 4 (4)), so dass Selektionen für Zwecke des Dialogmarketings darunter fallen können. Besondere Anforderungen knüpft die Verordnung an automatisierte Einzelentscheidungen jedoch nur, wenn sie eine rechtliche Wirkung entfalten oder die betroffene Person in ähnlicher Weise erheblich beeinträchtigen.

Selektionen für die Zwecke des Dialogmarketings werden durchgeführt, um den Kreis der angesprochenen Adressaten auf Personen reduzieren zu können, die an den beworbenen Produkten und Dienstleistungen potentiell Interesse haben könnten. Die Entscheidung, ob ein potentieller Adressat Werbung erhält oder nicht, hat für die betroffenen Personen keine rechtliche Wirkung und beeinträchtigt sie nicht in ähnlicher Weise. Artikel 22 ist deshalb auf den Bereich des Dialogmarketings in der Regel nicht anwendbar.

→

Die Zulässigkeit der Verarbeitung von personenbezogenen Daten zu Selektionszwecken richtet sich nach den allgemeinen Rechtsgrundlagen. Im Rahmen der so genannten Interessenabwägung ist zu beurteilen, ob die Selektion selbst überwiegende schutzwürdige Interessen der betroffenen Personen berührt. Dabei ist die Sensitivität der verwendeten Daten zu berücksichtigen. Eine formale Datenschutz-Folgenabschätzung nach Artikel 35 (3) (c) wird jedoch in der Regel nicht erforderlich sein, denn es fehlt an den potentiell negativen Folgen der Selektionsentscheidung.

ALTERNATIVE 1: INTERESSENABWÄGUNG

Die Verordnung erlaubt die Verarbeitung von personenbezogenen Daten, wenn das Interesse der betroffenen Person am Schutz der Daten das Interesse des Unternehmens an der Verarbeitung der Daten nicht überwiegt (Artikel 6 (1) (f)). Unter „Verarbeitung" versteht die Verordnung insbesondere die Erhebung, Speicherung, Verwendung oder Übermittlung von personenbezogenen Daten (Artikel 4 (2)). Damit findet die Rechtsgrundlage auf die Verarbeitung von personenbezogenen Daten zu Zwecken des Dialogmarketings von der Erhebung über die Selektion bis zur konkreten Ansprache Anwendung.

Die Verordnung stellt ausdrücklich klar, dass die Durchführung von Dialogmarketing als berechtigtes Interesse betrachtet werden kann (Erwägungsgrund 47). Dies entspricht dem bisherigen Verständnis unter der Europäischen Datenschutzrichtlinie. Zum Ausgleich sieht die Verordnung für Dialogmarketing ein bedingungsloses Widerspruchsrecht vor, mit dem der Adressat künftige Ansprachen ausschließen kann (siehe Ziffer 2.2 des Best Practice Guides). Das Widerspruchsrecht gilt auch für Profiling zu Zwecken des Dialogmarketings.

Ihre Grenze findet die Interessenabwägung dann, wenn die betroffene Person der Verarbeitung der Daten zu Zwecken des Dialogmarketings widerspricht (siehe Ziffer 2.2 des Best Practice Guides), besondere Arten von Daten verarbeitet werden (wie beispielsweise Gesundheitsdaten) oder ein überwiegendes Interesse der betroffenen Person am Schutz der Daten besteht. Die Schutzwürdigkeit von Kindern unter 16 Jahren ist besonders zu berücksichtigen und auch bei Jugendlichen zwischen 16 und 18 Jahren sind angemessene Anforderungen zu stellen.

Ein überwiegendes Interesse der betroffenen Person ist beispielsweise anzunehmen, wenn besonders umfangreiche oder sensible Datensätze zu Zwecken des Dialogmarketings an Dritte übermittelt werden. In der Praxis des Dialogmarketings kommt es hierzu jedoch in der Regel nicht, da die Selektionskriterien vor ihrer Übermittlung in generischen Gruppen aggregiert werden. Außerdem fließt in die Abwägung ein, ob die Daten gegen besondere Risiken geschützt sind. Ein solcher Schutz kann beispielsweise durch die Pseudonymisierung der Daten erreicht werden.

Im Rahmen der Abwägung der Interessen ist zu berücksichtigen, ob der Adressat die Verwendung seiner Daten zu Zwecken des Dialogmarketings erwarten konnte (Erwägungsgrund 47). Bei kommerziellen Kontakten mit den betroffenen Personen werden diese in der Regel mit einer Verwendung der Daten im Rahmen des rechtlich Zulässigen rechnen müssen. Dabei geht die allgemeine Erwartungshaltung hinsichtlich des Umgangs mit den Daten häufig weit über das hinaus, was tatsächlich in der Praxis des Dialogmarketings passiert. In den Datenschutzinformationen der Unternehmen sollten die betroffenen Personen dennoch konkret informiert werden, denn dann wissen sie sicher, was sie zu erwarten haben.

Die Interessenabwägungsklausel verweist ausdrücklich darauf, dass auch Interessen von Dritten in der Abwägung Berücksichtigung finden können. Dies ist in Konstellationen relevant, in denen ein Werbetreibender die Daten nicht selbst verarbeitet. Andere Marktteilnehmer oder Datendienstleister können sich im Rahmen der Abwägung auf das Interesse des Werbetreibenden an der Durchführung der Werbung berufen. Dies gilt außerdem im Falle der Übermittlung von Daten an den Werbetreibenden.

Um die Ansprache oder Selektion von Adressaten zu erleichtern, können Daten anderer Marktteilnehmer, aus öffentlich zugänglichen Quellen oder von Datendienstleistern hinzugespeichert werden, solange dabei die Schutzinteressen der betroffenen Personen ausreichend Berücksichtigung finden.

Die Verwendung von besonderen Arten von Daten (Artikel 9) oder von Daten über strafrechtliche Verurteilung oder Straftaten (Artikel 10) ist für Zwecke des Dialogmarketings grundsätzlich ausgeschlossen. Hier bedarf es der Einwilligung der betroffenen Person. Besondere Arten von Daten sind solche, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer Person oder Daten über Gesundheit oder Sexualleben und sexuelle Ausrichtung. Im deutschen Umsetzungsgesetz werden für solche besonderen Arten von Daten umfangreiche Ausnahmen für die Verarbeitung zu statistischen Zwecken eingeführt. Dies erleichtert insbesondere die Auswahl von Daten für anonymisierte Selektionsdatenbanken, beispielsweise im Gesundheitssektor.

Die Regelung zu automatisierten Einzelentscheidungen in Artikel 22 schränkt die Verwendung der Interessenabwägungsklausel für das Dialogmarketing nicht ein. Die Entscheidung, eine Person im Rahmen des Dialogmarketings anzusprechen, hat weder rechtliche Wirkungen für den Adressaten noch beeinträchtigt ihn diese in ähnlich erheblicher Weise.

Die Anwendung der Interessenabwägungsklausel bedarf der Abwägung der schutzwürdigen Interessen der betroffenen Person mit denen des datenverarbeitenden oder werbetreibenden Unternehmens. Die Verordnung soll insbesondere mit dem Recht auf unternehmerische Freiheit in Einklang stehen (Erwägungsgrund 4). Es können aber auch andere Grundwerte in die Abwägung einfließen. Beispielsweise dient Dialogmarketing zum Zwecke der Spendenwerbung für gemeinnützige Organisationen einem öffentlich anerkannten Zweck.

Wie die Interessen im Rahmen der Abwägung zu gewichten sind, lässt sich an folgenden Beispielen veranschaulichen:

BEISPIEL1: INTERESSENTEN UND BESTANDSKUNDEN

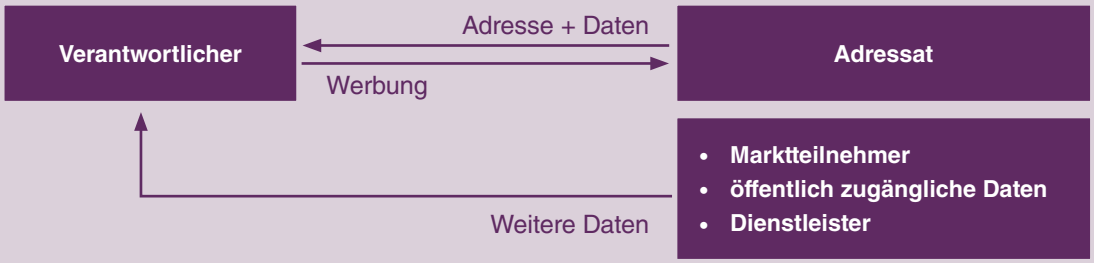
Unternehmen erhalten personenbezogene Daten von Interessenten, die sich direkt an das Unternehmen wenden, oder von Personen, die vom Unternehmen Produkte erwerben oder Dienstleistungen in Anspruch nehmen. Die Datensätze enthalten Angaben darüber, wie mit den Personen Kontakt aufgenommen werden kann und an welchen Produkten oder Dienstleistungen Interesse gezeigt wurde. Außerdem können weitere Selektionskriterien, die gegebenenfalls von anderen Marktteilnehmern, aus öffentlich zugänglichen Quellen oder von Datendienstleistern stammen, hinzugespeichert sein.

Ein Unternehmen hat ein gewichtiges berechtigtes Interesse daran, personenbezogene Daten zu Zwecken des Dialogmarketings zu verarbeiten, um die Geschäftsbeziehung zu Interessenten und Bestandskunden zu pflegen.

→

Die Schutzinteressen der betroffenen Person sind in der Regel gering. Der Adressat hat selbst kommerziellen Kontakt mit dem Unternehmen aufgenommen. Erwägungsgrund 47 der Datenschutz-Grundverordnung weist darauf hin, dass eine solche Beziehung zum Adressaten bei der Interessenabwägung beachtlich ist. Eine Werbeansprache wird er nach allgemeiner Lebenserfahrung oder auf Grund einer entsprechenden Datenschutzinformation erwarten, solange er der Verwendung seiner Daten für diese Zwecke nicht widersprochen hat. Die Verwendung von Selektionskriterien führt im positiven Sinne dazu, dass er interessengerecht angesprochen wird.

Im Falle der Übermittlung von Daten zu Zwecken des Dialogmarketings sind die Schutzinteressen der Adressaten unter Berücksichtigung der Tatsache zu bewerten, dass es bisher an einem kommerziellen Kontakt zum werbenden Unternehmen fehlt. Dies ist besonders bei Kontakten mit privaten Konsumenten zu beachten. Höhere Schutzinteressen dieser Art lassen sich beispielsweise durch die Aggregation oder Pseudonymisierung von Selektionskriterien kompensieren, so dass in der Regel auch in diesen Fällen die Datenverarbeitung durch die Interessenabwägungsklausel gerechtfertigt ist.



BEISPIEL 2: ÖFFENTLICH ZUGÄNGLICHE DATEN

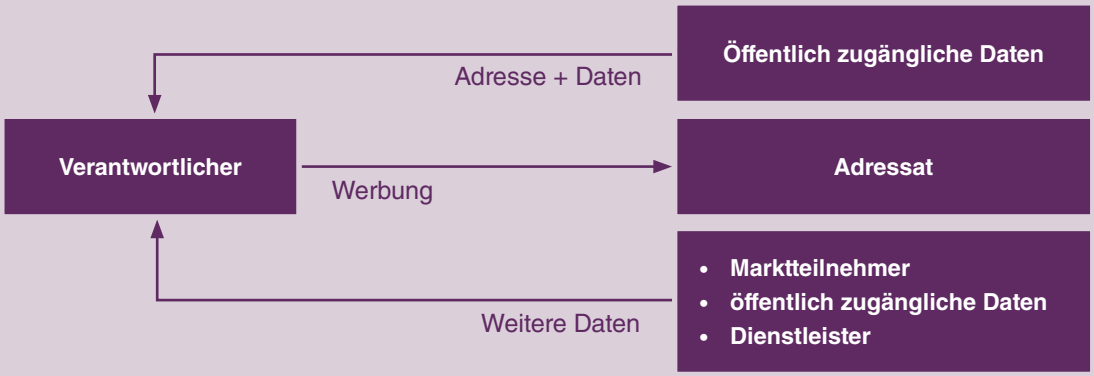
Werbetreibende und deren Datendienstleister erheben Daten aus öffentlich zugänglichen Quellen, um diese zu Zwecken des Dialogmarketings zu verwenden. Hieran besteht ein berechtigtes Interesse. Die Daten dienen entweder der Neukundenwerbung oder der Hinzuspeicherung von Selektionskriterien zu bestehenden Kontakten. Entweder werden die Daten vom Werbetreibenden selbst aus öffentlichen Quellen erhoben oder Datendienstleister stellen diese bereit.

Das Interesse von Unternehmen an der Neukundengewinnung hat hohes Gewicht, denn mit einer reinen Bestandskundenpflege können sie langfristig nicht erfolgreich sein. Aber auch für die Bestandskundenpflege sind die hinzugespeicherten Daten von großer Bedeutung, weil sie die Bildung aussagekräftiger Selektionskriterien ermöglichen.

Das Interesse der betroffenen Person am Schutz der Daten ist im Regelfall eher gering, denn die Daten sind bereits öffentlich und für jedermann weltweit zugänglich. Mitveröffentlichte Widersprüche (beispielsweise in Impressumsdaten im Internet) sind zu beachten. Urheberrechtliche Beschränkungen sind zu berücksichtigen, wenn Daten aus rechtlich geschützten Quellen entnommen werden.

→

Wenn die betroffene Person die Daten selbst veröffentlicht hat, wiegen ihre schutzwürdigen Interessen geringer als in einer Konstellation, in der Dritte die Daten veröffentlicht haben. Bei Sozialen Netzwerken des privaten Umfeldes sollte zwischen Daten unterschieden werden, die für jedermann oder nur dem Freundeskreis zugänglich sind. Die Verwendung von umfangreichen Profilen aus Sozialen Netzwerken zu Werbezwecken wird teilweise kritisch gesehen.

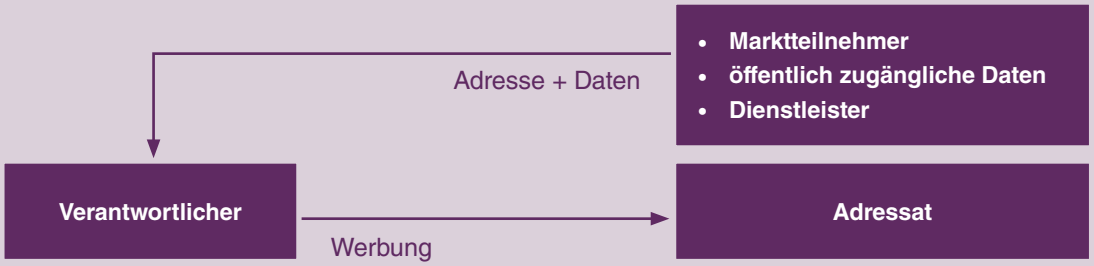


BEISPIEL 3: B2B

Die Interessenabwägungsklausel unterscheidet nicht ausdrücklich danach, ob potentielle B2B- oder B2C-Kunden angesprochen werden. Die Interessen der Adressaten am Schutz ihrer Daten sind jedoch unterschiedlich hoch zu bewerten. Bei der Abwägung ergibt sich deshalb ein weiterer Spielraum für die Verarbeitung von personenbezogenen Daten zu Zwecken des Dialogmarketings im B2B-Bereich. Geschäftliche Adressen und dazugehörige Selektionskriterien können direkt bei den Adressaten erhoben werden oder von anderen Marktteilnehmern, aus öffentlich zugänglichen Quellen oder von Datendienstleistern stammen.

Im Bereich der B2B-Werbung handelt es sich bei den Selektionskriterien in der Regel nicht um personenbezogene Daten über den Ansprechpartner im Unternehmen, sondern um Informationen zum Unternehmen selbst (wie Angaben zu Branche, Tätigkeitsbereichen, Umsatz oder dem Bedarf an Zulieferungsprodukten). Diese Daten fallen bei juristischen Personen nicht unter das Datenschutzrecht (Erwägungsgrund 14). Sie werden nur im Rahmen der ePrivacy Richtlinie geschützt.

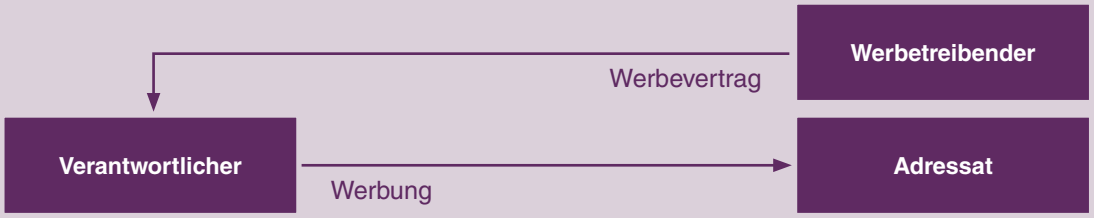
Informationen zur geschäftlichen Tätigkeit des konkreten Ansprechpartners sind in ihrer Schutzwürdigkeit geringer einzustufen als Informationen aus dem rein persönlichen Umfeld. Deshalb sollten Daten aus dem persönlichen Umfeld möglichst nicht zu Zwecken des Dialogmarketings im B2B-Bereich verwendet werden.



BEISPIEL 4: EMPFEHLUNGEN

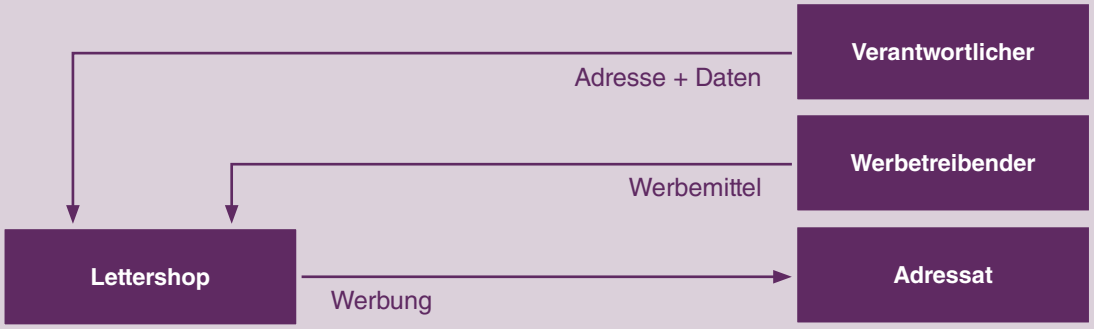
Unternehmen unterstützen sich gegenseitig durch die Empfehlung ihrer jeweiligen Produkte und Dienstleistungen. Im Rahmen der Interessenabwägung können die Interessen von Dritten (hier dem empfohlenen Unternehmen) in die Abwägung einbezogen werden.

Entweder versendet das empfehlende Unternehmen die Werbung oder es setzt Dienstleister als Auftragsverarbeiter hierfür ein. Die Daten der Adressaten müssen deshalb nicht an das empfohlene Unternehmen übermittelt werden. Damit werden die Interessen der Adressaten bezüglich ihrer Daten auf besondere Weise geschützt.



BEISPIEL 5: LETTERSHOP-VERFAHREN

In Anlehnung an die Empfehlungswerbung wird für Dialogmarketing auch das so genannte Lettershop-Verfahren verwendet. Wie bei der Empfehlungswerbung wird dabei die Werbung entweder direkt von dem Unternehmen mit der bestehenden Kundenbeziehung (so genannte Adresseigner) oder durch einen Dienstleister durchgeführt. Der entscheidende Unterschied zur Empfehlungswerbung besteht darin, dass die Ansprache unter dem Absender bzw. auf dem Briefkopf des empfohlenen Unternehmens erfolgt. Wie bei der Empfehlungswerbung veranlasst das empfehlende Unternehmen die Selektionen und Ansprache, ohne hierfür die Daten der Adressaten an das empfohlene Unternehmen übermitteln zu müssen. Für die Zwecke der Interessenabwägung sind deshalb dieselben Kriterien wie bei der Empfehlungswerbung zu beachten.



BEISPIEL 6: ONLINE BEHAVIORAL ADVERTISING

Ziel des Online Behavioral Advertising ist es, eine interessengerechte Einblendung von Werbung im Rahmen der Nutzung von Internetdiensten zu ermöglichen. Hierzu werden entweder pseudonymisierte oder anonymisierte Nutzungsdaten als Selektionskriterien verwendet.

Sowohl die Betreiber von Internetdiensten als auch die Werbetreibenden haben ein berechtigtes Interesse an der Einblendung interessengerechter Werbung. Die Einnahmen aus dieser Art Werbung sind eine wichtige Finanzierungsquelle für Internetdienste. Den Werbetreibenden wird auf diese Weise ein werthaltiger Kommunikationskanal eröffnet. Dies sind gewichtige Interessen, die in die Abwägung eingehen.

Das Schutzinteresse des Nutzers kann hoch sein, wenn der Umfang und die Sensibilität der verwendeten personenbezogenen Daten nicht durch andere Maßnahmen hinreichend kompensiert werden. Dabei ist zu berücksichtigen, ob die Einbindung von Dienstleistern sicherstellt, dass die konkreten Selektionskriterien nicht direkt an die Werbetreibenden übermittelt werden. Außerdem können personenbezogene Daten durch Pseudonymisierung einen zusätzlichen Schutz erhalten. Den Schutzinteressen der Nutzer kann weiterhin durch Transparenz und Präferenzmanagement entsprochen werden. Deshalb überwiegen die Interessen der Unternehmen in der Praxis regelmäßig die der betroffenen Personen.

Die Europäische Kommission schlägt in der ePrivacy Verordnung umfangreichere Einwilligungsanforderungen für Online Behavioral Advertising vor. Es bleibt abzuwarten, in welcher Form sich diese Vorschläge im europäischen Gesetzgebungsverfahren durchsetzen.

ALTERNATIVE 2: EINWILLIGUNG

Die Verarbeitung von Daten zu Zwecken des Dialogmarketings ist auch zulässig, wenn die betroffene Person in diese eingewilligt hat. Die Frage, welche Voraussetzungen an eine wirksame Einwilligung zu knüpfen sind, wurde im Verlauf der Verhandlungen der Verordnung insbesondere mit Blick auf soziale Medien betrachtet. Die politische Kompromisssuche hat ein unübersichtliches und teilweise inkonsistentes Regelungsgerüst in der Verordnung hinterlassen.

Die Definition des Begriffs der Einwilligung hat sich im Vergleich zur Datenschutzrichtlinie von 1995 nicht wesentlich geändert. In der Regel werden deshalb Einwilligungen, die der Datenschutzrichtlinie entsprochen haben, auch den Anforderungen der Verordnung entsprechen. Die Verordnung erläutert jedoch die Detailanforderungen genauer. Teilweise unterscheiden sich diese Anforderungen von denen, die sich heute im nationalen Recht einiger Mitgliedstaaten finden. Es besteht deshalb das Risiko, dass im Einzelfall Einwilligungserklärungen unter der Grundverordnung nicht mehr wirksam sind. Deshalb sollten vorhandene Einwilligungserklärungen geprüft und gegebenenfalls überarbeitet werden.

ANFORDERUNG	ERLÄUTERUNG	QUELLE
Freiwillig	Gegebenenfalls nicht erfüllt, wenn • Vertrag von Abgabe der Einwilligung abhängig gemacht wird • Ungleichgewicht zwischen Verantwortlichem und einwilligender betroffener Person besteht (Beispiel Behörde) • für verschiedene Verarbeitungsvorgänge keine gesonderten Einwilligungen abgegeben werden können.	**Artikel 4 (11)** **Artikel 7 (4)** **Erwägungsgrund 42 und 43**
Für bestimmte Fälle	Die Einwilligung soll für konkrete Fälle gelten und sich auf alle Zwecke der Verarbeitungsvorgänge beziehen.	**Artikel 4 (11)** **Erwägungsgrund 32**
Informiert	Zumindest über Verantwortlichen und Zwecke der einwilligungsbasierten Verarbeitung.	**Artikel 4 (11)** **Erwägungsgrund 42**
Unmissverständlich	In Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung. Mündlich, schriftlich oder elektronisch. Jedoch nicht Stillschweigen oder Untätigkeit wie bei einem vorangekreuzten Kästchen.	**Artikel 4 (11)** **Erwägungsgrund 32**
Nachweisbar	Unternehmen muss Abgabe der Einwilligung nachweisen können.	**Artikel 7 (1)** **Erwägungsgrund 42**
Nicht missbräuchlich	Verweis auf Bedingungen für missbräuchliche Klauseln in Verbraucherverträgen.	**Erwägungsgrund 42**
Hinweis auf Widerrufsrecht	Muss vor Abgabe der Einwilligung erfolgen.	**Artikel 7 (3)**
Klar zu unterscheiden, verständlich, leicht zugänglich, klare und einfache Sprache	Unterscheidungspflicht gilt nur, wenn Einwilligung durch eine schriftliche Erklärung abgegeben wird, die noch andere Sachverhalte betrifft. Es muss klar sein, dass und in welchem Umfang eine Einwilligung erteilt wird.	**Artikel 7 (2)** **Erwägungsgrund 42**

→

ANFORDERUNG	ERLÄUTERUNG	QUELLE
Abgabe oder Zustimmung durch Erziehungs-berechtigten	Gilt nur bei Kindern bis 16 Jahren, wobei nationale Vorschriften die Grenze auf bis zu 13 Jahre heruntersetzen können.	**Artikel 8**
Ausdrücklich	Gilt nur bei besonderen Arten von Daten und beim Drittländertransfer.	**Artikel 9 (2) (a)** **Artikel 49 (1) (a)**
Knapp, klar und ohne unnötige Unterbrechung des Dienstes	Gilt nur für Einwilligungen, zu denen elektronisch aufgefordert wird.	**Erwägungsgrund 32**

Die vielfältigen Anforderungen der Verordnung an wirksame Einwilligungen führen in der Praxis zu erheblicher Rechtsunsicherheit. Deshalb stellt sich im konkreten Anwendungsfall immer erst die Frage, ob tatsächlich eine Einwilligung erforderlich ist. Häufig wird der Rückgriff auf andere Rechtsgrundlagen wie die Interessenabwägungsklausel) vorzugswürdig sein.

Die Anforderungen an Einwilligungen werden in den Erwägungsgründen teilweise anhand von Beispielen erläutert. Das Anklicken eines Kästchens beim Besuch einer Internetseite wird als eine solche Bekundung angesehen. Hingegen soll ein stillschweigendes Einverständnis durch ein standardmäßig vorangekreuztes Kästchen nicht ausreichend sein (Erwägungsgrund 32).

§ Einwilligung als zusätzliche Absicherung

Im Zweifel kann eine Einwilligung zur zusätzlichen Absicherung eingeholt werden. Sollte sie widerrufen werden, unwirksam oder nicht ausreichend nachweisbar sein, dann bleibt die Möglichkeit des Rückgriffs auf anderweitige Rechtsgrundlagen für die Verarbeitung der Daten erhalten. Die Verordnung erwähnt diese Möglichkeit konkret in der Regelung zum Recht auf Vergessenwerden (Artikel 17 (1) (b)). Daraus kann die Schlussfolgerung gezogen werden, dass ganz allgemein ein Rückgriff auf anderweitige Rechtsgrundlagen zulässig ist, wenn die Einwilligung nicht den Anforderungen der Verordnung genügt.

§ Einwilligung in elektronische Ansprache

Bei der elektronischen Ansprache fordert die ePrivacy Richtlinie in bestimmten Konstellationen Einwilligungen der betroffenen Personen. Die Verordnung stellt klar, dass sie keine zusätzlichen Pflichten auferlegen will (Artikel 95), soweit die ePrivacy Richtlinie Pflichten regelt, die dasselbe Ziel verfolgen. Dies gilt bis zur geplanten Ablösung der ePrivacy Richtlinie. Die ePrivacy Richtlinie bleibt vorerst wirksam. Für die nationalen Umsetzungsgesetze gilt dies jedoch nur, soweit sie nicht über den eingeschränkten Anwendungsbereich der ePrivacy Richtlinie hinausgehen.

Bei Einwilligungen in die elektronische Ansprache ist es in der Regel so, dass die Verarbeitung der Daten zur Vorbereitung einer Aussendung im Rahmen der Interessenabwägungsklausel zulässig ist. Hier genügt es, wenn sich die Einwilligung für elektronische Werbung nach der ePrivacy Richtlinie ausschließlich auf die elektronische Aussendung

bezieht. Es sollte aber darauf hingewiesen werden, ob die Werbung nur eigene oder auch fremde Produkte und Dienstleistungen umfasst. Außerdem sollte deutlich werden, ob die Einwilligung auch für Aussendungen durch dritte Unternehmen gelten soll.

§ Unmissverständliche oder ausdrückliche Einwilligung

Die Verordnung unterscheidet zwischen unmissverständlichen und ausdrücklichen Einwilligungen. Ausdrücklich muss die Einwilligung bei besonderen Kategorien von personenbezogenen Daten (Artikel 9) und bei Übermittlungen in Drittländer erklärt werden (Artikel 49 (1) (a)). Im Bereich des Dialogmarketings wird damit nur in Ausnahmefällen eine ausdrückliche Einwilligung erforderlich sein. Untätigkeit, Stillschweigen oder vorangekreuzte Kästchen genügen aber auch für eine „unmissverständliche" Einwilligung nicht. Der Einwurf einer Visitenkarte bei einer Messe sollte jedoch der Anforderung genügen.

§ Eingeschränktes Kopplungsverbot

Die Verordnung fordert, dass bei der Beurteilung der Freiwilligkeit einer Einwilligung in „größtmöglichem Umfang" berücksichtigt werden solle, ob die Erfüllung eines Vertrages von einer Einwilligung abhängig gemacht wird (Artikel 7 (4)). Die Einwilligung soll nur dann als freiwillig gelten, wenn eine echte oder freie Wahl besteht. Die Verweigerung oder der Widerruf der Einwilligung darf keine Nachteile nach sich ziehen (Erwägungsgrund 42). Für verschiedene Verarbeitungsvorgänge sollten getrennte Einwilligungserklärungen eingeholt werden (Erwägungsgrund 43).

Aus den Anforderungen ergibt sich ein eingeschränktes Kopplungsverbot. Dies soll nicht gelten, wenn die „Einwilligung" zur Erfüllung eines Vertrages erforderlich ist. Die Verordnung meint hier nicht Konstellationen, bei denen die „Verarbeitung" der Daten für die Erfüllung eines Vertrages erforderlich ist, denn hierfür bedarf es ohnehin keiner Einwilligung (Artikel 6 (1) (b)).

Wenn ein Vertrag geschlossen wird, der die Verarbeitung von Daten zu Werbezwecken als Leistung oder Gegenleistung enthält, dann ist eine Einwilligung in diese Verarbeitung zur Erfüllung des Vertrages nicht erforderlich. Artikel 7 (4) betrifft dagegen Fälle, in denen es einer Einwilligung bedarf. Und eine solche Einwilligung darf nur dann an den Vertragsschluss gekoppelt werden, wenn sie zur Erfüllung des Vertrages erforderlich ist. Beispiele hierfür sind Gewinnspiele, Gutscheine oder andere Sonderleistungen, die im Austausch gegen eine Einwilligung gewährt werden. Die Voraussetzung wird auch erfüllt, wenn der Dienst sich über einwilligungsbasierte Datenverarbeitungen finanziert. Teilweise wird das Kopplungsverbot strenger ausgelegt. Insofern ist zu empfehlen, von Kopplungen soweit möglich abzusehen.

§ Einwilligung durch Kinder

Für Einwilligungen, die von Kindern unter 16 Jahren im Zusammenhang mit dem Angebot eines Dienstes der Informationsgesellschaft einholt werden, fordert die Verordnung die Zustimmung der Erziehungsberechtigten (Artikel 8). Den Mitgliedstaaten ist freigestellt, die Altersgrenze auf 13 Jahre zu senken. Die Regelung dürfte deshalb wenig zur Harmonisierung in der Europäischen Union beitragen. Wer Dienste gegenüber Kindern unter 16 Jahre anbietet, wird angesichts der bestehenden technischen Möglichkeiten außerdem selten mit Sicherheit feststellen können, ob eine Zustimmung der Erziehungsberechtigten vorliegt.

Deshalb ist auch hier stets die Frage zu stellen, ob überhaupt eine Einwilligung erforderlich ist. Bei der Interessenabwägung wird zwar ausdrücklich darauf hingewiesen, dass die schutzwürdigen Interessen von Kindern zu beachten sind (Artikel 6 (1) (f)). Die Anwendung der Interessenabwägungsklausel als Alternative zu einer Einwilligung ist jedoch nicht ausgeschlossen. Bei der Beurteilung der schutzwürdigen Interessen muss aber eine sensiblere Gewichtung erfolgen.

ALTERNATIVE 3: ZWECKÄNDERUNG

Eine weitere Grundlage für die Verarbeitung von Daten besteht dann, wenn die Daten ursprünglich zwar nicht zu Zwecken des Dialogmarketings erhoben wurden, die Zwecke der ursprünglichen Erhebung jedoch hiermit vereinbar sind (Artikel 5 (1) (b) und 6 (4)). In einer solchen Konstellation bedarf es keiner gesonderten Rechtsgrundlage (Erwägungsgrund 50) für die weitere Verarbeitung. Die Anforderungen an eine „vereinbare" Zweckänderung ersetzen damit die Prüfung unter der Interessenabwägungsklausel. Teilweise wird vertreten, dass die Zweckänderungsregelung zusätzliche eingrenzende Kriterien enthält. Die Ansicht ist jedoch mit dem Wortlaut von Erwägungsgrund 50 nicht vereinbar.

Im Dialogmarketing hat die Klausel zu Zweckänderungen nur eine sehr eingeschränkte Bedeutung, denn im kommerziellen Umfeld werden Daten stets auch zu Werbezwecken erhoben. Spätere Zweckänderungen sind nicht erforderlich und die Zweckänderungsklausel findet deshalb keine Anwendung. Soweit Daten zu statistischen Zwecken weiterverwendet werden (beispielsweise im Rahmen von Big Data-Anwendungen) und nicht auch zu diesen Zwecken erhoben wurden, liegt stets eine zulässige Zweckänderung vor (Artikel 5 (1) (b)).

In den seltenen Fällen, in denen im Dialogmarketing ein Rückgriff auf die Zweckänderungsklausel erforderlich ist, bedarf es eines Abgleichs mit den ursprünglichen Zwecken der Erhebung. Die Rechtsgrundlage listet fünf Kriterien auf, die im Ergebnis eine besondere Art der Interessenabwägung darstellen (Artikel 6 (4)). In der Regel dürfte deshalb die Zweckänderungsklausel die Verarbeitung von Daten zu Zwecken des Dialogmarketings rechtfertigen, selbst wenn sie ursprünglich zu anderen Zwecken erhoben wurden.

§ Kann eine Zweckänderung auf Grund der Interessenabwägungsklausel erfolgen?

Im ursprünglichen Entwurf der Verordnung hatte die Europäische Kommission vorgeschlagen, dass Zweckänderungen nicht auf Grund der Interessenabwägungsklausel gerechtfertigt werden können. Wenn die neuen Zwecke mit den alten nicht „vereinbar" gewesen wären, hätte diese Regelung eine weitere Verarbeitung auf Grund der Interessenabwägungsklausel ausgeschlossen. Diese einschränkende Klausel wurde im Verlauf der Verhandlungen gestrichen. Die Verordnung belässt es im Ergebnis beim Verhältnis zwischen Zweckänderung und Rechtsgrundlage, wie es bereits in der Europäischen Datenschutzrichtlinie enthalten ist.

Die Konzeption der Zweckänderungsklausel sieht demnach wie folgt aus: Wenn die Zweckänderung mit den ursprünglichen Zwecken vereinbar ist, dann bedarf es keiner weiteren Rechtsgrundlage. Wenn sie unvereinbar ist, dann ist die Verarbeitung zu den weiteren Zwecken grundsätzlich nicht zulässig. Wie unter der Europäischen Datenschutzrichtlinie schließt dies aber nicht aus, dass eine weitere Verarbeitung durch eine andere Rechtsvorschrift erlaubt wird.

Selbst wenn die Verwendung zu Zwecken des Dialogmarketings ausnahmsweise nicht von Anfang an Zweck der Verarbeitung war, lässt sich die Verarbeitung deshalb durch die Interessenabwägungsklausel rechtfertigen.

→

Angesichts der kontrovers geführten Verhandlungen zur Zweckbindung ist damit zu rechnen, dass im Rahmen der Auslegung der neuen Regelung unterschiedliche Meinungen vertreten werden. Die Verfechter einer strengen Zweckbindung werden eine Rückgriffsmöglichkeit auf die Interessenabwägungsklausel gegebenenfalls ablehnen. Dagegen sprechen Formulierungen in Erwägungsgrund 50. Er stellt klar, dass Zweckänderungen, die mit den ursprünglichen Zwecken vereinbar sind, keine eigene Rechtsgrundlage benötigen. Damit wird eine Zweistufigkeit der Anforderungen vorgegeben (1. Stufe: ohne gesonderte Rechtsgrundlage; 2. Stufe: mit gesonderter Rechtsgrundlage), die eine Rückgriffsmöglichkeit auf andere Rechtsgrundlagen nahe legt.

Da „unvereinbare" Zweckänderungen im Bereich des Dialogmarketings ohnehin einen seltenen Sonderfall darstellen, ist die Frage für die Praxis jedoch nicht von ausschlaggebender Bedeutung.

2.2 WIDERSPRUCH DES ADRESSATEN BEACHTEN

Da die Verordnung im Grundsatz das Opt-Out-Prinzip bei der Verarbeitung von Daten zu Zwecken des Dialogmarketings beibehält, sind die Regelungen zum Widerspruchsrecht von großer praktischer Bedeutung (Artikel 21 und Erwägungsgrund 57). Widerspricht die betroffene Person der Verarbeitung für Zwecke der Direktwerbung, so hat der Verantwortliche dies unverzüglich sicherzustellen. Die betroffene Person muss spätestens zum Zeitpunkt der ersten Kommunikation ausdrücklich auf das Widerspruchsrecht hingewiesen werden (Artikel 21 (4)). Der Hinweis soll verständlich und getrennt von anderen Informationen erfolgen. Konkrete Beispiele für solche Hinweise werden unter Ziffer 3 dieses Best Practice Guides gegeben.

Wenn ein Adressat der Verwendung seiner Daten zu Werbezwecken widerspricht, dann ist ein solcher Widerspruch strikt zu beachten. Niemandem darf Werbung gegen seinen Willen gesendet werden. Die Selbstbestimmung der betroffenen Person ist in diesem Fall vorrangig.

Bei der Umsetzung von Werbewidersprüchen stellt sich immer wieder das Problem, dass zum Zeitpunkt des Empfangs eines Widerspruchs bereits weitere Werbesendungen veranlasst worden sind. So können beispielsweise Prospekte mit den Adressen bedruckt worden sein. Wenn es mit angemessenem Aufwand nicht möglich ist, solche Sendung noch auszusortieren, dann sollte der Empfänger in der Antwort auf das Widerspruchsschreiben hierauf hingewiesen werden.

Soweit unternehmensübergreifende Sperrlisten geführt werden, wie beispielsweise die unter www.ichhabediewahl.de erreichbare Robinsonliste des DDV, können diejenigen darüber informiert werden, die bei einem Unternehmen einen Widerspruch einlegen.

Wenn der Werbetreibende den Widerspruch einer betroffenen Person erhält, dann kommt es für die notwendige Reaktion auf den genauen Willen der betroffenen Person an. In der Praxis sind die Variationen der Eingaben von Verbrauchern unbegrenzt. Häufig lässt sich der tatsächliche Wille nur durch Auslegung zu ermitteln.

Variante 1: „Ich möchte von Ihnen keine Werbung erhalten."
Der Widerspruch richtet sich an den Werbetreibenden. Um dem Willen der widersprechenden Person zu entsprechen, kann er die Adresse beispielsweise in eine interne Sperrliste aufnehmen. Die Führung einer solchen Sperrliste erfolgt im Interesse des Betroffenen. Er ist über die Aufnahme in die Sperrliste zu informieren. Neue Werbeaussendungen des Werbetreibenden sind mit der Sperrliste abzugleichen. Wegen der bekannten und nicht zu verhindernden Unsicherheiten bei Adressabgleichen lässt sich damit nicht immer eine erneute Werbeaussendung an die betroffene Person vermeiden. Vom Werbetreibenden kann aber nicht mehr als die Anwendung der erforderlichen Sorgfalt erwartet werden.

Variante 2: „Ich möchte keine Werbung von Firmen erhalten, mit denen ich nichts zu tun habe."
Der Werbetreibende sollte die widersprechende Person auch hier in eine interne Sperrliste aufnehmen. Darüber hinaus wird empfohlen, dass die Adressdaten nicht mehr Dritten zur Verfügung gestellt werden. Die widersprechende Person ist über die Aufnahme in die Sperrliste zu informieren.

Variante 3: „Bitte löschen Sie meine Daten".
Häufig wird von betroffenen Personen die Löschung ihrer Daten gefordert, um damit weitere Werbezusendungen zu verhindern. Wenn der Betroffene ein solches Löschungsbegehren vorbringt, sollte er in die Sperrliste aufgenommen werden. Anschließend sollte darauf hingewiesen werden, dass eine dauerhafte Einstellung von Werbeansprachen nur mit Hilfe der Sperrung, nicht jedoch einer Löschung der Daten sichergestellt werden kann. Zugleich sollte die betroffene Person darauf hingewiesen werden, dass sie sich nochmals melden möge, wenn sie gleichwohl eine vollständige Löschung, also auch aus der Sperrdatei, wünscht.

2.3 VERARBEITUNGSGRUNDSÄTZE

Die Verordnung enthält eine Reihe von Verarbeitungsgrundsätzen (Artikel 5). Diese werden weitgehend durch die Detailregelungen der Verordnung konkretisiert und haben insofern keine eigenständige Bedeutung. Unternehmen müssen nachweisen können, dass sie die Grundsätze einhalten (Artikel 5 (2)). Für das Dialogmarketing ist hinsichtlich der Verarbeitungsgrundsätze insbesondere Folgendes zu beachten:

Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
Personenbezogene Daten müssen auf rechtmäßige Weise, nach dem Grundsatz von Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden. Dieser Anforderung wird genügt, wenn die konkreten Rechtmäßigkeits- und Transparenzanforderungen eingehalten werden (siehe Ziffern 2 und 3 dieses Best Practice Guides).

Zweckbindung
Personenbezogene Daten sollen für festgelegte, eindeutige und rechtmäßige Zwecke verarbeitet werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden. Da im kommerziellen Umfeld personenbezogene Daten stets auch für Zwecke des Dialogmarketings erhoben werden, kommt es in der Regel nicht zu späteren Zweckänderungen (siehe Ziffer 2.1 Alternative 3 dieses Best Practice

Guides). Der Verarbeitungsgrundsatz ist deshalb von untergeordneter praktischer Bedeutung für den Bereich des Dialogmarketings. Wichtig ist, dass die Verarbeitung zu Werbezwecken von Anfang an zu den Zwecken der Erhebung der Daten gehört.

Datenminimierung
Personenbezogene Daten sollen für die Zwecke ihrer Verarbeitung angemessen und sachlich relevant sowie auf das für Zwecke der Verarbeitung notwendige Maß beschränkt sein. Wenn personenbezogene Daten zu Zwecken des Dialogmarketings verarbeitet werden, dann muss entsprechend darauf geachtet werden, dass die verarbeiteten Daten für die Ansprache und Selektion angemessen und sachlich relevant sind.

Richtigkeit
Personenbezogene Daten sollen richtig sein und erforderlichenfalls auf den neusten Stand gebracht werden. Hierzu sind angemessene Maßnahmen zu treffen. In Bezug auf Dialogmarketing ist dabei vor allem an Maßnahmen zur Adressbereinigung, -korrektur und -aktualisierung zu denken. Die Maßnahmen können je nach Einzelfall angemessen sein, wenn beispielsweise Datendienstleister entsprechende Leistungen zu angemessenen Konditionen anbieten.

Speicherbegrenzung
Die Identifizierung der betroffenen Personen soll nur solange möglich sein, wie sie zum Zweck der Speicherung erforderlich ist. Da Dialogmarketing die Ansprache der Adressaten erfordert, bedarf es in der Regel einer Identifizierung. Im Bereich der Selektionsverfahren können pseudonymisierte Datenbestände in Betracht kommen. Meistens wird aber auch die Selektion eine Identifizierung erfordern. Ihre zeitliche Grenze findet die Speicherung der Daten zu Zwecken des Dialogmarketings jedoch dann, wenn die Daten kein Werbepotential mehr haben und deshalb für die Zwecke des Dialogmarketings nicht mehr brauchbar sind. Pauschalisierte zeitliche Grenzen lassen sich hierfür nicht festlegen. Wenn jedoch ein Adressat über einen längeren Zeitraum offensichtlich nicht mehr auf Ansprachen reagiert hat, sollten die Daten nicht mehr für Zwecke des Dialogmarketings verwendet werden. Es greifen außerdem Informationspflichten in Bezug auf die Speicherdauer (siehe Ziffer 3.1 des Best Practice Guides), die eine Festlegung von Löschrichtlinien erfordern. Auch diese müssen jedoch keine fixen Zeitvorgaben enthalten.

Integrität und Vertraulichkeit
Bei der Verarbeitung personenbezogener Daten ist ein angemessener Schutz zu gewährleisten. Die Verordnung spezifiziert diese Anforderung durch konkrete Anforderungen an die Datensicherheit (Artikel 32). Es sind geeignete technische und organisatorische Maßnahmen zu treffen. Dabei sind der Stand der Technik, die Implementierungskosten sowie Art, Umfang, Umstände, Zweck und Risiko der Verarbeitung zu berücksichtigen. Bei der Verarbeitung von reinen Adressen sind die Anforderungen damit geringer als bei der Verarbeitung von Adressen mit umfangreichen und sensiblen Selektionskriterien.

2.4 DATENVERARBEITUNG IM KONZERN

Die Verordnung sieht keine pauschale Vereinfachung für den Datenaustausch zwischen Konzerngesellschaften vor. Jede Gesellschaft ist weiterhin datenschutzrechtlich als separate Einheit zu betrachten. Um konzernübergreifende Customer Relationship Management-Systeme (CRM-Systeme) zu betreiben und Daten hieraus für Zwecke des Dialogmarketings verwenden zu können, kann auf die Interessenabwägungsklausel oder auf Konzerneinwilligungen zurückgegriffen werden. Das berechtigte Interesse am konzerninternen Datenaustausch für interne Verwaltungszwecke erkennt die Verordnung ausdrücklich an (Erwägungsgrund 48).

Die Rechtsgrundlagen geben den Handlungsspielraum für konzernweite CRM-Systeme vor. Im Rahmen der Interessenabwägung sind bei einer konzerninternen Übermittlung die berechtigten Interessen der Unternehmen in der Regel höher und die schutzwürdigen Interessen der betroffenen Personen niedriger als beim Austausch zwischen konzernfremden Unternehmen zu bewerten.

Die Verordnung regelt gesondert die Konstellation, dass mehrere Unternehmen gemeinsam für einen Datenbestand verantwortlich sein können (Artikel 26). Die beteiligten Unternehmen können hierzu untereinander vertraglich ihre jeweiligen Verpflichtungen regeln. Für konzernübergreifende CRM-Systeme liegt eine solche gemeinsame Verantwortlichkeit häufig nahe. Alternativ ist zu überlegen, ob das CRM-System durch eine Dienstleistungsgesellschaft im Rahmen einer Auftragsverarbeitung (siehe Ziffer 4 des Best Practice Guides) gestaltet werden kann. Es sind auch Mischformen denkbar.

3. TRANSPARENZ VERSTÄNDLICH HERSTELLEN

3.1 ALLGEMEINE INFORMATIONSPFLICHTEN

Die Verordnung unterscheidet bei den Informationspflichten zwischen der Erhebung der Daten bei der betroffenen Person (Artikel 13) und der Erhebung aus anderen Quellen (Artikel 14). Die Unterscheidung rechtfertigt sich deshalb, weil im Falle einer Erhebung bei der betroffenen Person die Benachrichtigung in der Regel einfacher durchführbar ist. Die Informationspflichten sind im Falle einer Erhebung bei der betroffenen Person strikter und nur im Falle der Erhebung aus anderen Quellen gelten Ausnahmen.

Die Benachrichtigungspflichten unterscheiden weiter nach Mindestinformationen und zusätzlichen Informationen. Die Mindestinformationen sind immer mitzuteilen. Die zusätzlichen Informationen sind dann zur Verfügung zu stellen, wenn sie für eine faire und transparente Verarbeitung notwendig bzw. erforderlich sind. Das Differenzierungskriterium bietet wenig Rechtssicherheit. Deshalb empfiehlt sich eine umfassende Information immer dann, wenn dies technisch einfach umzusetzen ist (wie beispielsweise in Datenschutzinformationen auf Internetseiten).

Erwägungsgrund 58 erwähnt ausdrücklich, dass Datenschutzinformationen auch auf einer öffentlich zugänglichen Internetseite gegeben werden können. Insofern bietet sich die Möglichkeit an, die Informationen in zwei Schichten zu geben. Beispielsweise können die gesetzlich zwingenden Informationen unmittelbar in einem Werbeschreiben gegeben werden und für weitere Informationen wird auf eine Internetseite verwiesen. Dort können auch Informationen gegeben werden, die nicht zwingend erforderlich sind oder Änderungen unterliegen (wie beispielsweise Nennung des Datenschutzbeauftragten, der Konzernunternehmen oder von Kategorien von möglichen Empfängern der Daten).

In der Praxis problematisch ist die Einhaltung der Informationspflichten, wenn Werbeträger verwendet werden, die keine umfangreichen Informationen zulassen. Dies gilt beispielsweise für Zeitungsanzeigen mit Coupons. Auch hier sind Verweise auf Internet-Seiten denkbar, wobei sich auf einem Coupon in der Regel nicht einmal die Mindestinformationen unterbringen lassen. Zu überlegen ist deshalb, wann in dieser Konstellation die Erhebung stattfindet, denn die Daten erreichen den Werbetreibenden erst, wenn der zurückgesendete Coupon im Unternehmen eingeht. Zu diesem Zeitpunkt ist dann die Information durchzuführen. Die Verordnung fordert nicht, dass die Information „vor“ der Erhebung erfolgt. Insofern erscheint es vertretbar, wenn die betroffenen Personen unmittelbar nach Zugang des Coupons im Unternehmen informiert werden.

Auf das Widerspruchsrecht gegen die Nutzung zu Marketingzwecken sollte möglichst frühzeitig hingewiesen werden, obgleich ein Hinweis in der ersten Kommunikation ausreichend ist (Artikel 21 (4)). Wenn eine Einwilligung eingeholt wird, sind die dafür geforderten Informationen gleichzeitig zu erteilen (siehe Ziffer 2.1 des Best Practice Guides).

Soweit die betroffene Person bereits über eine Information verfügt, bedarf es keiner nochmaligen Information (Artikel 13 (4) und 14 (5) (a)). Da allgemein bekannt ist, dass im kommerziellen Umfeld erhobene Daten auch zu Zwecken des Dialogmarketings verwendet werden, stellt sich deshalb die Frage, ob hierüber überhaupt informiert werden muss. Ein Auslassen der Informationen mit dieser Begründung ist jedoch nicht zu empfehlen, denn die Erwartungen der betroffenen Personen können je nach Konstellation unterschiedlich sein. Außerdem sollte auf das Widerspruchsrecht möglichst in jeder Werbeansprache hingewiesen werden. Der Hinweis muss in verständlicher Form erfolgen und sollte von anderen Informationen getrennt sein (Artikel 21 (4)).

Wenn die Daten nicht direkt von der betroffenen Person erhoben werden (wie beispielsweise bei der Erhebung aus öffentlich zugänglichen Quellen oder von anderen Marktteilnehmern), besteht die Informationspflicht nur insoweit, als sie keinen unverhältnismäßigen Aufwand verursacht (Artikel 14 (5) (b)). Dies kann beispielsweise wegen der hohen Anzahl der betroffenen Personen der Fall sein.

Wenn wegen eines möglichen unverhältnismäßigen Aufwands keine Information erfolgt, dann sollte zumindest auf der Webseite des Unternehmens eine allgemeine Datenschutzinformation erfolgen.

Die Information der betroffenen Person sollte spätestens bei der ersten Ansprache erfolgen. Zu diesem Zeitpunkt ist spätestens über das Widerspruchsrecht der betroffenen Person zu informieren (Artikel 21 (4)). Wenn eine solche Ansprache erfolgt, dürfte die sonstige Information auch keinen unverhältnismäßigen Aufwand mehr darstellen. Deshalb sollte spätestens zum Zeitpunkt der ersten Ansprache vollständig informiert werden.

BEISPIEL 1: Ein Werbetreibender setzt Adressdaten von eigenen Kunden und Interessenten zur Bewerbung eigener Waren und Dienstleistungen ein und plant auch Dritten die Daten im Lettershop-Verfahren zur Neukundengewinnung zur Verfügung zu stellen. Bereits bei der Erhebung der Daten sollte er über diese Zwecke und das Widerspruchsrecht informieren.

FORMULIERUNGSVORSCHLAG:
„Datenschutzinformation: Wir sind daran interessiert, die Kundenbeziehung mit Ihnen zu pflegen und Ihnen Informationen und Angebote zukommen zu lassen. Deshalb verarbeiten wir auf Grundlage von Artikel 6 (1) (f) der Europäischen Datenschutz-Grundverordnung (auch mit Hilfe von Dienstleistern) Ihre Daten, um Ihnen Informationen und Angebote von uns und anderen Unternehmen zuzusenden. Wenn Sie dies nicht wünschen, können Sie jederzeit bei uns der Verwendung Ihrer Daten für Werbezwecke widersprechen. [OPTIONAL: Sie können den Widerspruch auch per E-Mail senden an: E-MAIL ADRESSE.] Weitere Informationen zum Datenschutz erhalten Sie unter [INTERNETLINK ZUR AUSFÜHRLICHEN DATENSCHUTZINFORMATION]. Unseren Datenschutzbeauftragten erreichen Sie ebenfalls unter unserer Anschrift."

3.2 INFORMATIONEN IM WERBESCHREIBEN

Zum Zeitpunkt der Versendung der ersten Kommunikation verfügen die betroffenen Personen in der Regel über die erforderlichen Informationen. Wenn frühzeitig über das Widerspruchsrecht informiert wird, bedarf es auch hierzu keiner erneuten Information.

Insofern können sich Teile der Information erübrigen. Da das Widerspruchsrecht jedoch die zentrale gesetzgeberische Rechtfertigung dafür ist, dass ohne Einwilligung Werbung versendet werden kann, sollte die Information hierüber bei jeder Ansprache erfolgen.

Wenn ein Unternehmen (Adresseigner) Werbung für einen Dritten im Lettershopverfahren versendet, dann sollte die Datenschutzinformation des Werbetreibenden (siehe Bespiel 1) aufgenommen werden. Auf diese Weise werden die Adressaten über die Zwecke der Erhebung und ihr Widerspruchsrecht informiert, wenn sie sich auf Grund des Werbeschreibens an den Werbetreibenden wenden.

Erhält der Werbetreibende aufgrund einer im Lettershopverfahren verwendeten Werbung einen Werbewiderspruch des Adressaten, dann hat er diesen zu beachten. Außerdem sollte der Werbetreibende das Unternehmen, das die Versendung vorgenommen hat, über den Widerspruch informieren, damit die Adresse nicht mehr im Lettershopverfahren zur Verfügung gestellt wird.

Wenn Daten nicht direkt bei der betroffenen Person erhoben werden (beispielsweise aus öffentlich zugänglichen Quellen, von anderen Marktteilnehmern oder Datendienstleistern), dann wird die erste Kommunikation in der Regel die erste Gelegenheit sein, um die betroffene Person ohne unverhältnismäßigen Aufwand zu informieren. In diesem Fall muss die Information umfassend erfolgen und auch die Information über das Widerspruchsrecht enthalten.

BEISPIEL 2: Ein Werbetreibender erhebt Adressdaten aus einer öffentlich zugänglichen Quelle und setzt diese für Werbekampagnen ein.

FORMULIERUNGSVORSCHLAG:
„Datenschutzinformation: Wir sind daran interessiert, Sie als Kunden zu gewinnen, die Kundenbeziehung mit Ihnen zu pflegen und Ihnen Informationen und Angebote zukommen zu lassen. Deshalb verarbeiten wir auf Grundlage von Artikel 6 (1) (f) der Europäischen Datenschutz-Grundverordnung (auch mit Hilfe von Dienstleistern) Ihre Adressdaten und Kriterien zur interessengerechten Werbeselektion, um Ihnen solche Informationen und Angebote von uns und anderen Unternehmen zuzusenden. Wenn Sie dies nicht wünschen, können Sie bei uns jederzeit der Verwendung Ihrer Daten für Werbezwecke widersprechen. Sie erleichtern uns die schnelle Bearbeitung eines Widerspruchs, wenn Sie das Werbemittel beifügen. [OPTIONAL: Sie können den Widerspruch auch per E-Mail senden an: E-MAIL ADRESSE.] Weitere Informationen zum Datenschutz erhalten Sie unter [INTERNETLINK ZUR AUSFÜHRLICHEN DATENSCHUTZINFORMATION]. Unseren Datenschutzbeauftragten erreichen Sie ebenfalls unter unserer Anschrift.“

3.3 INFORMATION ÜBER DATENSCHUTZVERSTÖSSE

Die Verordnung sieht für den Fall der Verletzung des Schutzes personenbezogener Daten Melde- und Informationspflichten vor (Artikel 33 und 34). Die Aufsichtsbehörde ist unverzüglich (spätestens innerhalb von 72 Stunden) zu informieren, wenn die Verletzung voraussichtlich zu einem Risiko für persönlichen Rechte und Freiheiten der betroffenen Personen führt (Artikel 33). Besteht die Wahrscheinlichkeit eines „hohen“ Risikos, dann müssen auch die betroffenen Personen unverzüglich informiert werden.

Um diesen Informationspflichten ausreichend gerecht werden zu können und um eine möglichst zuverlässige Reaktion auf Datenschutzverstöße sicherzustellen, sind organisatorische Maßnahmen im Unternehmen zu treffen. Jedem Mitarbeiter muss bekannt sein, an wen Datenschutzverstöße im Unternehmen zu melden sind. Entsprechend sind Auftragsverarbeiter zu einer Durchmeldung zu verpflichten, die eine rechtzeitige Information durch das Unternehmen ermöglicht.

4. DIENSTLEISTER RICHTIG BEAUFTRAGEN

4.1 AUFTRAGSVERARBEITER

Die Verordnung erlaubt den Einsatz von Lettershops und anderen Dienstleistern als so genannte Auftragsverarbeiter, die weisungsgebunden für das beauftragende Unternehmen tätig sind (Artikel 28). Dabei gilt weiterhin die Besonderheit, dass die Weitergabe von Daten an solche Dienstleister keine Übermittlung an einen Dritten darstellt (Artikel 4 (10)). Es wird praktisch so getan, als wenn der Dienstleister Teil des beauftragenden Unternehmens wäre. Ebenso werden Unterauftragnehmer der jeweiligen Dienstleister behandelt. Auf diese Weise soll sichergestellt werden, dass datenschutzrechtliche Vorschriften die Arbeitsteilung mit Dienstleistern nicht unnötig erschweren.

Die Sonderregelungen für Auftragsverarbeiter schützen die betroffenen Personen und erleichtern die rechtliche Zulässigkeit des Einsatzes von Dienstleistern. Wenn beispielsweise über einen Lettershop eine Werbung ausgesendet wird, werden die Adressdaten in der Regel nicht für die Aussendung an den Werbetreibenden übermittelt. Stattdessen beauftragt der Adresseigner die Dienstleister (Lettershop oder andere Dienstleister) als Auftragsverarbeiter (so genanntes Lettershop-Verfahren). Auf diese Weise bleibt der Adresseigner Verantwortlicher für die Verarbeitung der Daten.

Keine Auftragsverarbeitung liegt bei einer so genannten Funktionsübertragung vor. Die Abgrenzung zwischen Auftragsverarbeitung und Funktionsübertragung ist ungenau. Lettershops und andere Dienstleister werden als Auftragsverarbeiter angesehen, wenn der Auftraggeber allein über die Zwecke und Mittel der Datenverarbeitung entscheidet. Deshalb ist es wichtig, dass Adresseigner die Entscheidung über die Nutzung ihrer Adressen selbst treffen.

4.2 MINDESTANFORDERUNGEN AN DEN VERTRAG

Der Vertrag mit einem Auftragsverarbeiter muss Gegenstand, Dauer, Art und Zweck der Verarbeitung sowie die Art der personenbezogenen Daten, die Kategorien der betroffenen Personen und die Rechte und Pflichten des Auftraggebers festlegen (Artikel 28 (3)).

Außerdem sind zumindest folgende Themen zu regeln:

- Dokumentierte Weisung
- Vertraulichkeitsverpflichtung
- Sicherheitsmaßnahmen
- Unterauftragsverarbeiter
- Betroffenenrechte
- Unterstützung
- Löschung und Rückgabe von Daten

Der DDV hat die besonderen Anforderungen der Auftragsverarbeitung in seinen Qualitäts- und Leistungsstandards (QuLS) umgesetzt. Zusätzlich stellt der DDV Mitgliedern und Nichtmitgliedern als Mustertext eine Indidualvereinbarung zur Auftragsverarbeitung bereit.

In der Übergangsphase bis zum Wirksamwerden der Verordnung ist zu empfehlen, parallel die Regelungen zu vereinbaren, die bis zum 24. Mai 2018 gelten sollen und solche, die ab dem 25. Mai 2018 die alten Regelungen ablösen. Auf diese Weise kann der Aufwand der Umstellung reduziert werden.

Die DDV-Mitglieder, die sich den DDV-Regeln zur Auftragverarbeitung unterworfen haben, sind auf der Website des DDV (www.ddv.de) aufgelistet. Diese werden vom DDV im Rahmen der Kontrolle der Einhaltung der Qualitäts- und Leistungsstandards geprüft.

4.3 VERANTWORTLICHKEITEN DES DIENSTLEISTERS

Die Verordnung erweitert die Verantwortlichkeiten von Dienstleistern. Sie müssen beispielsweise Aufzeichnungen über die von ihnen durchgeführten Verarbeitungen führen (Artikel 30 (2)) und mit den Aufsichtsbehörden kooperieren (Artikel 31). Außerdem können betroffene Personen direkt gegen den Auftragsverarbeiter Haftungsansprüche geltend machen. Die Aufsichtsbehörden können Sanktionen verhängen. Im Verhältnis zwischen Auftraggeber und Auftragnehmer entsteht deshalb zusätzlicher Regelungsbedarf über einen möglichen Innenausgleich.

5. DATENSCHUTZ EFFEKTIV DURCHSETZEN

5.1 VERFAHRENSVERZEICHNIS

Unternehmen und ihre Dienstleister sollen die von ihnen durchgeführte Datenverarbeitung überblicken. Hierzu müssen Verzeichnisse über die Verarbeitungstätigkeiten geführt werden. Ausgenommen von der Verpflichtung sind Unternehmen mit weniger als 250 Mitarbeitern. Die Ausnahme gilt jedoch nicht, wenn ein besonderes Risiko mit der Verarbeitung verbunden ist, sie nicht nur gelegentlich erfolgt oder besonders sensible Daten verarbeitet werden (Artikel 30 (5)).

Im Bereich des Dialogmarketings sind bei einem Großteil der Unternehmen und Dienstleister weniger als 250 Mitarbeiter beschäftigt. Jedoch finden die Verarbeitungen in der Regel „nicht nur gelegentlich“ statt. Deshalb dürfte die Pflicht zum Führen eines Verfahrensverzeichnisses häufig Anwendung finden. Neu ist, dass auch Auftragsverarbeiter ein Verfahrensverzeichnis führen müssen. Mit dem Auftraggeber ist deshalb zu vereinbaren, wie der Auftragnehmer die entsprechenden Informationen erhält oder ob der Auftraggeber das Verzeichnis für den Auftragnehmer führt.

Das Verzeichnis kann in elektronischer Form geführt werden (Artikel 30 (3)). Auf Anforderung ist es der zuständigen Aufsichtsbehörde zur Verfügung zu stellen. Die Verordnung sieht keine Registrierung oder Meldung von Datenverarbeitungen an die jeweiligen Aufsichtsbehörden vor. Es besteht kein Recht von Jedermann auf Einsicht in das Verzeichnis.

5.2 BETRIEBLICHE DATENSCHUTZBEAUFTRAGTE

Die Verordnung fordert in bestimmten Konstellationen die Bestellung eines betrieblichen Datenschutzbeauftragten (Artikel 37). Auslöser für die Verpflichtung sind unter der Verordnung keine starren Mitarbeitergrenzen. Ausgangspunkt ist die Frage, worin die Kerntätigkeit eines Unternehmens besteht. Ein Datenschutzbeauftragter ist zu bestellen, wenn die Kerntätigkeit eine umfangreiche, regelmäßige und systematische Beobachtung von

betroffenen Personen erfordert oder eine umfangreiche Verarbeitung von sensiblen Daten erfolgt. Im Bereich des Dialogmarketings ist dies regelmäßig nicht der Fall. Es kann aber empfehlenswert sein, dennoch einen betrieblichen Datenschutzbeauftragten zu bestellen oder zumindest einen Datenschutzverantwortlichen zu benennen, um intern die hiermit verbundenen Aufgaben zuzuweisen.

Die Verordnung gibt den Mitgliedstaaten die Möglichkeit, die Verpflichtung zur Bestellung auf weitere Fälle zu erweitern. Es bleibt abzuwarten, in welchem Umfang die Mitgliedstaaten hiervon Gebrauch machen. Im deutschen Umsetzungsgesetz wurde von diesem Regelungsspielraum Gebrauch gemacht. Wenn mehr als neun Mitarbeiter ständig mit der Verarbeitung von personenbezogenen Daten befasst sind, ist ein Datenschutzbeauftragter zu bestellen. Dies gilt auch für Auftragsverarbeiter.

5.3 TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

Unternehmen treffen in der Regel bereits aus betriebswirtschaftlichen Gesichtspunkten geeignete technische und organisatorische Maßnahmen zum Schutz ihrer Daten. Die Verordnung verpflichtet im Hinblick auf die Verarbeitung von personenbezogenen Daten hierzu (Artikel 32). Welche Maßnahmen geeignet sind, richtet sich nach dem Stand der Technik, den Implementierungskosten und den konkreten Risiken. Im Ergebnis soll ein angemessenes Schutzniveau sichergestellt werden. Im Rahmen der Kontrolle der Einhaltung der Qualitäts- und Leistungsstandards des DDV werden diese Maßnahmen geprüft.

5.4 DATENSCHUTZRECHTLICHE FOLGENABSCHÄTZUNG

Die Verordnung verpflichtet Unternehmen dazu, in bestimmten Konstellationen vor der Einführung einer Datenverarbeitung eine Datenschutz-Folgenabschätzung durchzuführen und zu dokumentieren (Artikel 35). Dies gilt für Datenverarbeitungen, die hohe Risiken für die Rechte und Freiheiten natürlicher Personen bergen. Im Bereich des Dialogmarketings liegen diese Voraussetzungen in der Regel nicht vor.

5.5 ROLLE DER AUFSICHTSBEHÖRDEN UND DES EUROPÄISCHEN DATENSCHUTZAUSSCHUSSES

Den Aufsichtsbehörden werden in der Verordnung umfassende Aufgaben (Artikel 57) zugewiesen und Befugnisse (Artikel 58) eingeräumt. Sie sollen europaweit zusammenarbeiten und ihre Positionen im Europäischen Datenschutzausschuss (Artikel 68 - früher die so genannte Artikel 29 Arbeitsgruppe) abstimmen.

Die Verordnung legt hohe Bußgeldrahmen für mögliche Datenschutzverstöße fest (Artikel 83). Die Höhe des Bußgeldrahmens unterscheidet zwischen formalen und materiellen Datenschutzverstößen. Es können Bußgelder bis zu 20 Millionen EUR verhängt werden. Wenn 4% des Weltumsatzes eines Unternehmens diesen Betrag überschreiten, dann erhöht sich der Bußgeldrahmen entsprechend.

5.6 VERBRAUCHERSCHUTZ

Betroffene Personen können sich bei der Wahrnehmung ihrer Rechte - insbesondere von Verbraucherschutzorganisationen - vertreten lassen (Artikel 80 (1)). Den Mitgliedstaaten wird zusätzlich die Möglichkeit der Schaffung eines Verbandsklagerechts gegeben (Artikel 80 (2)). Unabhängig davon bleibt es bei den Verbandsklagerechten aufgrund anderer Vorschrift (beispielsweise in Bezug auf Allgemeine Geschäftsbedingungen). Verbraucherschutzorganisationen sind dabei nicht an die Rechtsmeinung der Aufsichtsbehörden gebunden.

5.7 ZERTIFIZIERUNG

Die Verordnung eröffnet die Möglichkeit zur Schaffung von Verhaltensregeln und Einführung von Zertifizierungsverfahren (Artikel 40 bis 43). Diese unterliegen jedoch sehr detaillierten formalen und prozessualen Anforderungen. Ob sie sich in der Praxis in dieser Form durchsetzen werden, bleibt abzuwarten.

Der DDV hat bereits im Jahr 1992 Qualitäts- und Leistungsstandards für Adressdienstleister erarbeitet und ständig weiterentwickelt. DDV-Mitglieder, die sich über die Verbandsmitgliedschaft hinaus den Vorschriften der Qualitäts- und Leistungsstandards und den damit verbundenen regelmäßigen unabhängigen Kontrollen unterwerfen, führen bereits jetzt ein freiwilliges Datenschutzaudit mit strengen Auditierungskriterien durch. Nur diese Unternehmen sind berechtigt, das Qualitätssiegel mit den Piktogrammen für die jeweils geprüften Bereiche zu führen.

6. GRENZÜBERSCHREITENDE VERARBEITUNG ANGEMESSEN ABSICHERN

6.1 SCHUTZ GILT FÜR JEDERMANN

Die Verordnung schützt personenbezogene Daten und zwar unabhängig von der Nationalität oder dem Wohnsitz der betroffenen Person. Es gibt mehrere Anknüpfungspunkte für die räumliche Anwendung der Verordnung. Wenn die Datenverarbeitung im Rahmen der Tätigkeit einer Niederlassung eines Unternehmens oder eines Auftragsverarbeiters in der Europäischen Union erfolgt, unterliegt sie der Verordnung. Selbst wenn diese Voraussetzungen nicht erfüllt sind, kann die Verordnung Anwendung finden. Dies gilt, wenn ein Unternehmen Personen in der Europäischen Union Waren oder Dienstleistungen anbietet (auch wenn diese vergütungsfrei sind). Außerdem greift die Verordnung, wenn ein Unternehmen das Verhalten betroffener Personen in der Europäischen Union beobachtet.

Wenn also beispielsweise in Deutschland Daten eines US-Amerikaners erhoben, verarbeitet oder genutzt werden, dann greift die Verordnung, auch wenn die betroffene Person noch nie in ihrem Leben in Deutschland gewesen ist. Wenn in diesem Beispiel die Adresse des US-Amerikaners von einem deutschen Unternehmen gekauft wird und das Unternehmen ihm von Deutschland aus einen Katalog schickt, müssen die Anforderungen der Verordnung eingehalten werden.

6.2 FREIHEITEN INNERHALB DER EUROPÄISCHEN UNION

Die Verordnung verbietet datenschutzrechtliche Beschränkungen für den freien Verkehr personenbezogener Daten zwischen den Mitgliedstaaten. Dies gilt für die gesamte Europäische Union und wird vermutlich von den zusätzlichen Ländern im Europäischen Wirtschaftsraum (Norwegen, Island und Liechtenstein - nicht aber der Schweiz) übernommen.

Grenzenlos ist die Freiheit innerhalb des Europäischen Wirtschaftsraums damit nicht. Die Anforderungen der Verordnung müssen eingehalten werden. Es ist aber unerheblich, ob Daten von München nach Hamburg oder von München nach Paris übermittelt werden. In beiden Fällen muss auf gleiche Weise geprüft werden, ob die Verordnung die Übermittlung erlaubt.

Zu beachten ist jedoch, dass die Regeln der Verordnung durch nationale Umsetzungsvorschriften der ePrivacy Richtlinie ergänzt werden. Diese soll noch überarbeitet werden. Solange dies nicht erfolgt ist, gelten die entsprechenden nationalen Regeln weiter. Auswirkungen hat dies vor allem auf elektronische Werbung, denn die ist weitgehend nur mit Einwilligung der Adressaten zulässig.

6.3 GRENZEN DER EUROPÄISCHEN UNION

Die Freizügigkeit innerhalb des Europäischen Wirtschaftsraums rechtfertigt sich damit, dass in allen Mitgliedstaaten das Schutzniveau der Verordnung gilt. Außerhalb der Europäischen Union gilt dies nicht. Hier gibt es nur wenige Länder, die vergleichbar strenge Datenschutzgesetze haben.

Die Verordnung stellt wegen des unterschiedlichen Schutzniveaus außerhalb der Europäischen Union besondere Anforderungen an Datenübermittlungen in so genannte Drittländer. Die besonderen Anforderungen gelten, wenn das Schutzniveau im Empfängerland nicht angemessen ist. Wenn ein angemessenes Datenschutzniveau vorhanden ist, müssen für die Übermittlung nur die Anforderungen eingehalten werden, die auch für Länder innerhalb der Europäischen Union gelten. Voraussetzung hierfür ist aber, dass die Europäische Kommission die Angemessenheit in einem Beschluss anerkennt.

Wenn im Drittland kein angemessenes Datenschutzniveau besteht, sind die besonderen Einschränkungen für Drittlandübermittlungen zu beachten. Das gilt auch für die Weitergabe von Daten an Auftragsverarbeiter.

Wichtig ist, dass die besonderen Anforderungen für die Übermittlung in Drittländer zusätzlich zu den allgemeinen Anforderungen gelten. Wenn also beispielsweise Adressdaten mit Merkmalen übermittelt werden sollen, dann muss auf der ersten Stufe geprüft werden, ob dies innerhalb der Europäischen Union zulässig wäre. In der zweiten Stufe ist dann zu prüfen, ob besondere Beschränkungen für die Übermittlung in Länder außerhalb der Europäischen Union greifen.

Die Europäische Kommission hat das Datenschutzniveau in einer Reihe von Ländern geprüft. In Andorra, Argentinien, Kanada (für kommerzielle Organisationen), Israel, Neuseeland, Uruguay und der Schweiz sowie auf den britischen Kanalinseln Guernsey und Jersey, der Insel Man und den dänischen Färöer-Inseln hat die Europäische Kommission (teilweise mit Einschränkungen) ein angemessenes Datenschutzniveau festgestellt. Für die Vereinigten Staaten gilt dies auch, wenn die empfangenden Unternehmen sich auf den EU-US Privacy Shield verpflichtet haben.

Die Feststellungen der Europäischen Kommission unter der Verordnung sind abschließend und die bestehenden Beschlüsse gelten unter der Verordnung fort. Ein angemessenes Schutzniveau kann zwar auch in Ländern bestehen, zu denen noch keine offizielle Feststellung der Europäischen Kommission getroffen wurde. Darauf kann man sich jedoch nicht berufen.

6.3.1 Die Bedeutung von Binding Corporate Rules

Ein Instrument zur Sicherstellung eines angemessenen Datenschutzniveaus kann in der Einführung von bindenden Unternehmensregeln liegen. Diese müssen von den zuständigen Datenschutzaufsichtsbehörden genehmigt werden. Da das Genehmigungsverfahren langwierig ist, gibt es bisher nur wenige Unternehmen mit genehmigten Binding

Corporate Rules. In der Praxis haben sie bisher nur untergeordnete Bedeutung. Es zeigt sich aber, dass immer mehr Unternehmen die Einführung von Binding Corporate Rules in Angriff nehmen, so dass das Modell an Bedeutung gewinnt.

6.3.2 Schutz durch Standardvertragsklauseln

Wenn ein Land außerhalb der Europäischen Union kein angemessenes Datenschutzniveau für eine Datenübermittlung sicherstellt, dann kann das übermittelnde Unternehmen mit dem empfangenden Unternehmen so genannte Standardvertragsklauseln abschließen. Hierfür hat die Europäische Kommission Musterverträge beschlossen, die sie veröffentlicht hat: http://ec.europa.eu/justice/data-protection/index_de.htm.

Es gibt zwei Typen von Standardvertragsklauseln. Der erste Typ gilt für die Übermittlung von Daten zu einem anderen Unternehmen (2001/497/EC und alternativ C(2004)5271) und der zweite Typ für die Beauftragung von so genannten Auftragsverarbeitern (neue Fassung C(2010) 593). In der Praxis sind die Standardvertragsklauseln das am häufigsten verwendete Instrument, um Datenübermittlungen in Drittländer zu ermöglichen. Sie sind besonders bei der Einbindung von Auftragsverarbeitern in Drittländern geeignet.

Die Standardvertragsklauseln dürfen nur mit Zustimmung der zuständigen Datenschutzaufsichtsbehörde inhaltlich verändert werden. Deshalb werden sie in der Praxis nicht geändert und wie Formulare ausgefüllt. Die Standardvertragsklauseln gelten dann ergänzend zu den kommerziellen vertraglichen Regelungen, die im Zusammenhang mit der Übermittlung geschlossen werden.

6.3.3 Wirksame Einwilligung in die Übermittlung

Die Übermittlung in Drittländer kann auch durch eine ausdrückliche Einwilligung der jeweils betroffenen Personen erlaubt werden. In der Praxis fehlt es aber häufig an einer realistischen Möglichkeit, eine solche Einwilligung einzuholen. Wenn eine betroffene Person die Übermittlung in Drittländer erlauben soll, dann muss dies auch klar aus der Einwilligung hervorgehen. Außerdem muss im Einwilligungstext vor einem gegebenenfalls nicht angemessenen Datenschutzniveau im Empfängerland gewarnt werden. Nicht zuletzt gelten die allgemeinen Hindernisse für die Einholung einer wirksamen Einwilligung (siehe Ziffer 2.1 Alternative 2 des Best Practice Guides).

6.4 DIE SONDERSTELLUNG VON DIENSTLEISTERN

In der Verordnung existieren Sonderregelungen für Dienstleister, die weisungsgebunden tätig sind. Sie sind unter bestimmten Voraussetzungen so genannte Auftragsverarbeiter (siehe Ziffer 4 des Best Practice Guides).

Der Vorteil der Auftragsverarbeitung liegt darin, dass der Auftraggeber für die Datenverarbeitung der so genannte „Verantwortliche“ bleibt und der Auftragnehmer nicht als „Dritter“ angesehen wird.

Die Konstruktion der Auftragsverarbeitung wird im so genannten Lettershop-Verfahren verwendet, so dass es datenschutzrechtlich zu keiner Übermittlung der Adressen vom Listeigener an den Werbetreibenden kommt. Der Lettershop wird hierbei als Auftragsverarbeiter für den Adresseigner tätig. Auf diese Weise bleibt der Adresseigner „Herr der Daten“ und damit Verantwortlicher im Sinne der Verordnung.

Die Vorteile einer Auftragsverarbeitung gelten unabhängig davon, ob der Auftragsverarbeiter in Deutschland oder in einem anderen Land des Europäischen Wirtschaftsraums sitzt. Es macht deshalb keinen Unterschied, ob ein deutscher Werbetreibender für ein Mailing an seine Kunden einen Lettershop in Frankfurt oder Warschau beauftragt.

7. BEGRIFFLICHKEITEN RICHTIG VERSTEHEN

Adressdaten:
Die Daten, unter denen eine Person postalisch, elektronisch oder telefonisch erreicht werden kann.

Adresseigner (= Listeigner)
Ein Unternehmen, dem Adressdaten als Verantwortlichem gehören und der diese für Werbung Dritter zur Verfügung stellt.

Auftragsverarbeiter:
Ein Dienstleister, der personenbezogene Daten auf Weisung des Verantwortlichen verarbeitet. Die Zwecke und Mittel der Verarbeitung sind vom Verantwortlichen zu bestimmen.

Betroffene Person:
Die natürliche Person, deren personenbezogene Daten verarbeitet werden.

Empfehlungswerbung:
Eine Werbung, die ein Verantwortlicher versendet oder versenden lässt und in der für die Produkte eines Dritten geworben wird.

Lettershop:
Ein Dienstleister, der Leistungen wie die Produktion, Konfektionierung und Versendung von Werbung oder anderer Korrespondenz an einen Adressatenkreis im Auftrag durchführt.

Öffentlich zugängliche Quellen:
Jedermann zugängliche Quellen wie allgemein zugängliche Seiten im Internet oder Adress-, Rufnummern-, Branchen- oder vergleichbare Verzeichnisse.

Personenbezogene Daten:
Informationen über eine identifizierte oder identifizierbare natürliche Person (inklusive identifizierbare pseudonymisierte Daten). Nicht aber Daten, die sich allein auf eine juristische Person beziehen.

Selektionskriterien:
Daten, mit denen ausgewählt wird, welche Adressaten aus einer Adressliste für Werbezwecke sinvoller Weise angesprochen werden.

Verantwortlicher:
Jede natürliche oder juristische Person, die gemeinsam oder mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet, wie beispielsweise Listeigner, nicht aber Auftragsverarbeiter.

8. AUSSCHNITTE AUS DER DATENSCHUTZ-GRUNDVERORDNUNG

ERWÄGUNGSGRUND 4

Die Verarbeitung personenbezogener Daten sollte im Dienste der Menschheit stehen. Das Recht auf Schutz der personenbezogenen Daten ist kein uneingeschränktes Recht; es muss im Hinblick auf seine gesellschaftliche Funktion gesehen und unter Wahrung des Verhältnismäßigkeitsprinzips gegen andere Grundrechte abgewogen werden. Diese Verordnung steht im Einklang mit allen Grundrechten und achtet alle Freiheiten und Grundsätze, die mit der Charta anerkannt wurden und in den Europäischen Verträgen verankert sind, insbesondere Achtung des Privat- und Familienlebens, der Wohnung und der Kommunikation, Schutz personenbezogener Daten, Gedanken-, Gewissens- und Religionsfreiheit, Freiheit der Meinungsäußerung und Informationsfreiheit, unternehmerische Freiheit, Recht auf einen wirksamen Rechtsbehelf und ein faires Verfahren und Vielfalt der Kulturen, Religionen und Sprachen.

ERWÄGUNGSGRUND 14

Der durch diese Verordnung gewährte Schutz sollte für die Verarbeitung der personenbezogenen Daten natürlicher Personen ungeachtet ihrer Staatsangehörigkeit oder ihres Aufenthaltsorts gelten. Diese Verordnung gilt nicht für die Verarbeitung personenbezogener Daten juristischer Personen und insbesondere als juristische Person gegründeter Unternehmen, einschließlich Name, Rechtsform oder Kontaktdaten der juristischen Person.

ERWÄGUNGSGRUND 26

Die Grundsätze des Datenschutzes sollten für alle Informationen gelten, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Einer Pseudonymisierung unterzogene personenbezogene Daten, die durch Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden könnten, sollten als Informationen über eine identifizierbare natürliche Person betrachtet werden. Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren, wie beispielsweise das Aussondern. Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind. Die Grundsätze des Datenschutzes sollten daher nicht für anonyme Informationen gelten, d.h. für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann. Diese Verordnung betrifft somit nicht die Verarbeitung solcher anonymer Daten, auch für statistische oder für Forschungszwecke.

ERWÄGUNGSGRUND 30

Natürlichen Personen werden unter Umständen Online-Kennungen wie IP-Adressen und Cookie-Kennungen, die sein Gerät oder Software-Anwendungen und -Tools oder Protokolle liefern, oder sonstige Kennungen wie Funkfrequenzkennzeichnungen zugeordnet. Dies kann Spuren hinterlassen, die insbesondere in Kombination mit eindeutigen Kennungen und anderen beim Server eingehenden Informationen dazu benutzt werden können, um Profile der natürlichen Personen zu erstellen und sie zu identifizieren.

ERWÄGUNGSGRUND 32

Die Einwilligung sollte durch eine eindeutige bestätigende Handlung erfolgen, mit der freiwillig, für den konkreten Fall, in informierter Weise und unmissverständlich bekundet wird, dass die betroffene Person mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist, etwa in Form einer schriftlichen Erklärung, die auch elektronisch erfolgen kann, oder einer mündlichen Erklärung. Dies könnte etwa durch Anklicken eines Kästchens beim Besuch einer Internetseite, durch die Auswahl technischer Einstellungen für Dienste der Informationsgesellschaft oder durch eine andere Erklärung oder Verhaltensweise geschehen, mit der die betroffene Person in dem jeweiligen Kontext eindeutig ihr Einverständnis mit der beabsichtigten Verarbeitung ihrer personenbezogenen Daten signalisiert. Stillschweigen, bereits angekreuzte Kästchen oder Untätigkeit der betroffenen Person sollten daher keine Einwilligung darstellen. Die Einwilligung sollte sich auf alle zu demselben Zweck oder denselben Zwecken vorgenommenen Verarbeitungsvorgänge beziehen. Wenn die Verarbeitung mehreren Zwecken dient, sollte für alle diese Verarbeitungszwecke eine Einwilligung gegeben werden. Wird die betroffene Person auf elektronischem Weg zur Einwilligung aufgefordert, so muss die Aufforderung in klarer und knapper Form und ohne unnötige Unterbrechung des Dienstes, für den die Einwilligung gegeben wird, erfolgen.

ERWÄGUNGSGRUND 42

Erfolgt die Verarbeitung mit Einwilligung der betroffenen Person, sollte der Verantwortliche nachweisen können, dass die betroffene Person ihre Einwilligung zu dem Verarbeitungsvorgang gegeben hat. Insbesondere bei Abgabe einer schriftlichen Erklärung in anderer Sache sollten Garantien sicherstellen, dass die betroffene Person weiß, dass und in welchem Umfang sie ihre Einwilligung erteilt. Gemäß der Richtlinie 93/13/EWG des Rates (10) sollte eine vom Verantwortlichen vorformulierte Einwilligungserklärung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zur Verfügung gestellt werden, und sie sollte keine missbräuchlichen Klauseln beinhalten. Damit sie in Kenntnis der Sachlage ihre Einwilligung geben kann, sollte die betroffene Person mindestens wissen, wer der Verantwortliche ist und für welche Zwecke ihre personenbezogenen Daten verarbeitet werden sollen. Es sollte nur

dann davon ausgegangen werden, dass sie ihre Einwilligung freiwillig gegeben hat, wenn sie eine echte oder freie Wahl hat und somit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden.ziehen, ohne Nachteile zu erleiden.

ERWÄGUNGSGRUND 43

Um sicherzustellen, dass die Einwilligung freiwillig erfolgt ist, sollte diese in besonderen Fällen, wenn zwischen der betroffenen Person und dem Verantwortlichen ein klares Ungleichgewicht besteht, insbesondere wenn es sich bei dem Verantwortlichen um eine Behörde handelt, und es deshalb in Anbetracht aller Umstände in dem speziellen Fall unwahrscheinlich ist, dass die Einwilligung freiwillig gegeben wurde, keine gültige Rechtsgrundlage liefern. Die Einwilligung gilt nicht als freiwillig erteilt, wenn zu verschiedenen Verarbeitungsvorgängen von personenbezogenen Daten nicht gesondert eine Einwilligung erteilt werden kann, obwohl dies im Einzelfall angebracht ist, oder wenn die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung abhängig ist, obwohl diese Einwilligung für die Erfüllung nicht erforderlich ist.

ERWÄGUNGSGRUND 47

Die Rechtmäßigkeit der Verarbeitung kann durch die berechtigten Interessen eines Verantwortlichen, auch eines Verantwortlichen, dem die personenbezogenen Daten offengelegt werden dürfen, oder eines Dritten begründet sein, sofern die Interessen oder die Grundrechte und Grundfreiheiten der betroffenen Person nicht überwiegen; dabei sind die vernünftigen Erwartungen der betroffenen Person, die auf ihrer Beziehung zu dem Verantwortlichen beruhen, zu berücksichtigen. Ein berechtigtes Interesse könnte beispielsweise vorliegen, wenn eine maßgebliche und angemessene Beziehung zwischen der betroffenen Person und dem Verantwortlichen besteht, z. B. wenn die betroffene Person ein Kunde des Verantwortlichen ist oder in seinen Diensten steht. Auf jeden Fall wäre das Bestehen eines berechtigten Interesses besonders sorgfältig abzuwägen, wobei auch zu prüfen ist, ob eine betroffene Person zum Zeitpunkt der Erhebung der personenbezogenen Daten und angesichts der Umstände, unter denen sie erfolgt, vernünftigerweise absehen kann, dass möglicherweise eine Verarbeitung für diesen Zweck erfolgen wird. Insbesondere dann, wenn personenbezogene Daten in Situationen verarbeitet werden, in denen eine betroffene Person vernünftigerweise nicht mit einer weiteren Verarbeitung rechnen muss, könnten die Interessen und Grundrechte der betroffenen Person das Interesse des Verantwortlichen überwiegen. Da es dem Gesetzgeber obliegt, per Rechtsvorschrift die Rechtsgrundlage für die Verarbeitung personenbezogener Daten durch die Behörden zu schaffen, sollte diese Rechtsgrundlage nicht für Verarbeitungen durch Behörden gelten, die diese in Erfüllung ihrer Aufgaben vornehmen. Die Verarbeitung personenbezogener Daten im für die Verhinderung von Betrug unbedingt erforderlichen Umfang stellt ebenfalls ein berechtigtes Interesse des jeweiligen Verantwortlichen dar. Die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung kann als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden.

ERWÄGUNGSGRUND 50

Die Verarbeitung personenbezogener Daten für andere Zwecke als die, für die die personenbezogenen Daten ursprünglich erhoben wurden, sollte nur zulässig sein, wenn die Verarbeitung mit den Zwecken, für die die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist. In diesem Fall ist keine andere gesonderte Rechtsgrundlage erforderlich als diejenige für die Erhebung der personenbezogenen Daten. Ist die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde, so können im Unionsrecht oder im Recht der Mitgliedstaaten die Aufgaben und Zwecke bestimmt und konkretisiert werden, für die eine Weiterverarbeitung als vereinbar und rechtmäßig erachtet wird. Die Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke sollte als vereinbarer und rechtmäßiger Verarbeitungsvorgang gelten. Die im Unionsrecht oder im Recht der Mitgliedstaaten vorgesehene Rechtsgrundlage für die Verarbeitung personenbezogener Daten kann auch als Rechtsgrundlage für eine Weiterverarbeitung dienen. Um festzustellen, ob ein Zweck der Weiterverarbeitung mit dem Zweck, für den die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist, sollte der Verantwortliche nach Einhaltung aller Anforderungen für die Rechtmäßigkeit der ursprünglichen Verarbeitung unter anderem prüfen, ob ein Zusammenhang zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung besteht, in welchem Kontext die Daten erhoben wurden, insbesondere die vernünftigen Erwartungen der betroffenen Person, die auf ihrer Beziehung zu dem Verantwortlichen beruhen, in Bezug auf die weitere Verwendung dieser Daten, um welche Art von personenbezogenen Daten es sich handelt, welche Folgen die beabsichtigte Weiterverarbeitung für die betroffenen Personen hat und ob sowohl beim ursprünglichen als auch beim beabsichtigten Weiterverarbeitungsvorgang geeignete Garantien bestehen.

Hat die betroffene Person ihre Einwilligung erteilt oder beruht die Verarbeitung auf Unionsrecht oder dem Recht der Mitgliedstaaten, was in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zum Schutz insbesondere wichtiger Ziele des allgemeinen öffentlichen Interesses darstellt, so sollte der Verantwortliche die personenbezogenen Daten ungeachtet der Vereinbarkeit der Zwecke weiterverarbeiten dürfen. In jedem Fall sollte gewährleistet sein, dass die in dieser Verordnung niedergelegten Grundsätze angewandt werden und insbesondere die betroffene Person über diese anderen Zwecke und über ihre Rechte einschließlich des Widerspruchsrechts unterrichtet wird.

Der Hinweis des Verantwortlichen auf mögliche Straftaten oder Bedrohungen der öffentlichen Sicherheit und die Übermittlung der maßgeblichen personenbezogenen Daten in Einzelfällen oder in mehreren Fällen, die im Zusammenhang mit derselben Straftat oder derselben Bedrohung der öffentlichen Sicherheit stehen, an eine zuständige Behörde sollten als berechtigtes Interesse des Verantwortlichen gelten. Eine derartige Übermittlung personenbezogener Daten im berechtigten Interesse des Verantwortlichen oder deren Weiterverarbeitung sollte jedoch unzulässig sein, wenn die Verarbeitung mit einer rechtlichen, beruflichen oder sonstigen verbindlichen Pflicht zur Geheimhaltung unvereinbar ist.

ERWÄGUNGSGRUND 57

Kann der Verantwortliche anhand der von ihm verarbeiteten personenbezogenen Daten eine natürliche Person nicht identifizieren, so sollte er nicht verpflichtet sein, zur bloßen Einhaltung einer Vorschrift dieser Verordnung zusätzliche Daten einzuholen, um die betroffene Person zu identifizieren. Allerdings sollte er sich nicht weigern, zusätzliche Informationen entgegenzunehmen, die von der betroffenen Person beigebracht werden, um ihre Rechte geltend zu machen. Die Identifizierung sollte die digitale Identifizierung einer betroffenen Person – beispielsweise durch Authentifizierungsverfahren etwa mit denselben Berechtigungsnachweisen, wie sie die betroffene Person verwendet, um sich bei dem von dem Verantwortlichen bereitgestellten Online-Dienst anzumelden – einschließen.

ERWÄGUNGSGRUND 58

Der Grundsatz der Transparenz setzt voraus, dass eine für die Öffentlichkeit oder die betroffene Person bestimmte Information präzise, leicht zugänglich und verständlich sowie in klarer und einfacher Sprache abgefasst ist und gegebenenfalls zusätzlich visuelle Elemente verwendet werden. Diese Information könnte in elektronischer Form bereitgestellt werden, beispielsweise auf einer Website, wenn sie für die Öffentlichkeit bestimmt ist. Dies gilt insbesondere für Situationen, wo die große Zahl der Beteiligten und die Komplexität der dazu benötigten Technik es der betroffenen Person schwer machen, zu erkennen und nachzuvollziehen, ob, von wem und zu welchem Zweck sie betreffende personenbezogene Daten erfasst werden, wie etwa bei der Werbung im Internet. Wenn sich die Verarbeitung an Kinder richtet, sollten aufgrund der besonderen Schutzwürdigkeit von Kindern Informationen und Hinweise in einer dergestalt klaren und einfachen Sprache erfolgen, dass ein Kind sie verstehen kann.

ARTIKEL 4 Begriffsbestimmungen

Im Sinne dieser Verordnung bezeichnet der Ausdruck:

1. „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann;
2. „Verarbeitung“ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung; […]
4. „Profiling“ jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen;
5. „Pseudonymisierung“ die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden; […]
10. „Dritter“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten;
11. „Einwilligung“ der betroffenen Person jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie

mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist; […]

ARTIKEL 5 Grundsätze für die Verarbeitung personenbezogener Daten

(1) Personenbezogene Daten müssen
a) auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“);
b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken („Zweckbindung“);
c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);
d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit“);
e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden („Speicherbegrenzung“);
f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“);

(2) Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“).

ARTIKEL 6 Rechtmäßigkeit der Verarbeitung

(1) Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:
a) Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;
b) die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;
c) die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;
d) die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;
e) die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;
f) die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Unterabsatz 1 Buchstabe f gilt nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung.

(2) Die Mitgliedstaaten können spezifischere Bestimmungen zur Anpassung der Anwendung der Vorschriften dieser Verordnung in Bezug auf die Verarbeitung zur Erfüllung von Absatz 1 Buchstaben c und e beibehalten oder einführen, indem sie spezifische Anforderungen für die Verarbeitung sowie sonstige Maßnahmen präziser bestimmen, um eine rechtmäßig und nach Treu und Glauben erfolgende Verarbeitung zu gewährleisten, einschließlich für andere besondere Verarbeitungssituationen gemäß Kapitel IX.

(3) Die Rechtsgrundlage für die Verarbeitungen gemäß Absatz 1 Buchstaben c und e wird festgelegt durch
a) Unionsrecht oder
b) das Recht der Mitgliedstaaten, dem der Verantwortliche unterliegt.

Der Zweck der Verarbeitung muss in dieser Rechtsgrundlage festgelegt oder hinsichtlich der Verarbeitung gemäß Absatz 1 Buchstabe e für die Erfüllung einer Aufgabe erforderlich sein, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Diese Rechtsgrundlage kann spezifische Bestimmungen zur Anpassung der Anwendung der Vorschriften dieser Verordnung enthalten, unter anderem Bestimmungen darüber, welche allgemeinen Bedingungen für die Regelung der Rechtmäßigkeit der Verarbeitung durch

den Verantwortlichen gelten, welche Arten von Daten verarbeitet werden, welche Personen betroffen sind, an welche Einrichtungen und für welche Zwecke die personenbezogenen Daten offengelegt werden dürfen, welcher Zweckbindung sie unterliegen, wie lange sie gespeichert werden dürfen und welche Verarbeitungsvorgänge und -verfahren angewandt werden dürfen, einschließlich Maßnahmen zur Gewährleistung einer rechtmäßig und nach Treu und Glauben erfolgenden Verarbeitung, wie solche für sonstige besondere Verarbeitungssituationen gemäß Kapitel IX. Das Unionsrecht oder das Recht der Mitgliedstaaten müssen ein im öffentlichen Interesse liegendes Ziel verfolgen und in einem angemessenen Verhältnis zu dem verfolgten legitimen Zweck stehen.

(4) Beruht die Verarbeitung zu einem anderen Zweck als zu demjenigen, zu dem die personenbezogenen Daten erhoben wurden, nicht auf der Einwilligung der betroffenen Person oder auf einer Rechtsvorschrift der Union oder der Mitgliedstaaten, die in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zum Schutz der in Artikel 23 Absatz 1 genannten Ziele darstellt, so berücksichtigt der Verantwortliche – um festzustellen, ob die Verarbeitung zu einem anderen Zweck mit demjenigen, zu dem die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist – unter anderem

a) jede Verbindung zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung,
b) den Zusammenhang, in dem die personenbezogenen Daten erhoben wurden, insbesondere hinsichtlich des Verhältnisses zwischen den betroffenen Personen und dem Verantwortlichen,
c) die Art der personenbezogenen Daten, insbesondere ob besondere Kategorien personenbezogener Daten gemäß Artikel 9 verarbeitet werden oder ob personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 verarbeitet werden,
d) die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen,
e) das Vorhandensein geeigneter Garantien, wozu Verschlüsselung oder Pseudonymisierung gehören kann.

ARTIKEL 7 Bedingungen für die Einwilligung

(1) Beruht die Verarbeitung auf einer Einwilligung, muss der Verantwortliche nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat.

(2) Erfolgt die Einwilligung der betroffenen Person durch eine schriftliche Erklärung, die noch andere Sachverhalte betrifft, so muss das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen, dass es von den anderen Sachverhalten klar zu unterscheiden ist. Teile der Erklärung sind dann nicht verbindlich, wenn sie einen Verstoß gegen diese Verordnung darstellen.

(3) Die betroffene Person hat das Recht, ihre Einwilligung jederzeit zu widerrufen. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. Die betroffene Person wird vor Abgabe der Einwilligung hiervon in Kenntnis gesetzt. Der Widerruf der Einwilligung muss so einfach wie die Erteilung der Einwilligung sein.

(4) Bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, muss dem Umstand in größtmöglichem Umfang Rechnung getragen werden, ob unter anderem die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich sind.

ARTIKEL 8 Bedingungen für die Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft

(1) Gilt Artikel 6 Absatz 1 Buchstabe a bei einem Angebot von Diensten der Informationsgesellschaft, das einem Kind direkt gemacht wird, so ist die Verarbeitung der personenbezogenen Daten des Kindes rechtmäßig, wenn das Kind das sechzehnte Lebensjahr vollendet hat. Hat das Kind noch nicht das sechzehnte Lebensjahr vollendet, so ist diese Verarbeitung nur rechtmäßig, sofern und soweit diese Einwilligung durch den Träger der elterlichen Verantwortung für das Kind oder mit dessen Zustimmung erteilt wird.
Die Mitgliedstaaten können durch Rechtsvorschriften zu diesen Zwecken eine niedrigere Altersgrenze vorsehen, die jedoch nicht unter dem vollendeten dreizehnten Lebensjahr liegen darf.

(2) Der Verantwortliche unternimmt unter Berücksichtigung der verfügbaren Technik angemessene Anstrengungen, um sich in solchen Fällen zu vergewissern, dass die Einwilligung durch den Träger der elterlichen Verantwortung für das Kind oder mit dessen Zustimmung erteilt wurde.

(3) Absatz 1 lässt das allgemeine Vertragsrecht der Mitgliedstaaten, wie etwa die Vorschriften zur Gültigkeit, zum Zustandekommen oder zu den Rechtsfolgen eines Vertrags in Bezug auf ein Kind, unberührt.

ARTIKEL 9 Verarbeitung besonderer Kategorien personenbezogener Daten

(1) Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten,

biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person ist untersagt.

(2) Absatz 1 gilt nicht in folgenden Fällen:

a) Die betroffene Person hat in die Verarbeitung der genannten personenbezogenen Daten für einen oder mehrere festgelegte Zwecke ausdrücklich eingewilligt, es sei denn, nach Unionsrecht oder dem Recht der Mitgliedstaaten kann das Verbot nach Absatz 1 durch die Einwilligung der betroffenen Person nicht aufgehoben werden,

b) die Verarbeitung ist erforderlich, damit der Verantwortliche oder die betroffene Person die ihm bzw. ihr aus dem Arbeitsrecht und dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte ausüben und seinen bzw. ihren diesbezüglichen Pflichten nachkommen kann, soweit dies nach Unionsrecht oder dem Recht der Mitgliedstaaten oder einer Kollektivvereinbarung nach dem Recht der Mitgliedstaaten, das geeignete Garantien für die Grundrechte und die Interessen der betroffenen Person vorsieht, zulässig ist,

c) die Verarbeitung ist zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich und die betroffene Person ist aus körperlichen oder rechtlichen Gründen außerstande, ihre Einwilligung zu geben,

d) die Verarbeitung erfolgt auf der Grundlage geeigneter Garantien durch eine politisch, weltanschaulich, religiös oder gewerkschaftlich ausgerichtete Stiftung, Vereinigung oder sonstige Organisation ohne Gewinnerzielungsabsicht im Rahmen ihrer rechtmäßigen Tätigkeiten und unter der Voraussetzung, dass sich die Verarbeitung ausschließlich auf die Mitglieder oder ehemalige Mitglieder der Organisation oder auf Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßige Kontakte mit ihr unterhalten, bezieht und die personenbezogenen Daten nicht ohne Einwilligung der betroffenen Personen nach außen offengelegt werden,

e) die Verarbeitung bezieht sich auf personenbezogene Daten, die die betroffene Person offensichtlich öffentlich gemacht hat,

f) die Verarbeitung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder bei Handlungen der Gerichte im Rahmen ihrer justiziellen Tätigkeit erforderlich,

g) die Verarbeitung ist auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht, aus Gründen eines erheblichen öffentlichen Interesses erforderlich,

h) die Verarbeitung ist für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats oder aufgrund eines Vertrags mit einem Angehörigen eines Gesundheitsberufs und vorbehaltlich der in Absatz 3 genannten Bedingungen und Garantien erforderlich,

i) die Verarbeitung ist aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie dem Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren oder zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten, auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person, insbesondere des Berufsgeheimnisses, vorsieht, erforderlich, oder

j) die Verarbeitung ist auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht, für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 erforderlich.

(3) Die in Absatz 1 genannten personenbezogenen Daten dürfen zu den in Absatz 2 Buchstabe h genannten Zwecken verarbeitet werden, wenn diese Daten von Fachpersonal oder unter dessen Verantwortung verarbeitet werden und dieses Fachpersonal nach dem Unionsrecht oder dem Recht eines Mitgliedstaats oder den Vorschriften nationaler zuständiger Stellen dem Berufsgeheimnis unterliegt, oder wenn die Verarbeitung durch eine andere Person erfolgt, die ebenfalls nach dem Unionsrecht oder dem Recht eines Mitgliedstaats oder den Vorschriften nationaler zuständiger Stellen einer Geheimhaltungspflicht unterliegt.

(4) Die Mitgliedstaaten können zusätzliche Bedingungen, einschließlich Beschränkungen, einführen oder aufrechterhalten, soweit die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten betroffen ist.

ARTIKEL 10 Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten

Die Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln aufgrund von Artikel 6 Absatz 1 darf nur unter behördlicher Aufsicht vorgenommen werden oder wenn dies nach dem Uni-

onsrecht oder dem Recht der Mitgliedstaaten, das geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen vorsieht, zulässig ist. Ein umfassendes Register der strafrechtlichen Verurteilungen darf nur unter behördlicher Aufsicht geführt werden.

ARTIKEL 13 Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person

(1) Werden personenbezogene Daten bei der betroffenen Person erhoben, so teilt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten Folgendes mit:

a) den Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters;
b) gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten;
c) die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung;
d) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden;
e) gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten und
f) gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln, sowie das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Kommission oder im Falle von Übermittlungen gemäß Artikel 46 oder Artikel 47 oder Artikel 49 Absatz 1 Unterabsatz 2 einen Verweis auf die geeigneten oder angemessenen Garantien und die Möglichkeit, wie eine Kopie von ihnen zu erhalten ist, oder wo sie verfügbar sind.

(2) Zusätzlich zu den Informationen gemäß Absatz 1 stellt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten folgende weitere Informationen zur Verfügung, die notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten:

a) die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
b) das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit;
c) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a beruht, das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird;
d) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
e) ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche mögliche Folgen die Nichtbereitstellung hätte und
f) das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

(3) Beabsichtigt der Verantwortliche, die personenbezogenen Daten für einen anderen Zweck weiterzuverarbeiten als den, für den die personenbezogenen Daten erhoben wurden, so stellt er der betroffenen Person vor dieser Weiterverarbeitung Informationen über diesen anderen Zweck und alle anderen maßgeblichen Informationen gemäß Absatz 2 zur Verfügung.

(4) Die Absätze 1, 2 und 3 finden keine Anwendung, wenn und soweit die betroffene Person bereits über die Informationen verfügt.

ARTIKEL 14 Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden

(1) Werden personenbezogene Daten nicht bei der betroffenen Person erhoben, so teilt der Verantwortliche der betroffenen Person Folgendes mit:

a) den Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters;
b) zusätzlich die Kontaktdaten des Datenschutzbeauftragten;
c) die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung;
d) die Kategorien personenbezogener Daten, die verarbeitet werden;
e) gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten;
f) gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an einen Empfänger in einem Drittland oder einer internationalen Organisation zu übermitteln, sowie das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Kommission oder im Falle von Übermittlungen gemäß Artikel 46 oder Artikel 47 oder Artikel 49 Absatz 1 Unterabsatz 2 einen Verweis auf die geeigneten oder angemessenen Garantien und die Möglichkeit, eine Kopie von ihnen zu erhalten, oder wo sie verfügbar sind.

(2) Zusätzlich zu den Informationen gemäß Absatz 1 stellt der Verantwortliche der betroffenen Person die fol-

genden Informationen zur Verfügung, die erforderlich sind, um der betroffenen Person gegenüber eine faire und transparente Verarbeitung zu gewährleisten:

a) die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
b) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden;
c) das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung und eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit;
d) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a beruht, das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird;
e) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
f) aus welcher Quelle die personenbezogenen Daten stammen und gegebenenfalls ob sie aus öffentlich zugänglichen Quellen stammen;
g) das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

(3) Der Verantwortliche erteilt die Informationen gemäß den Absätzen 1 und 2

a) unter Berücksichtigung der spezifischen Umstände der Verarbeitung der personenbezogenen Daten innerhalb einer angemessenen Frist nach Erlangung der personenbezogenen Daten, längstens jedoch innerhalb eines Monats,
b) falls die personenbezogenen Daten zur Kommunikation mit der betroffenen Person verwendet werden sollen, spätestens zum Zeitpunkt der ersten Mitteilung an sie, oder,
c) falls die Offenlegung an einen anderen Empfänger beabsichtigt ist, spätestens zum Zeitpunkt der ersten Offenlegung.

(4) Beabsichtigt der Verantwortliche, die personenbezogenen Daten für einen anderen Zweck weiterzuverarbeiten als den, für den die personenbezogenen Daten erlangt wurden, so stellt er der betroffenen Person vor dieser Weiterverarbeitung Informationen über diesen anderen Zweck und alle anderen maßgeblichen Informationen gemäß Absatz 2 zur Verfügung.

(5) Die Absätze 1 bis 4 finden keine Anwendung, wenn und soweit

a) die betroffene Person bereits über die Informationen verfügt,
b) die Erteilung dieser Informationen sich als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde; dies gilt insbesondere für die Verarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke vorbehaltlich der in Artikel 89 Absatz 1 genannten Bedingungen und Garantien oder soweit die in Absatz 1 des vorliegenden Artikels genannte Pflicht voraussichtlich die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt In diesen Fällen ergreift der Verantwortliche geeignete Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person, einschließlich der Bereitstellung dieser Informationen für die Öffentlichkeit,
c) die Erlangung oder Offenlegung durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche unterliegt und die geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person vorsehen, ausdrücklich geregelt ist oder
d) die personenbezogenen Daten gemäß dem Unionsrecht oder dem Recht der Mitgliedstaaten dem Berufsgeheimnis, einschließlich einer satzungsmäßigen Geheimhaltungspflicht, unterliegen und daher vertraulich behandelt werden müssen.

ARTIKEL 17 Recht auf Löschung („Recht auf Vergessenwerden“)

(1) Die betroffene Person hat das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, und der Verantwortliche ist verpflichtet, personenbezogene Daten unverzüglich zu löschen, sofern einer der folgenden Gründe zutrifft:

a) Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig.
b) Die betroffene Person widerruft ihre Einwilligung, auf die sich die Verarbeitung gemäß Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a stützte, und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung.
c) Die betroffene Person legt gemäß Artikel 21 Absatz 1 Widerspruch gegen die Verarbeitung ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor, oder die betroffene Person legt gemäß Artikel 21 Absatz 2 Widerspruch gegen die Verarbeitung ein.
d) Die personenbezogenen Daten wurden unrechtmäßig verarbeitet.
e) Die Löschung der personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich, dem der Verantwortliche unterliegt.

f) Die personenbezogenen Daten wurden in Bezug auf angebotene Dienste der Informationsgesellschaft gemäß Artikel 8 Absatz 1 erhoben.

(2) Hat der Verantwortliche die personenbezogenen Daten öffentlich gemacht und ist er gemäß Absatz 1 zu deren Löschung verpflichtet, so trifft er unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten angemessene Maßnahmen, auch technischer Art, um für die Datenverarbeitung Verantwortliche, die die personenbezogenen Daten verarbeiten, darüber zu informieren, dass eine betroffene Person von ihnen die Löschung aller Links zu diesen personenbezogenen Daten oder von Kopien oder Replikationen dieser personenbezogenen Daten verlangt hat.

(3) Die Absätze 1 und 2 gelten nicht, soweit die Verarbeitung erforderlich ist

a) zur Ausübung des Rechts auf freie Meinungsäußerung und Information;
b) zur Erfüllung einer rechtlichen Verpflichtung, die die Verarbeitung nach dem Recht der Union oder der Mitgliedstaaten, dem der Verantwortliche unterliegt, erfordert, oder zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;
c) aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit gemäß Artikel 9 Absatz 2 Buchstaben h und i sowie Artikel 9 Absatz 3;
d) für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1, soweit das in Absatz 1 genannte Recht voraussichtlich die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt, oder
e) zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

ARTIKEL 21 Widerspruchsrecht

(1) Die betroffene Person hat das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten, die aufgrund von Artikel 6 Absatz 1 Buchstaben e oder f erfolgt, Widerspruch einzulegen; dies gilt auch für ein auf diese Bestimmungen gestütztes Profiling. Der Verantwortliche verarbeitet die personenbezogenen Daten nicht mehr, es sei denn, er kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

(2) Werden personenbezogene Daten verarbeitet, um Direktwerbung zu betreiben, so hat die betroffene Person das Recht, jederzeit Widerspruch gegen die Verarbeitung sie betreffender personenbezogener Daten zum Zwecke derartiger Werbung einzulegen; dies gilt auch für das Profiling, soweit es mit solcher Direktwerbung in Verbindung steht.

(3) Widerspricht die betroffene Person der Verarbeitung für Zwecke der Direktwerbung, so werden die personenbezogenen Daten nicht mehr für diese Zwecke verarbeitet.

(4) Die betroffene Person muss spätestens zum Zeitpunkt der ersten Kommunikation mit ihr ausdrücklich auf das in den Absätzen 1 und 2 genannte Recht hingewiesen werden; dieser Hinweis hat in einer verständlichen und von anderen Informationen getrennten Form zu erfolgen.

(5) Im Zusammenhang mit der Nutzung von Diensten der Informationsgesellschaft kann die betroffene Person ungeachtet der Richtlinie 2002/58/EG ihr Widerspruchsrecht mittels automatisierter Verfahren ausüben, bei denen technische Spezifikationen verwendet werden.

(6) Die betroffene Person hat das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, gegen die sie betreffende Verarbeitung sie betreffender personenbezogener Daten, die zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken gemäß Artikel 89 Absatz 1 erfolgt, Widerspruch einzulegen, es sei denn, die Verarbeitung ist zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe erforderlich.

ARTIKEL 22 Automatisierte Entscheidungen im Einzelfall einschließlich Profiling

(1) Die betroffene Person hat das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.

(2) Absatz 1 gilt nicht, wenn die Entscheidung

a) für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich ist,
b) aufgrund von Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche unterliegt, zulässig ist und diese Rechtsvorschriften angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten oder
c) mit ausdrücklicher Einwilligung der betroffenen Person erfolgt.

(3) In den in Absatz 2 Buchstaben a und c genannten Fällen trifft der Verantwortliche angemessene Maßnahmen, um die Rechte und Freiheiten sowie die berechtigten Interessen der betroffenen Person zu wahren, wozu mindestens das Recht auf Erwirkung des Eingreifens einer Person seitens des Verantwortlichen, auf

Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung gehört.

(4) Entscheidungen nach Absatz 2 dürfen nicht auf besonderen Kategorien personenbezogener Daten nach Artikel 9 Absatz 1 beruhen, sofern nicht Artikel 9 Absatz 2 Buchstabe a oder g gilt und angemessene Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person getroffen wurden.

ARTIKEL 26 Gemeinsam für die Verarbeitung Verantwortliche

(1) Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie gemeinsam Verantwortliche. Sie legen in einer Vereinbarung in transparenter Form fest, wer von ihnen welche Verpflichtung gemäß dieser Verordnung erfüllt, insbesondere was die Wahrnehmung der Rechte der betroffenen Person angeht, und wer welchen Informationspflichten gemäß den Artikeln 13 und 14 nachkommt, sofern und soweit die jeweiligen Aufgaben der Verantwortlichen nicht durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen die Verantwortlichen unterliegen, festgelegt sind. In der Vereinbarung kann eine Anlaufstelle für die betroffenen Personen angegeben werden.

(2) Die Vereinbarung gemäß Absatz 1 muss die jeweiligen tatsächlichen Funktionen und Beziehungen der gemeinsam Verantwortlichen gegenüber betroffenen Personen gebührend widerspiegeln. Das wesentliche der Vereinbarung wird der betroffenen Person zur Verfügung gestellt.

(3) Ungeachtet der Einzelheiten der Vereinbarung gemäß Absatz 1 kann die betroffene Person ihre Rechte im Rahmen dieser Verordnung bei und gegenüber jedem einzelnen der Verantwortlichen geltend machen.

ARTIKEL 28 Auftragsverarbeiter

(1) Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

(2) Der Auftragsverarbeiter nimmt keinen weiteren Auftragsverarbeiter ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Verantwortlichen in Anspruch. Im Fall einer allgemeinen schriftlichen Genehmigung informiert der Auftragsverarbeiter den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben.

(3) Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, der bzw. das den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet und in dem Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festgelegt sind. Dieser Vertrag bzw. dieses andere Rechtsinstrument sieht insbesondere vor, dass der Auftragsverarbeiter

a) die personenbezogenen Daten nur auf dokumentierte Weisung des Verantwortlichen – auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation – verarbeitet, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet;
b) gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen;
c) alle gemäß Artikel 32 erforderlichen Maßnahmen ergreift;
d) die in den Absätzen 2 und 4 genannten Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters einhält;
e) angesichts der Art der Verarbeitung den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützt, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III genannten Rechte der betroffenen Person nachzukommen;
f) unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 genannten Pflichten unterstützt;
g) nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder löscht oder zurückgibt, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht;
h) dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Artikel niedergelegten Pflichten zur Verfügung stellt und Überprüfungen – einschließlich Inspektionen –, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglicht und dazu beiträgt.

Mit Blick auf Unterabsatz 1 Buchstabe h informiert der Auftragsverarbeiter den Verantwortlichen unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen diese Verordnung oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt.

(4) Nimmt der Auftragsverarbeiter die Dienste eines weiteren Auftragsverarbeiters in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen des Verantwortlichen auszuführen, so werden diesem weiteren Auftragsverarbeiter im Wege eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats dieselben Datenschutzpflichten auferlegt, die in dem Vertrag oder anderen Rechtsinstrument zwischen dem Verantwortlichen und dem Auftragsverarbeiter gemäß Absatz 3 festgelegt sind, wobei insbesondere hinreichende Garantien dafür geboten werden muss, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen dieser Verordnung erfolgt. Kommt der weitere Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der erste Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten jenes anderen Auftragsverarbeiters.

(5) Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 durch einen Auftragsverarbeiter kann als Faktor herangezogen werden, um hinreichende Garantien im Sinne der Absätze 1 und 4 des vorliegenden Artikels nachzuweisen.

(6) Unbeschadet eines individuellen Vertrags zwischen dem Verantwortlichen und dem Auftragsverarbeiter kann der Vertrag oder das andere Rechtsinstrument im Sinne der Absätze 3 und 4 des vorliegenden Artikels ganz oder teilweise auf den in den Absätzen 7 und 8 des vorliegenden Artikels genannten Standardvertragsklauseln beruhen, auch wenn diese Bestandteil einer dem Verantwortlichen oder dem Auftragsverarbeiter gemäß den Artikeln 42 und 43 erteilten Zertifizierung sind.

(7) Die Kommission kann im Einklang mit dem Prüfverfahren gemäß Artikel 87 Absatz 2 Standardvertragsklauseln zur Regelung der in den Absätzen 3 und 4 des vorliegenden Artikels genannten Fragen festlegen.

(8) Eine Aufsichtsbehörde kann im Einklang mit dem Kohärenzverfahren gemäß Artikel 63 Standardvertragsklauseln zur Regelung der in den Absätzen 3 und 4 des vorliegenden Artikels genannten Fragen festlegen.

(9) Der Vertrag oder das andere Rechtsinstrument im Sinne der Absätze 3 und 4 ist schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann.

(10) Unbeschadet der Artikel 82, 83 und 84 gilt ein Auftragsverarbeiter, der unter Verstoß gegen diese Verordnung die Zwecke und Mittel der Verarbeitung bestimmt, in Bezug auf diese Verarbeitung als Verantwortlicher.

ARTIKEL 30 Verzeichnis von Verarbeitungstätigkeiten

(1) Jeder Verantwortliche und gegebenenfalls sein Vertreter führen ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen. Dieses Verzeichnis enthält sämtliche folgenden Angaben:

a) den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten;
b) die Zwecke der Verarbeitung;
c) eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;
d) die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen;
e) gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;
f) wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;
g) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1.

(2) Jeder Auftragsverarbeiter und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung, die Folgendes enthält:

a) den Namen und die Kontaktdaten des Auftragsverarbeiters oder der Auftragsverarbeiter und jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie gegebenenfalls des Vertreters des Verantwortlichen oder des Auftragsverarbeiters und eines etwaigen Datenschutzbeauftragten;
b) die Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden;
c) gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;
d) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1.

(3) Das in den Absätzen 1 und 2 genannte Verzeichnis ist schriftlich zu führen, was auch in einem elektronischen Format erfolgen kann.

(4) Der Verantwortliche oder der Auftragsverarbeiter sowie gegebenenfalls der Vertreter des Verantwortlichen oder des Auftragsverarbeiters stellen der Aufsichtsbehörde das Verzeichnis auf Anfrage zur Verfügung.

(5) Die in den Absätzen 1 und 2 genannten Pflichten gelten nicht für Unternehmen oder Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen, sofern die von ihnen vorgenommene Verarbeitung nicht ein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt, die Verarbeitung nicht nur gelegentlich erfolgt oder nicht die Verarbeitung besonderer Datenkategorien gemäß Artikel 9 Absatz 1 bzw. die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Artikels 10 einschließt.

ARTIKEL 32 Sicherheit der Verarbeitung

(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

(2) Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch – ob unbeabsichtigt oder unrechtmäßig – Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.

(3) Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in Absatz 1 des vorliegenden Artikels genannten Anforderungen nachzuweisen.

(4) Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

ARTIKEL 33 Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde

(1) Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Artikel 51 zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen.

(2) Wenn dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt wird, meldet er diese dem Verantwortlichen unverzüglich.

(3) Die Meldung gemäß Absatz 1 enthält zumindest folgende Informationen:

a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
b) den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
c) eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
d) eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(4) Wenn und soweit die Informationen nicht zur gleichen Zeit bereitgestellt werden können, kann der Verantwortliche diese Informationen ohne unangemessene weitere Verzögerung schrittweise zur Verfügung stellen.

(5) Der Verantwortliche dokumentiert Verletzungen des Schutzes personenbezogener Daten einschließlich aller im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten stehenden Fakten, von de-

ren Auswirkungen und der ergriffenen Abhilfemaßnahmen. Diese Dokumentation muss der Aufsichtsbehörde die Überprüfung der Einhaltung der Bestimmungen dieses Artikels ermöglichen.

ARTIKEL 34 Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person

(1) Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so benachrichtigt der Verantwortliche die betroffene Person unverzüglich von der Verletzung.

(2) Die in Absatz 1 genannte Benachrichtigung der betroffenen Person beschreibt in klarer und einfacher Sprache die Art der Verletzung des Schutzes personenbezogener Daten und enthält zumindest die in Artikel 33 Absatz 3 Buchstaben b, c und d genannten Informationen und Maßnahmen.

(3) Die Benachrichtigung der betroffenen Person gemäß Absatz 1 ist nicht erforderlich, wenn eine der folgenden Bedingungen erfüllt ist:

a) der Verantwortliche geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen hat und diese Vorkehrungen auf die von der Verletzung betroffenen personenbezogenen Daten angewandt wurden, insbesondere solche, durch die die personenbezogenen Daten für alle Personen, die nicht zum Zugang zu den personenbezogenen Daten befugt sind, unzugänglich gemacht werden, etwa durch Verschlüsselung;
b) der Verantwortliche durch nachfolgende Maßnahmen sichergestellt hat, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 aller Wahrscheinlichkeit nach nicht mehr besteht;
c) dies mit einem unverhältnismäßigen Aufwand verbunden wäre. In diesem Fall hat stattdessen eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme zu erfolgen, durch die die betroffenen Personen vergleichbar wirksam informiert werden.

(4) Wenn der Verantwortliche die betroffene Person nicht bereits über die Verletzung des Schutzes personenbezogener Daten benachrichtigt hat, kann die Aufsichtsbehörde unter Berücksichtigung der Wahrscheinlichkeit, mit der die Verletzung des Schutzes personenbezogener Daten zu einem hohen Risiko führt, von dem Verantwortlichen verlangen, dies nachzuholen, oder sie kann mit einem Beschluss feststellen, dass bestimmte der in Absatz 3 genannten Voraussetzungen erfüllt sind.

ARTIKEL 35 Datenschutz-Folgenabschätzung

(1) Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden.

(2) Der Verantwortliche holt bei der Durchführung einer Datenschutz-Folgenabschätzung den Rat des Datenschutzbeauftragten, sofern ein solcher benannt wurde, ein.

(3) Eine Datenschutz-Folgenabschätzung gemäß Absatz 1 ist insbesondere in folgenden Fällen erforderlich:

a) systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen;
b) umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 Absatz 1 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 oder
c) systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche.

(4) Die Aufsichtsbehörde erstellt eine Liste der Verarbeitungsvorgänge, für die gemäß Absatz 1 eine Datenschutz-Folgenabschätzung durchzuführen ist, und veröffentlicht diese. Die Aufsichtsbehörde übermittelt diese Listen dem in Artikel 68 genannten Ausschuss.

(5) Die Aufsichtsbehörde kann des Weiteren eine Liste der Arten von Verarbeitungsvorgängen erstellen und veröffentlichen, für die keine Datenschutz-Folgenabschätzung erforderlich ist. Die Aufsichtsbehörde übermittelt diese Listen dem Ausschuss.

(6) Vor Festlegung der in den Absätzen 4 und 5 genannten Listen wendet die zuständige Aufsichtsbehörde das Kohärenzverfahren gemäß Artikel 63 an, wenn solche Listen Verarbeitungstätigkeiten umfassen, die mit dem Angebot von Waren oder Dienstleistungen für betroffene Personen oder der Beobachtung des Verhaltens dieser Personen in mehreren Mitgliedstaaten im Zusammenhang stehen oder die den freien Verkehr personenbezogener Daten innerhalb der Union erheblich beeinträchtigen könnten.

(7) Die Folgenabschätzung enthält zumindest Folgendes:

a) eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen;

b) eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;
c) eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 und
d) die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.

(8) Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 durch die zuständigen Verantwortlichen oder die zuständigen Auftragsverarbeiter ist bei der Beurteilung der Auswirkungen der von diesen durchgeführten Verarbeitungsvorgänge, insbesondere für die Zwecke einer Datenschutz-Folgenabschätzung, gebührend zu berücksichtigen.

(9) Der Verantwortliche holt gegebenenfalls den Standpunkt der betroffenen Personen oder ihrer Vertreter zu der beabsichtigten Verarbeitung unbeschadet des Schutzes gewerblicher oder öffentlicher Interessen oder der Sicherheit der Verarbeitungsvorgänge ein.

(10) Falls die Verarbeitung gemäß Artikel 6 Absatz 1 Buchstabe c oder e auf einer Rechtsgrundlage im Unionsrecht oder im Recht des Mitgliedstaats, dem der Verantwortliche unterliegt, beruht und falls diese Rechtsvorschriften den konkreten Verarbeitungsvorgang oder die konkreten Verarbeitungsvorgänge regeln und bereits im Rahmen der allgemeinen Folgenabschätzung im Zusammenhang mit dem Erlass dieser Rechtsgrundlage eine Datenschutz-Folgenabschätzung erfolgte, gelten die Absätze 1 bis 7 nur, wenn es nach dem Ermessen der Mitgliedstaaten erforderlich ist, vor den betreffenden Verarbeitungstätigkeiten eine solche Folgenabschätzung durchzuführen.

(11) Erforderlichenfalls führt der Verantwortliche eine Überprüfung durch, um zu bewerten, ob die Verarbeitung gemäß der Datenschutz-Folgenabschätzung durchgeführt wird; dies gilt zumindest, wenn hinsichtlich des mit den Verarbeitungsvorgängen verbundenen Risikos Änderungen eingetreten sind.

ARTIKEL 37 Benennung eines Datenschutzbeauftragten

(1) Der Verantwortliche und der Auftragsverarbeiter benennen auf jeden Fall einen Datenschutzbeauftragten, wenn
a) die Verarbeitung von einer Behörde oder öffentlichen Stelle durchgeführt wird, mit Ausnahme von Gerichten, die im Rahmen ihrer justiziellen Tätigkeit handeln,
b) die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen, oder
c) die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 besteht.

(2) Eine Unternehmensgruppe darf einen gemeinsamen Datenschutzbeauftragten ernennen, sofern von jeder Niederlassung aus der Datenschutzbeauftragte leicht erreicht werden kann.

(3) Falls es sich bei dem Verantwortlichen oder dem Auftragsverarbeiter um eine Behörde oder öffentliche Stelle handelt, kann für mehrere solcher Behörden oder Stellen unter Berücksichtigung ihrer Organisationsstruktur und ihrer Größe ein gemeinsamer Datenschutzbeauftragter benannt werden.

(4) In anderen als den in Absatz 1 genannten Fällen können der Verantwortliche oder der Auftragsverarbeiter oder Verbände und andere Vereinigungen, die Kategorien von Verantwortlichen oder Auftragsverarbeitern vertreten, einen Datenschutzbeauftragten benennen; falls dies nach dem Recht der Union oder der Mitgliedstaaten vorgeschrieben ist, müssen sie einen solchen benennen. Der Datenschutzbeauftragte kann für derartige Verbände und andere Vereinigungen, die Verantwortliche oder Auftragsverarbeiter vertreten, handeln.

(5) Der Datenschutzbeauftragte wird auf der Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens benannt, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie auf der Grundlage seiner Fähigkeit zur Erfüllung der in Artikel 39 genannten Aufgaben.

(6) Der Datenschutzbeauftragte kann Beschäftigter des Verantwortlichen oder des Auftragsverarbeiters sein oder seine Aufgaben auf der Grundlage eines Dienstleistungsvertrags erfüllen.

(7) Der Verantwortliche oder der Auftragsverarbeiter veröffentlicht die Kontaktdaten des Datenschutzbeauftragten und teilt diese Daten der Aufsichtsbehörde mit.

ARTIKEL 41 Überwachung der genehmigten Verhaltensregeln

(1) Unbeschadet der Aufgaben und Befugnisse der zuständigen Aufsichtsbehörde gemäß den Artikeln 57 und 58 kann die Überwachung der Einhaltung von Verhaltensregeln gemäß Artikel 40 von einer Stelle durchgeführt werden, die über das geeignete Fachwissen hin-

sichtlich des Gegenstands der Verhaltensregeln verfügt und die von der zuständigen Aufsichtsbehörde zu diesem Zweck akkreditiert wurde.

(2) Eine Stelle gemäß Absatz 1 kann zum Zwecke der Überwachung der Einhaltung von Verhaltensregeln akkreditiert werden, wenn sie

a) ihre Unabhängigkeit und ihr Fachwissen hinsichtlich des Gegenstands der Verhaltensregeln zur Zufriedenheit der zuständigen Aufsichtsbehörde nachgewiesen hat;
b) Verfahren festgelegt hat, die es ihr ermöglichen, zu bewerten, ob Verantwortliche und Auftragsverarbeiter die Verhaltensregeln anwenden können, die Einhaltung der Verhaltensregeln durch die Verantwortlichen und Auftragsverarbeiter zu überwachen und die Anwendung der Verhaltensregeln regelmäßig zu überprüfen;
c) Verfahren und Strukturen festgelegt hat, mit denen sie Beschwerden über Verletzungen der Verhaltensregeln oder über die Art und Weise, in der die Verhaltensregeln von dem Verantwortlichen oder dem Auftragsverarbeiter angewendet werden oder wurden, nachgeht und diese Verfahren und Strukturen für betroffene Personen und die Öffentlichkeit transparent macht, und
d) zur Zufriedenheit der zuständigen Aufsichtsbehörde nachgewiesen hat, dass ihre Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen.

(3) Die zuständige Aufsichtsbehörde übermittelt den Entwurf der Kriterien für die Akkreditierung einer Stelle nach Absatz 1 gemäß dem Kohärenzverfahren nach Artikel 63 an den Ausschuss.

(4) Unbeschadet der Aufgaben und Befugnisse der zuständigen Aufsichtsbehörde und der Bestimmungen des Kapitels VIII ergreift eine Stelle gemäß Absatz 1 vorbehaltlich geeigneter Garantien im Falle einer Verletzung der Verhaltensregeln durch einen Verantwortlichen oder einen Auftragsverarbeiter geeignete Maßnahmen, einschließlich eines vorläufigen oder endgültigen Ausschlusses des Verantwortlichen oder Auftragsverarbeiters von den Verhaltensregeln. Sie unterrichtet die zuständige Aufsichtsbehörde über solche Maßnahmen und deren Begründung.

(5) Die zuständige Aufsichtsbehörde widerruft die Akkreditierung einer Stelle gemäß Absatz 1, wenn die Voraussetzungen für ihre Akkreditierung nicht oder nicht mehr erfüllt sind oder wenn die Stelle Maßnahmen ergreift, die nicht mit dieser Verordnung vereinbar sind.

(6) Dieser Artikel gilt nicht für die Verarbeitung durch Behörden oder öffentliche Stellen.

ARTIKEL 42 Zertifizierung

(1) Die Mitgliedstaaten, die Aufsichtsbehörden, der Ausschuss und die Kommission fördern insbesondere auf Unionsebene die Einführung von datenschutzspezifischen Zertifizierungsverfahren sowie von Datenschutzsiegeln und -prüfzeichen, die dazu dienen, nachzuweisen, dass diese Verordnung bei Verarbeitungsvorgängen von Verantwortlichen oder Auftragsverarbeitern eingehalten wird. Den besonderen Bedürfnissen von Kleinstunternehmen sowie kleinen und mittleren Unternehmen wird Rechnung getragen.

(2) Zusätzlich zur Einhaltung durch die unter diese Verordnung fallenden Verantwortlichen oder Auftragsverarbeiter können auch datenschutzspezifische Zertifizierungsverfahren, Siegel oder Prüfzeichen, die gemäß Absatz 5 des vorliegenden Artikels genehmigt worden sind, vorgesehen werden, um nachzuweisen, dass die Verantwortlichen oder Auftragsverarbeiter, die gemäß Artikel 3 nicht unter diese Verordnung fallen, im Rahmen der Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen nach Maßgabe von Artikel 46 Absatz 2 Buchstabe f geeignete Garantien bieten. Diese Verantwortlichen oder Auftragsverarbeiter gehen mittels vertraglicher oder sonstiger rechtlich bindender Instrumente die verbindliche und durchsetzbare Verpflichtung ein, diese geeigneten Garantien anzuwenden, auch im Hinblick auf die Rechte der betroffenen Personen.

(3) Die Zertifizierung muss freiwillig und über ein transparentes Verfahren zugänglich sein.

(4) Eine Zertifizierung gemäß diesem Artikel mindert nicht die Verantwortung des Verantwortlichen oder des Auftragsverarbeiters für die Einhaltung dieser Verordnung und berührt nicht die Aufgaben und Befugnisse der Aufsichtsbehörden, die gemäß Artikel 55 oder 56 zuständig sind.

(5) Eine Zertifizierung nach diesem Artikel wird durch die Zertifizierungsstellen nach Artikel 43 oder durch die zuständige Aufsichtsbehörde anhand der von dieser zuständigen Aufsichtsbehörde gemäß Artikel 58 Absatz 3 oder – gemäß Artikel 63 – durch den Ausschuss genehmigten Kriterien erteilt. Werden die Kriterien vom Ausschuss genehmigt, kann dies zu einer gemeinsamen Zertifizierung, dem Europäischen Datenschutzsiegel, führen.

(6) Der Verantwortliche oder der Auftragsverarbeiter, der die von ihm durchgeführte Verarbeitung dem Zertifizierungsverfahren unterwirft, stellt der Zertifizierungsstelle nach Artikel 43 oder gegebenenfalls der zuständigen Aufsichtsbehörde alle für die Durchführung des Zertifizierungsverfahrens erforderlichen Informationen zur Verfügung und gewährt ihr den in diesem Zusammenhang erforderlichen Zugang zu seinen Verarbeitungstätigkeiten.

(7) Die Zertifizierung wird einem Verantwortlichen oder einem Auftragsverarbeiter für eine Höchstdauer von drei Jahren erteilt und kann unter denselben Bedingungen verlängert werden, sofern die einschlägigen Voraussetzungen weiterhin erfüllt werden. Die Zertifizierung wird gegebenenfalls durch die Zertifizierungsstellen nach

Artikel 43 oder durch die zuständige Aufsichtsbehörde widerrufen, wenn die Voraussetzungen für die Zertifizierung nicht oder nicht mehr erfüllt werden.

(8) Der Ausschuss nimmt alle Zertifizierungsverfahren und Datenschutzsiegel und -prüfzeichen in ein Register auf und veröffentlicht sie in geeigneter Weise.

ARTIKEL 49 Ausnahmen für bestimmte Fälle

(1) Falls weder ein Angemessenheitsbeschluss nach Artikel 45 Absatz 3 vorliegt noch geeignete Garantien nach Artikel 46, einschließlich verbindlicher interner Datenschutzvorschriften, bestehen, ist eine Übermittlung oder eine Reihe von Übermittlungen personenbezogener Daten an ein Drittland oder an eine internationale Organisation nur unter einer der folgenden Bedingungen zulässig:

a) die betroffene Person hat in die vorgeschlagene Datenübermittlung ausdrücklich eingewilligt, nachdem sie über die für sie bestehenden möglichen Risiken derartiger Datenübermittlungen ohne Vorliegen eines Angemessenheitsbeschlusses und ohne geeignete Garantien unterrichtet wurde,
b) die Übermittlung ist für die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen oder zur Durchführung von vorvertraglichen Maßnahmen auf Antrag der betroffenen Person erforderlich,
c) die Übermittlung ist zum Abschluss oder zur Erfüllung eines im Interesse der betroffenen Person von dem Verantwortlichen mit einer anderen natürlichen oder juristischen Person geschlossenen Vertrags erforderlich,
d) die Übermittlung ist aus wichtigen Gründen des öffentlichen Interesses notwendig,
e) die Übermittlung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich,
f) die Übermittlung ist zum Schutz lebenswichtiger Interessen der betroffenen Person oder anderer Personen erforderlich, sofern die betroffene Person aus physischen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu geben,
g) die Übermittlung erfolgt aus einem Register, das gemäß dem Recht der Union oder der Mitgliedstaaten zur Information der Öffentlichkeit bestimmt ist und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offensteht, aber nur soweit die im Recht der Union oder der Mitgliedstaaten festgelegten Voraussetzungen für die Einsichtnahme im Einzelfall gegeben sind.

Falls die Übermittlung nicht auf eine Bestimmung der Artikel 45 oder 46 – einschließlich der verbindlichen internen Datenschutzvorschriften – gestützt werden könnte und keine der Ausnahmen für einen bestimmten Fall gemäß dem ersten Unterabsatz anwendbar ist, darf eine Übermittlung an ein Drittland oder eine internationale Organisation nur dann erfolgen, wenn die Übermittlung nicht wiederholt erfolgt, nur eine begrenzte Zahl von betroffenen Personen betrifft, für die Wahrung der zwingenden berechtigten Interessen des Verantwortlichen erforderlich ist, sofern die Interessen oder die Rechte und Freiheiten der betroffenen Person nicht überwiegen, und der Verantwortliche alle Umstände der Datenübermittlung beurteilt und auf der Grundlage dieser Beurteilung geeignete Garantien in Bezug auf den Schutz personenbezogener Daten vorgesehen hat. Der Verantwortliche setzt die Aufsichtsbehörde von der Übermittlung in Kenntnis. Der Verantwortliche unterrichtet die betroffene Person über die Übermittlung und seine zwingenden berechtigten Interessen; dies erfolgt zusätzlich zu den der betroffenen Person nach den Artikeln 13 und 14 mitgeteilten Informationen.

(2) Datenübermittlungen gemäß Absatz 1 Unterabsatz 1 Buchstabe g dürfen nicht die Gesamtheit oder ganze Kategorien der im Register enthaltenen personenbezogenen Daten umfassen. Wenn das Register der Einsichtnahme durch Personen mit berechtigtem Interesse dient, darf die Übermittlung nur auf Anfrage dieser Personen oder nur dann erfolgen, wenn diese Personen die Adressaten der Übermittlung sind.

(3) Absatz 1 Unterabsatz 1 Buchstaben a, b und c und sowie Absatz 1 Unterabsatz 2 gelten nicht für Tätigkeiten, die Behörden in Ausübung ihrer hoheitlichen Befugnisse durchführen.

(4) Das öffentliche Interesse im Sinne des Absatzes 1 Unterabsatz 1 Buchstabe d muss im Unionsrecht oder im Recht des Mitgliedstaats, dem der Verantwortliche unterliegt, anerkannt sein.

(5) Liegt kein Angemessenheitsbeschluss vor, so können im Unionsrecht oder im Recht der Mitgliedstaaten aus wichtigen Gründen des öffentlichen Interesses ausdrücklich Beschränkungen der Übermittlung bestimmter Kategorien von personenbezogenen Daten an Drittländer oder internationale Organisationen vorgesehen werden. Die Mitgliedstaaten teilen der Kommission derartige Bestimmungen mit.

(6) Der Verantwortliche oder der Auftragsverarbeiter erfasst die von ihm vorgenommene Beurteilung sowie die angemessenen Garantien im Sinne des Absatzes 1 Unterabsatz 2 des vorliegenden Artikels in der Dokumentation gemäß Artikel 30.

ARTIKEL 83 Allgemeine Bedingungen für die Verhängung von Geldbußen

(1) Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von Geldbußen gemäß diesem Artikel für Verstöße gegen diese Verordnung gemäß den Absätzen 5 und 6 in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist.

(2) Geldbußen werden je nach den Umständen des Einzelfalls zusätzlich zu oder anstelle von Maßnahmen nach Artikel 58 Absatz 2 Buchstaben a bis h und i ver-

hängt. Bei der Entscheidung über die Verhängung einer Geldbuße und über deren Betrag wird in jedem Einzelfall Folgendes gebührend berücksichtigt:

a) Art, Schwere und Dauer des Verstoßes unter Berücksichtigung der Art, des Umfangs oder des Zwecks der betreffenden Verarbeitung sowie der Zahl der von der Verarbeitung betroffenen Personen und des Ausmaßes des von ihnen erlittenen Schadens;
b) Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes;
c) jegliche von dem Verantwortlichen oder dem Auftragsverarbeiter getroffenen Maßnahmen zur Minderung des den betroffenen Personen entstandenen Schadens;
d) Grad der Verantwortung des Verantwortlichen oder des Auftragsverarbeiters unter Berücksichtigung der von ihnen gemäß den Artikeln 25 und 32 getroffenen technischen und organisatorischen Maßnahmen;
e) etwaige einschlägige frühere Verstöße des Verantwortlichen oder des Auftragsverarbeiters;
f) Umfang der Zusammenarbeit mit der Aufsichtsbehörde, um dem Verstoß abzuhelfen und seine möglichen nachteiligen Auswirkungen zu mindern;
g) Kategorien personenbezogener Daten, die von dem Verstoß betroffen sind;
h) Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde, insbesondere ob und gegebenenfalls in welchem Umfang der Verantwortliche oder der Auftragsverarbeiter den Verstoß mitgeteilt hat;
i) Einhaltung der nach Artikel 58 Absatz 2 früher gegen den für den betreffenden Verantwortlichen oder Auftragsverarbeiter in Bezug auf denselben Gegenstand angeordneten Maßnahmen, wenn solche Maßnahmen angeordnet wurden;
j) Einhaltung von genehmigten Verhaltensregeln nach Artikel 40 oder genehmigten Zertifizierungsverfahren nach Artikel 42 und
k) jegliche anderen erschwerenden oder mildernden Umstände im jeweiligen Fall, wie unmittelbar oder mittelbar durch den Verstoß erlangte finanzielle Vorteile oder vermiedene Verluste.

(3) Verstößt ein Verantwortlicher oder ein Auftragsverarbeiter bei gleichen oder miteinander verbundenen Verarbeitungsvorgängen vorsätzlich oder fahrlässig gegen mehrere Bestimmungen dieser Verordnung, so übersteigt der Gesamtbetrag der Geldbuße nicht den Betrag für den schwerwiegendsten Verstoß.

(4) Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2 Geldbußen von bis zu 10 000 000 EUR oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist:

a) die Pflichten der Verantwortlichen und der Auftragsverarbeiter gemäß den Artikeln 8, 11, 25 bis 39, 42 und 43;
b) die Pflichten der Zertifizierungsstelle gemäß den Artikeln 42 und 43;
c) die Pflichten der Überwachungsstelle gemäß Artikel 41 Absatz 4.

(5) Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2 Geldbußen von bis zu 20 000 000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist:

a) die Grundsätze für die Verarbeitung, einschließlich der Bedingungen für die Einwilligung, gemäß den Artikeln 5, 6, 7 und 9;
b) die Rechte der betroffenen Person gemäß den Artikeln 12 bis 22;
c) die Übermittlung personenbezogener Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation gemäß den Artikeln 44 bis 49;
d) alle Pflichten gemäß den Rechtsvorschriften der Mitgliedstaaten, die im Rahmen des Kapitels IX erlassen wurden;
e) Nichtbefolgung einer Anweisung oder einer vorübergehenden oder endgültigen Beschränkung oder Aussetzung der Datenübermittlung durch die Aufsichtsbehörde gemäß Artikel 58 Absatz 2 oder Nichtgewährung des Zugangs unter Verstoß gegen Artikel 58 Absatz 1.

(6) Bei Nichtbefolgung einer Anweisung der Aufsichtsbehörde gemäß Artikel 58 Absatz 2 werden im Einklang mit Absatz 2 des vorliegenden Artikels Geldbußen von bis zu 20 000 000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist.

(7) Unbeschadet der Abhilfebefugnisse der Aufsichtsbehörden gemäß Artikel 58 Absatz 2 kann jeder Mitgliedstaat Vorschriften dafür festlegen, ob und in welchem Umfang gegen Behörden und öffentliche Stellen, die in dem betreffenden Mitgliedstaat niedergelassen sind, Geldbußen verhängt werden können.

(8) Die Ausübung der eigenen Befugnisse durch eine Aufsichtsbehörde gemäß diesem Artikel muss angemessenen Verfahrensgarantien gemäß dem Unionsrecht und dem Recht der Mitgliedstaaten, einschließlich wirksamer gerichtlicher Rechtsbehelfe und ordnungsgemäßer Verfahren, unterliegen.

(9) Sieht die Rechtsordnung eines Mitgliedstaats keine Geldbußen vor, kann dieser Artikel so angewandt werden, dass die Geldbuße von der zuständigen Aufsichtsbehörde in die Wege geleitet und von den zuständigen nationalen Gerichten verhängt wird, wobei sicherzustellen ist, dass diese Rechtsbehelfe wirksam sind und die gleiche Wirkung wie die von Aufsichtsbehörden verhängten Geldbußen haben. In jeden Fall müssen die verhängten Geldbußen wirksam, verhältnismäßig und abschreckend sein. Die betreffenden Mitgliedstaaten teilen der Kommission bis zum 25. Mai 2018 die

Rechtsvorschriften mit, die sie aufgrund dieses Absatzes erlassen, sowie unverzüglich alle späteren Änderungsgesetze oder Änderungen dieser Vorschriften.

ARTIKEL 95 **Verhältnis zur Richtlinie 2002/58/EG**

Diese Verordnung erlegt natürlichen oder juristischen Personen in Bezug auf die Verarbeitung in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der Union keine zusätzlichen Pflichten auf, soweit sie besonderen in der Richtlinie 2002/58/EG festgelegten Pflichten unterliegen, die dasselbe Ziel verfolgen.

www.ddv.de