1. Einführung

Vom Rechtsanwender werden zunehmend vertiefte Kenntnisse der technischen Hintergründe verlangt. Das wird zunehmend anspruchsvoller, da Sicherheitsmaßnahmen wie Verschlüsselung und das stetige Ziel, Anwendungen so benutzerfreundlich wie möglich zu machen, den Blick auf die Daten und die konkreten Verarbeitungsprozesse erschweren. Dies führt dazu, dass ohne technisches Verständnis des zu beurteilenden Sachverhalts die datenschutzrechtlichen Vorschriften nicht richtig angewendet werden können.

Dieser Leitfaden erhält daher nicht nur die datenschutzrechtlichen Anforderungen und hilfreiche Tipps zur Umsetzung, sondern beleuchtet auch die Funktionsweise von Online-Diensten.

Der vorliegende Ratgeber beschäftigt sich mit Datenschutz und ePrivacy bei Websites, Social Media und Messengern. Die in der Datenschutz-Grundverordnung (DS-GVO) enthaltenen allgemeinen Vorschriften sollen insofern bezüglich "elektronischer Kommunikationsdaten" durch eine Verordnung über Privatsphäre und elektronische Kommunikation (ePrivacy-VO) ergänzt und präzisiert werden. Das Gesetzgebungsverfahren verzögert sich allerdings und es besteht erhebliche Unsicherheit, wie bis zum Inkrafttreten der ePrivacy-VO mit Online-Sachverhalten umzugehen ist. Vom Rechtsanwender werden zudem zunehmend vertiefte Kenntnisse der technischen Hintergründe verlangt. Ohne technisches Verständnis des zu beurteilenden Sachverhalts können die datenschutzrechtlichen Vorschriften nicht richtig angewendet werden. Dieser Ratgeber soll den Rechtsanwendern in Unternehmen und Behörden insoweit praktische Unterstützung bieten.

Dazu wird zunächst ein Überblick über den europäischen und nationalen Rechtsrahmen für Online-Datenverarbeitungen gewährt und es werden die möglichen Rechtsgrundlagen (Vertrag, Interessenabwägung, Einwilligung) für Online-Datenverarbeitungen ausführlich dargestellt. Nachfolgend werden technische Erläuterungen zur Funktionsweise des Internets, zu den typischen Datenverarbeitungen im Zusammenhang mit Websites, Trackingverfahren sowie dem Einsatz von Cookies gegeben. Besonderen Nutzen für die Praxis bieten u.a. die im Ratgeber enthaltenen Beispiele für die möglichen Gestaltung von sog. „Cookie-Bannern“, vgl. Abschnitt 4.7. Insoweit erfolgt jeweils eine Bewertung der Rechtssicherheit der einzelnen Gestaltungen. Ein hilfreicher tabellarischer Überblick über die Zulässigkeit von Datenverarbeitungen im Zusammenhang mit der Website findet sich im Abschnitt 4.6.

Besondere Abschnitte befassen sich mit dem Einsatz von Social Media (Kapitel 5.) und Messengern wie z.B. WhatsApp (Kapitel 6.), der Umsetzung der Betroffenenrechte im Zusammenhang mit Onlineauftritten (Kapitel 7.) sowie Datenschutzerklärung und Impressum (Kapitel 8.). Abgeschlossen werden die Ausführungen durch einen Abschnitt zur Rechenschaftspflicht (Kapitel 9.), der insbesondere die Aspekte Nachweis der Einwilligung, Verzeichnis der Verarbeitungstätigkeiten (VVT), Dokumentation der Interessenabwägung und Datenschutzfolgenabschätzung aufgreift.

2. Rechtlicher Rahmen

Die datenschutzrechtlichen Anforderungen beim Betrieb einer Website und beim Einsatz von Social Media und Messenger ergeben sich aus einem Zusammenspiel von europäischem Sekundärrecht, Verordnungen und Richtlinien sowie den nationalen Regelungen.

Die Schwierigkeit liegt darin, die abstrakten Regelungen anzuwenden, da sich im Online-Bereich nicht zuletzt auf Grund der ständigen Innovationen stets neue Fragen zum geltenden Recht ergeben.

2.1 Europäisches Recht

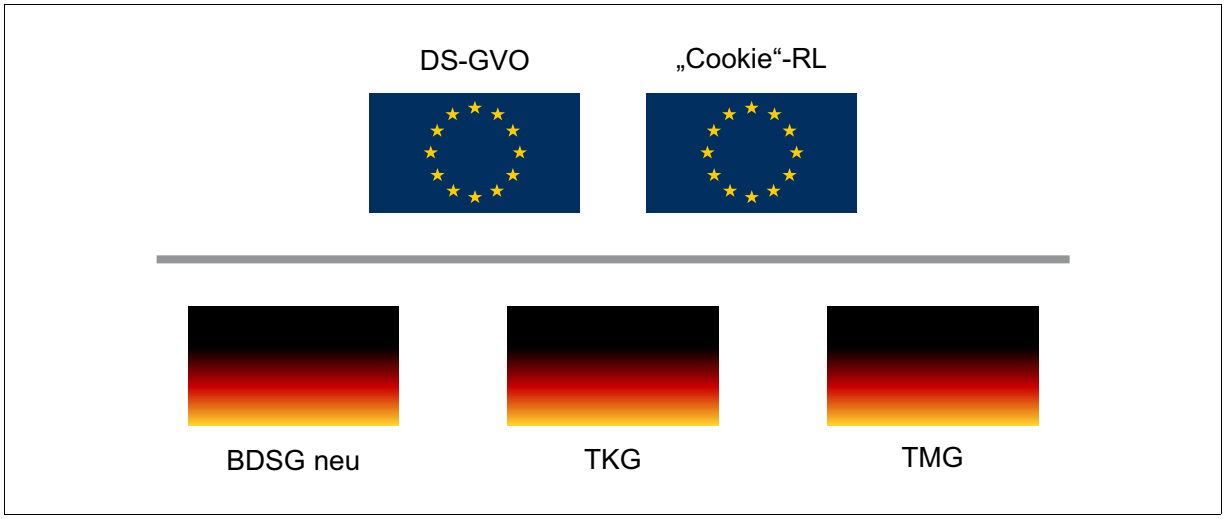

Abb. 1: Übersicht aller in Betracht kommenden nationalen und europäischen Regelungen

2.1.1 Datenschutz-Grundverordnung (DS-GVO)

Die **Datenschutz-Grundverordnung (DS-GVO)** enthält keine spezialgesetzlichen Regelungen zum Online-Bereich. Zwar ist den Erwägungsgründen zu entnehmen, dass der Gesetzgeber sich mit den spezifischen Risiken im Zusammenhang mit der Online-Nutzung auseinandergesetzt hat. Dennoch gelten für den Bereich Websites, Social Media und alle weiteren internetbasierten Dienste die abstrakten Regelungen der DS-GVO.

Verantwortliche müssen sicherstellen, dass sämtliche Verarbeitungstätigkeiten im Zusammenhang mit Online-Diensten rechtmäßig erfolgen und alle weiteren Pflichten der DS-GVO umgesetzt werden.

Die DS-GVO gilt unmittelbar in jedem Mitgliedsstaat und schützt die Grundrechte und Grundfreiheiten natürlicher Personen. Dazu gehört insbesondere das in Art. 8 der Grundrechte-Charta (GRCh) verankerte Recht auf Schutz personenbezogener Daten. Art. 8 GRCh schützt den Einzelnen vor Beeinträchtigungen, die durch eine Verarbeitung seiner Daten entstehen. Dies umfasst nicht nur unmittelbare Folgen einer Verarbeitung wie beispielsweise den Verlust von Daten durch eine Fehlversendung. Der Schutzbereich des Art. 8 GrCh umfasst auch mittelbare Folgen der Datenverarbeitung wie z.B. Diskriminierung oder finanzielle Schäden durch Identitätsdiebstahl bei Online-Shops.

Abb. 2: Online-Dienste nur in Erwägungsgründen erwähnt

Darüber hinaus regelt die DS-GVO auch den freien Verkehr personenbezogener Daten gem. Art. 1 Abs. 3 DS-GVO innerhalb der Europäischen Union. Der freie Verkehr von personenbezogenen Daten soll gewährleisten, dass Daten ohne Beeinträchtigung innerhalb der EU-Mitgliedsstaaten übermittelt werden dürfen. Dieses Recht leitet sich ebenfalls aus der Grundrechte-Charta ab und gewährleistet die wirtschaftliche Betätigung von Unternehmen im Zeitalter der Digitalisierung.

Die DS-GVO gilt für alle Unternehmen, die eine Niederlassung innerhalb der Europäischen Union haben, sowie für Unternehmen, die auf dem europäischen Markt Waren oder Dienstleistungen anbieten oder das Verhalten von betroffenen Personen beobachten, soweit sie sich in der EU befinden (**Marktortprinzip**).

Dies bedeutet konkret, dass die DS-GVO zu beachten ist, wenn ein Website-Betreiber eine Niederlassung in der EU hat. Darüber hinaus ist die DS-GVO von Website-Betreibern mit Sitz außerhalb der EU zu beachten, wenn sich der Online-Dienst erkennbar an Nutzer der EU richtet. Dies ist beispielsweise der Fall, wenn die Website in einer Amtssprache der EU erstellt ist und gezielt Nutzer der EU anspricht.

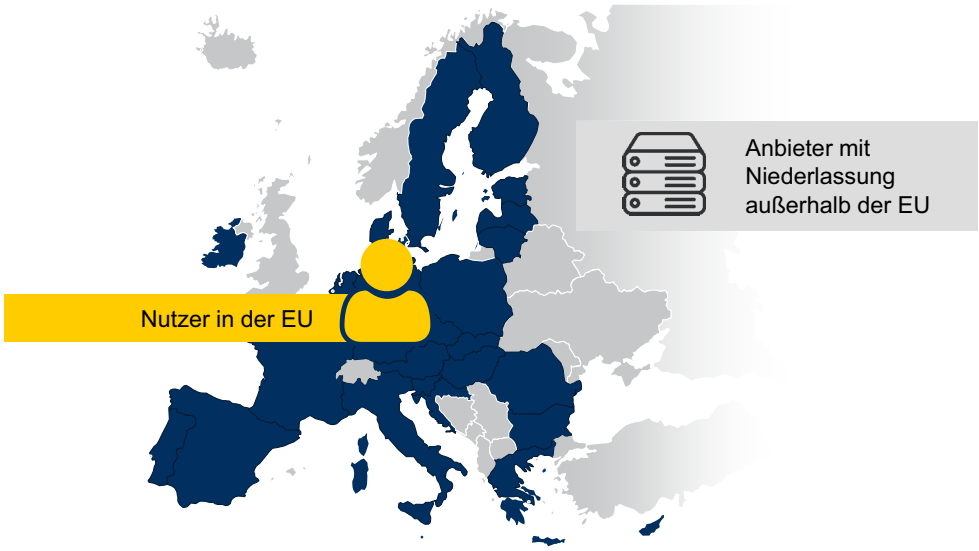

Abb. 3: Marktortprinzip

Praxisbeispiel

Der Betreiber eines Online-Shops hat seine einzige Niederlassung in Brasilien. Der Online-Shop steht in den Sprachen Spanisch, Deutsch und Französisch zur Verfügung und die Lieferung erfolgt an Nutzer in Spanien, Deutschland und Frankreich.

Die DS-GVO findet in diesem Fall Anwendung, da sich der Online-Shop gezielt an Nutzer der EU richtet.

2.1.2 ePrivacy-Richtlinie

Die **ePrivacy-Richtlinie (Richtlinie 2002/58/EG)** trat bereits 2002 in Kraft und regelt wie die DS-GVO den Schutz personenbezogener Daten sowie den freien Datenverkehr. Darüber hinaus schützt sie auch die Vertraulichkeit der Kommunikation gem. Art. 7 GRCh und geht damit über den Schutzbereich der DS-GVO hinaus.

Im Jahr 2009 wurde die ePrivacy-Richtlinie durch die sog. **„Cookie-Richtlinie" (Richtlinie 2009/136/EG)** ergänzt. Ihren Namen verdankt die Cookie-Richtlinie der Regelung in Art. 5 Abs. 3, die den Umgang mit Informationen auf Endgeräten der Nutzer regelt. Demnach ist die Speicherung oder der Zugriff auf Informationen von Endgeräten nur nach vorheriger Einwilligung des Nutzers zulässig, es sei denn, dies ist zur Erbringung des elektronischen Kommunikationsdienstes unbedingt erforderlich.

In der Praxis ist diese Vorschrift von großer Bedeutung, da u.a. Cookies[1], die für diverse Zwecke, vor allem beim Tracking, genutzt werden, unter diese Vorschrift fallen. Aufgrund Art. 5 Abs. 3 wurde häufig der falsche Schluss gezogen, der Einsatz von Cookies sei stets einwilligungsbedürftig. Daraufhin hat sich in der Praxis der sog. Cookie-Banner[2] etabliert, der beim Aufruf einer Website erscheint.

Art. 5 Abs. 3 ePrivacy-Richtlinie schützt nicht nur die Integrität des Geräts, sondern auch vor Beeinträchtigungen der Nutzer bei der Verwendung internetbasierter Dienste und zwar schon, bevor es zu einer Datenverarbeitung beim Verantwortlichen kommt. Daher fallen nicht nur der Einsatz von Cookies in den Anwendungsbereich dieser Vorschrift, sondern jede Form von eindeutigen Nutzerkennungen, z.B. Werbe-ID, MAC-Adresse oder weitere Nutzerkennungen.

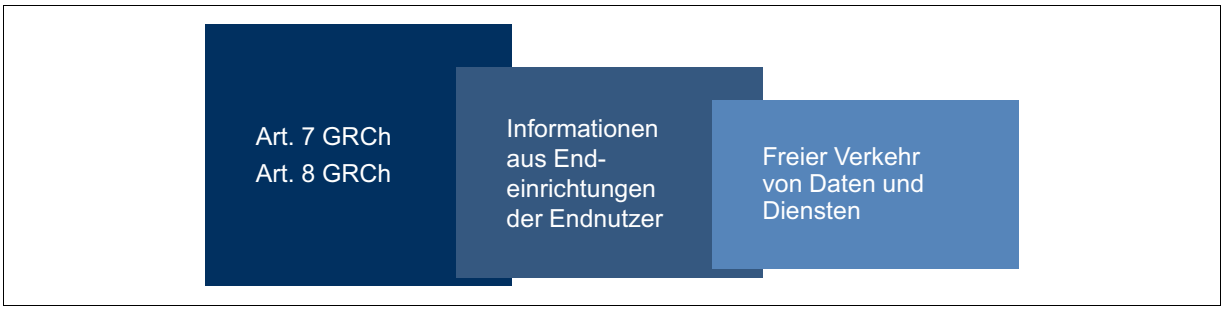

Abb. 4: Schutzbereich der ePrivacy-Richtlinie

Die Cookie-Richtlinie gilt nicht unmittelbar in den EU-Mitgliedstaaten. Vielmehr bedarf es gemäß Art. 288 AEUV eines Umsetzungsaktes durch die Mitgliedstaaten.

Die meisten Regelungen der ePrivacy-Richtlinie wurden im **Telekommunikationsgesetz (TKG)** umgesetzt. Dort ist beispielsweise der Umgang mit Verkehrs- und Standortdaten geregelt, die bei

1 Zu Cookies vgl. im Detail Abschnitt 4.5.2.

2 Zur Gestaltung von Cookie-Bannern vgl. 4.7.

der Telekommunikation anfallen. Darüber hinaus ist der Grundsatz der Vertraulichkeit der Kommunikation in § 88 TKG, der Vorschrift zum Fernmeldegeheimnis, verankert.

Auch das **Gesetz gegen den unlauteren Wettbewerb (UWG)** enthält eine Umsetzung der ePrivacy-RL mit Blick auf unerbetene Kommunikation. Gemäß Art. 13 ePrivacy-RL kann eine natürliche oder juristische Person, wenn sie von ihren Kunden im Zusammenhang mit dem Verkauf eines Produkts oder einer Dienstleistung gemäß der Richtlinie 95/46/EG deren elektronische Kontaktinformationen für elektronische Post erhalten hat, diese zur Direktwerbung für eigene ähnliche Produkte oder Dienstleistungen verwenden, sofern die Kunden klar und deutlich die Möglichkeit erhalten, eine solche Nutzung ihrer elektronischen Kontaktinformationen bei deren Erhebung und bei jeder Übertragung gebührenfrei und problemlos abzulehnen, wenn der Kunde diese Nutzung nicht von vornherein abgelehnt hat. Diese Vorschrift wurde in § 7 UWG umgesetzt, der u.a. den **Versand von Newslettern für Werbezwecke** regelt.

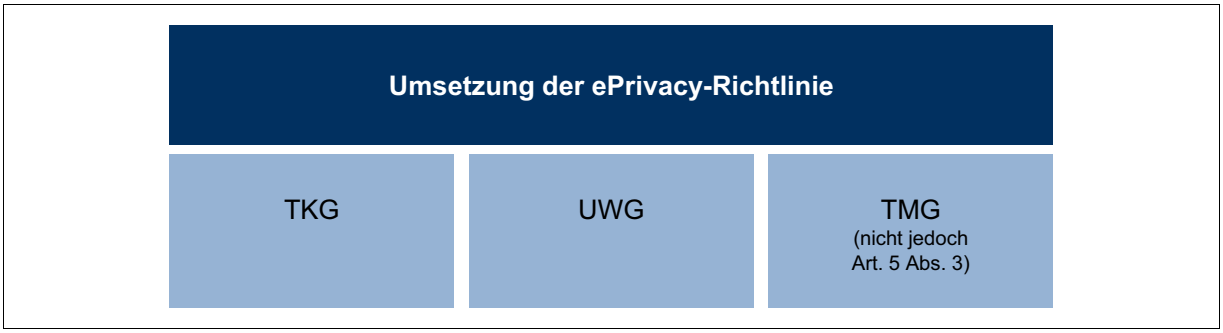

Abb. 5: Umsetzung der ePrivacy-RL im nationalen Recht

2.1.3 ePrivacy-Verordnung

Die **ePrivacy-Verordnung** sollte ursprünglich zusammen mit der DS-GVO am 25. Mai 2018 gelten und die ePrivacy-Richtlinie ersetzen. Allerdings verzögerte sich das Gesetzgebungsverfahren erheblich, sodass mit einem Inkrafttreten der ePrivacy-Verordnung nicht vor 2021 zu rechnen ist. Ob es eine Übergangsfrist geben wird, und wenn ja, wie lang diese dauern wird, ist ebenfalls noch unklar.

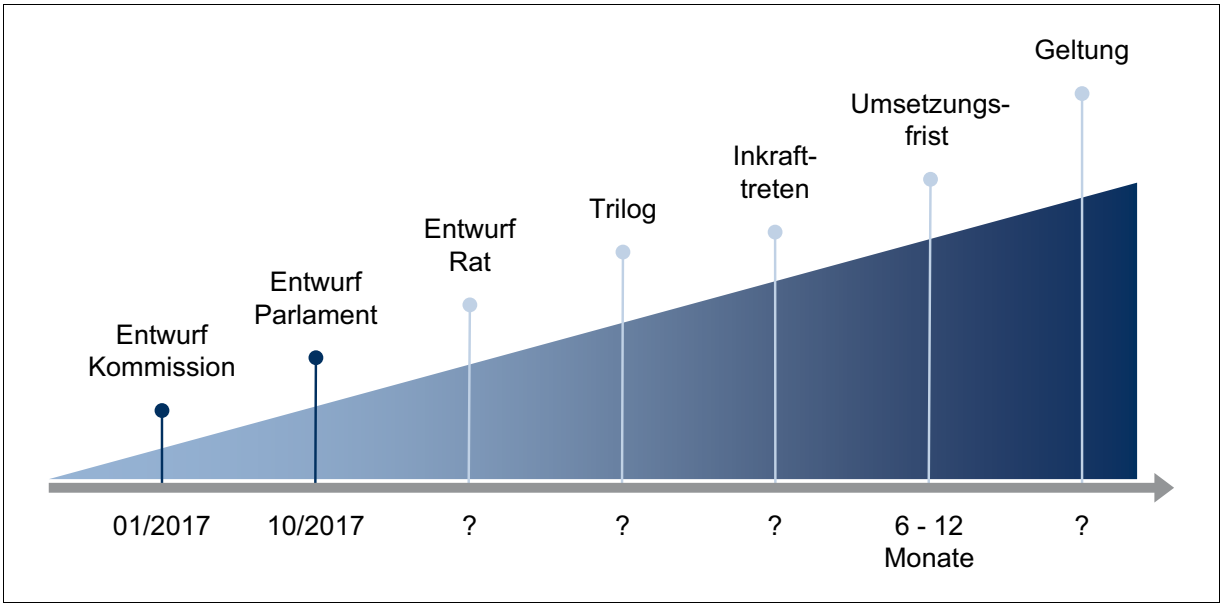

Abb. 6: Zeitplan ePrivacy-Verordnung

Anlass für eine Reform der ePrivacy-Vorgaben ist nicht nur die unterschiedliche Umsetzung der ePrivacy-RL durch die Mitgliedstaaten, sondern auch die uneinheitliche Vollzugspraxis der Aufsichtsbehörden. Vor diesem Hintergrund soll die ePrivacy-RL nicht nur aktualisiert und an die technologischen Fortschritte angepasst werden, sondern auch in Gestalt einer **Verordnung** in Kraft treten**, die** wie die DS-GVO **in allen Mitgliedsstaaten unmittelbar gilt**.

Die ePrivacy-Verordnung soll spezialgesetzliche Regelungen für die Verarbeitung von Kommunikationsdaten enthalten, die **gegenüber der DS-GVO vorrangig** gelten. Zu den wesentlichen Änderungen zählt der **erweiterte Anwendungsbereich der Verordnung**. Die ePrivacy-Verordnung soll neben klassischen Kommunikationsformen wie Telefonie, Fax und SMS auch neue Formen der elektronischen Kommunikation erfassen. Dazu gehören insbesondere **internetbasierte Kommunikationsdienste, sog. Over-The-Top-Dienste (OTT-Dienste) wie E-Mail oder Messenger**.

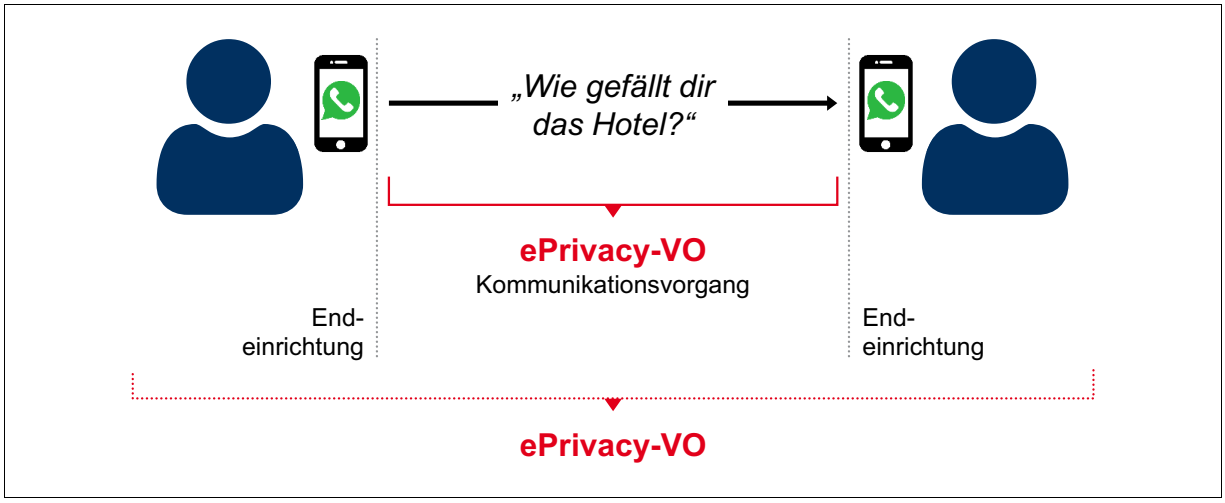

Abb. 7: Schutzbereich ePrivacy-Verordnung

Darüber hinaus soll auch die **Maschine-zu-Maschine-Kommunikation** erfasst werden, um Anwendungen im Bereich Smart Home, Internet of Things oder Connected Car zu regulieren.

Abb. 8: Maschine-zu-Maschine-Kommunikation

Daraus folgt, dass der **Anwendungsbereich der ePrivacy-Verordnung nicht nur auf personenbezogene Daten beschränkt** ist, sondern auch nicht personenbezogene Daten erfasst. In diesem Punkt geht die ePrivacy-Verordnung über den Schutzbereich der DS-GVO hinaus und ergänzt sie.

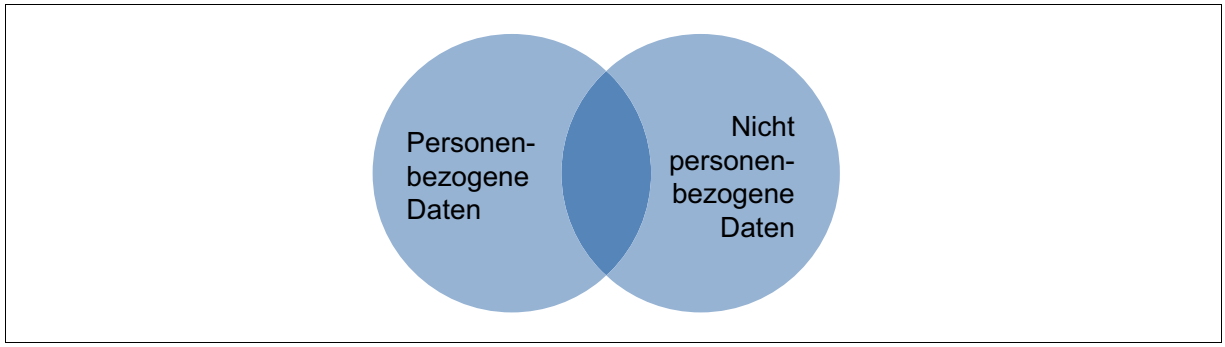

Abb. 9: Personenbezogene und nicht personenbezogene Daten

Die geplante ePrivacy-Verordnung enthält auch in Bezug auf den persönlichen Schutzbereich einen eigenständigen Regelungsgehalt im Vergleich zur DS-GVO. Die DS-GVO schützt ausschließlich personenbezogene Daten natürlicher Personen. Im Gegensatz dazu **soll die ePrivacy-Verordnung auch juristischen Personen schützen**. Dies führt in der Praxis zu einer besonderen Konstellation: Einerseits sind Unternehmen nach der DS-GVO als Verantwortliche zur Einhaltung der Anforderungen verpflichtet. Anderseits zählen sie nach der ePrivacy-Verordnung zugleich zum geschützten Personenkreis. Diese Doppelrolle kann bei aufsichtsbehördlichen Verfahren zu Konfliktsituationen führen.

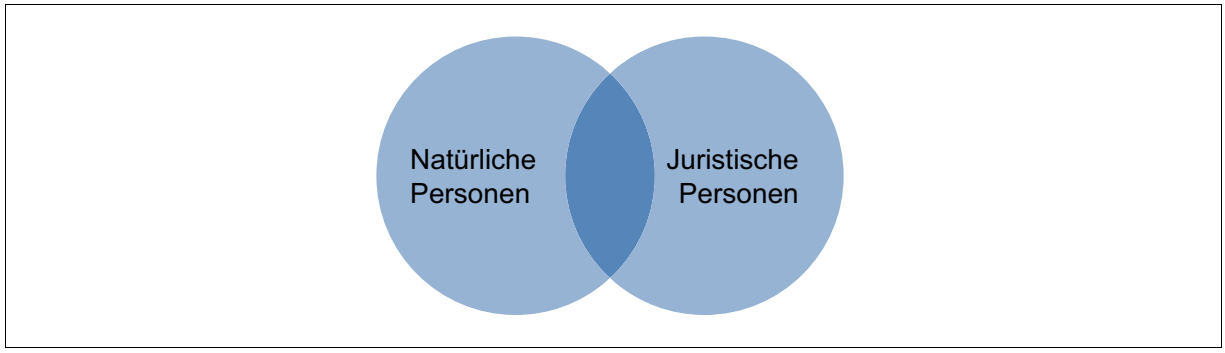

Abb. 10: Persönlicher Schutzbereich

Die Erweiterung des Anwendungsbereichs ist schon lange überfällig, da aufgrund der veralteten Rechtslage erhebliche Schutzlücken beim Einsatz von neuen Kommunikationsmitteln wie z.B. Messengern bestehen.

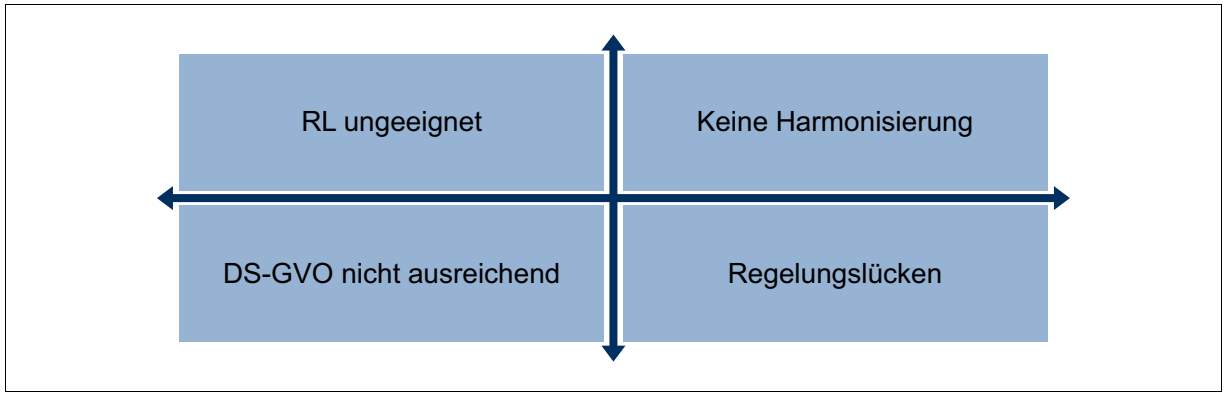

Abb. 11: Gründe für Reform der ePrivacy-Richtlinie

Anhand des folgenden Praxisbeispiels wird deutlich, wie notwendig es ist, die Vertraulichkeit der Kommunikation auch auf juristische Personen auszuweiten und technologieneutral zu regeln.

Praxisbeispiel

Ein Journalist, der sich einem Investigativ-Rechercheverbund angeschlossen hat, recherchiert zu illegalen Steuersparmodellen. Für die Recherche nutzt der Journalist sein Smartphone und seinen Laptop. Auf den Endgeräten befinden sich eine Vielzahl von Fotos und Notizen aus Interviews und ausgewerteten Quellen. Zum Austausch von Informationen versendet der Journalist E-Mails und Nachrichten über Messenger.

Die journalistische Arbeit wäre nicht möglich, ohne dass die Vertraulichkeit der Kommunikation gewährleistet ist. Sämtliche Kommunikationspartner müssen darauf vertrauen, dass nicht nur die Nachrichteninhalte vertraulich bleiben, sondern auch die Umstände der Kommunikation. Dazu zählt beispielsweise, zu welcher Zeit, zwischen welchen Kommunikationspartnern, von welchem Standort kommuniziert wurde, welche Fotos oder sonstige Dateien verschickt wurden und wann die Nachrichten empfangen, verschickt und gelesen wurden.

Dieser Anwendungsfall erstreckt sich aber nicht nur auf die jeweiligen Beteiligten, sondern umfasst auch weitere Grundrechte und Grundfreiheiten.

Das Beispiel verdeutlicht, dass ohne die Vertraulichkeit der Kommunikation eine journalistische Arbeit nahezu unmöglich wäre, da der Quellenschutz nicht sichergestellt wäre. Daraus ergeben sich unmittelbare Folgen für die Pressefreiheit. Ohne Gewährleistung der Pressefreiheit können weitergehende Grundrechte wie Meinungs- und Informationsfreiheit auch anderer Grundrechtsträger nicht umfassend gewährleistet werden.

Die Vertraulichkeit der Kommunikation gem. Art. 7 GRCh ist daher für die Wahrung weiterer Grundrechte unabdingbar.

2.2 Nationales Recht

2.2.1 Bundesdatenschutzgesetz (BDSG)

Das **BDSG** wurde aufgrund der DS-GVO umfassend angepasst. Bei der Reform des BDSG wurden nicht nur Vorschriften entfernt, die im Widerspruch zur DS-GVO standen. Darüber hinaus wurden Öffnungsklauseln und Regelungsaufträge der DS-GVO umgesetzt.

Für nichtöffentliche Stellen im Zusammenhang mit der Nutzung von Online-Diensten sind insbesondere die Regelungen für besondere Verarbeitungssituationen, z.B. im Beschäftigtenverhältnis (§ 26 BDSG), relevant. Darüber hinaus sind die BDSG-Vorschriften, die Einschränkungen und Ausnahmen zu den Betroffenenrechten gem. Art. 12 ff. DS-GVO enthalten, von besonderer Bedeutung.

2.2.2 Telekommunikationsgesetz (TKG)

Das **TKG** enthält **bereichsspezifische Regelungen zur Telekommunikation** und stellt im Wesentlichen eine Umsetzung der ePrivacy-Richtlinie dar. Das TKG **gilt nur für Anbieter von Telekommunikationsdiensten**. Darunter fallen die klassischen Provider, wie z.B. Telekom, Vodafone oder O2. Ein Kommunikationsdienst unterliegt nur dann den Regelungen des TKG, wenn der Dienst ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze besteht.

4.7 Praxisbeispiele für die Gestaltung von Cookie-Bannern und rechtliche Bewertung

Beispiel 1

Wir verwenden Cookies, um Ihnen den bestmöglichen Service zu gewährleisten.
Wenn Sie auf der Seite weitersurfen, stimmen Sie der Cookie-Nutzung zu.

✖

Ich stimme zu

Bewertung

- Nutzer hat keine Wahlmöglichkeit. Es fehlt Auswahl zwischen JA und NEIN [29]
- Verlinkung zu vollständiger Datenschutzerklärung fehlt
- Hinweis auf konkrete Verarbeitungszwecke fehlt
- Hinweis auf Widerrufsrecht fehlt
- Es handelt sich um ein verbreitetes Beispiel, welches häufig auf Websites eingesetzt wird. Selbst wenn der Nutzer nicht auf den Button klickt, sondern weitersurft, soll er eine Einwilligung erteilt haben. Bloßes „Weitersurfen“ ist aber keine aktive Handlung des Nutzers, die eine Einwilligung ausdrückt.

Beispiel 2

Deine Privatsphäre ist uns wichtig!
Deine Privatsphäre ist uns wichtig! Um dich ausführlich beraten und für dich ausgewählte Empfehlungen aussprechen zu können, nutzen wir auf unserer Seite Cookies. In den **Privatsphäre Einstellungen** kannst du einsehen, welche Dienste wir einsetzen, und dich über die **Datenschutzrichtlinie** informieren.

✖

Ich bin einverstanden

Bewertung

- Nutzer hat keine Wahlmöglichkeit. Es fehlt Auswahl zwischen JA und NEIN
- Nutzer erfährt nicht, worein er konkret einwilligt. Angaben zu den Verarbeitungs-tätigkeiten sind zu oberflächlich.
- Hinweis auf Widerrufsrecht fehlt

- Verlinkung auf umfassende Datenschutzerklärung

29 Zur (umstrittenen) Zulässigkeit sog. Cookie Walls/Pay Walls vgl. Abschnitt 3.4.2 dieses Ratgebers sowie Beispiel 6 in diesem Abschnitt.

Stichwortverzeichnis