Stellungnahme zu rechtlichen Aspekten eines Einwilligungsassistenten

Prof. Dr. Anne Riechert
Stiftung Datenschutz / Frankfurt University of Applied Sciences

Stand: Dezember 2016

Inhaltsverzeichnis

Inhaltsverzeichnis

Abrufdatum der Internetlinks in Teil B: 24. Februar 2017

A. Einführung

I. Allgemein

Im Fokus dieser rechtlichen Stellungnahme stehen technische Konzepte, die zum Ziel haben, Nutzer (als im datenschutzrechtlichen Sinne „betroffene Personen“) bei Ausübung ihrer Einwilligung automatisiert zu unterstützen. Hierbei soll die Zustimmung für unterschiedliche Datenverarbeitungsprozesse und Empfänger im Voraus erteilt werden. Im Folgenden werden die zugrunde liegenden Prozesse auch als „Einwilligungsassistenten“ bezeichnet.

Die Prüfung orientiert sich hierbei an den technischen Möglichkeiten, die das Projekt „LETsmart“ und die Plattform „CoMaFeDS“ bieten.[1]

In die Betrachtung fließen ebenso grundsätzliche rechtliche Erwägungen zur Anwendbarkeit und Auslegung der Datenschutz-Grundverordnung mit ein, um hieraus insgesamt und nicht nur für den Einwilligungsassistenten Handlungsempfehlungen für die Voraussetzungen der Einwilligung entwickeln zu können. Zudem erfolgen Darstellungen zur angewandten Praxis der so genannten Cookie-Richtlinie, da dies zum einen für die Auslegung der Einwilligungsvoraussetzungen relevant ist aber zum anderen für die Entwickler ein Prüfungsansatz darstellen soll, ob ihre Konzepte auf diese Einwilligungsprozesse ausgedehnt werden können. Denn nicht nur der Grundsatz „Datenschutz durch Technikgestaltung“ gemäß Artikel 25 Datenschutz-Grundverordnung fordert zur Entwicklung datenschutzgerechter technischer Lösungen auf, sondern die Artikel-29-Datenschutzgruppe hat ebenso zur Vorlage technischer Mittel zur Einhaltung des Rechtsrahmens bei Cookies aufgerufen.[2]

Da sich die Konzepte „LETsmart“ und „CoMaFeDS“ hinsichtlich möglicher Einsatzzwecke und Anwendungsgebiete in der Entwicklung befinden und Details teilweise der Geheimhaltung unterliegen, kann diese Stellungnahme darüber hinaus keine abschließende Begutachtung darstellen.

Insgesamt werden ausschließlich rechtliche und keine technischen Bewertungen vorgenommen.

1 *Siehe Studie der Stiftung Datenschutz, Kapitel II. 2.*

2 *Bei der Artikel-29-Datenschutzgruppe handelt es sich um ein unabhängiges Beratungsgremium der Europäischen Kommission und setzt sich aus Vertretern der nationalen Datenschutzbehörden, dem Europäischen Datenschutzbeauftragten sowie der Europäischen Kommission zusammen. Zu der gerade zitierten Aufforderung: Artikel-29-Datenschutzgruppe, WP 171 Stellungnahme 2/2010 zur Werbung auf Basis von Behavioural Targeting, angenommen am 22. Juni 2010, S. 27.*

II. Technische Konzepte

Zunächst werden nun in abstrakter Weise die Ziele und Funktionen der geplanten „Einwilligungsassistenten“ nochmals zusammengefasst (nähere Beschreibungen und Details sind in der Bestandsaufnahme der Studie enthalten):

Der Nutzer[3] soll im Vorhinein Vorgaben erteilen,
- welche Daten
- an welche Empfänger
- zu welchem Zweck

weitergegeben werden.

Ein System speichert die Daten der betroffenen Person entweder dezentral (bei der betroffenen Person) oder zentral (Cloud). „LETsmart“ bezeichnet die dezentrale Speicherung als „Datentresor“, über den der Nutzer die Kontrolle ausübt.

Das System ist darüber hinaus in der Lage, Datenschutzhinweise der Empfänger in eine maschinenlesbare Form zu übersetzen und die darin enthaltenen Angaben in Form einer Liste zusammenzufassen, so dass die betroffene Person die Möglichkeit hat, in die Verarbeitung der dort aufgezählten Daten, Zwecke und Empfänger detailliert einzuwilligen. Bei der Plattform „CoMaFeDS“ wird dies wie folgt beschrieben: „Potenzielle Empfänger der Daten sowie mögliche Verarbeitungszwecke sollen kategorisiert werden, indem Datenschutzerklärungen in definierten Formaten, die eine kurz gefasste Spezifikation von Kategorien und Empfängern beinhalten, dargestellt werden. Das gewählte Format muss außerdem willkürliche Detailstufen in den betrachteten Datenschutzerklärungen erlauben, so dass Definitionen von zahlreichen Unterkategorien möglich sind. Dies würde etwa Zustimmungen erlauben wie „Meine Daten dürfen von unterschiedlichen Forschungsinstitutionen für den Zwecke von demografischen Untersuchungen verarbeitet werden, aber nicht durch Regierungsbehörden für Steuerschätzungen“[4].

„LETsmart“ ist zunächst darauf ausgelegt, im Rahmen eines einzigen laufenden Vertragsverhältnisses zwischen betroffener Person und dem Vertragspartner die Einwilligungserklärungen automatisiert zu unterstützen, wobei nach Wegfall des Verwendungszwecks die Daten automatisiert gelöscht werden. Eine Erweiterung ist jedoch dahingehend geplant, dass auch die Datenschutzhinweise mehrerer Vertragspartner automatisiert in entsprechende Einwilligungserklärungen „übersetzt“ werden könnten.
Die Plattform „CoMaFeDS“ verfolgt aktuell, das Wissen über vorhandene Einwilligungserklärungen von betroffenen Personen auf einer zentralen Plattform bereitzustellen. Empfänger erhalten zunächst nur die Information, dass eine kompatible Einwilligungserklärung vorliegt, jedoch noch keine Information über die betroffene Person. Die Übereinstimmung soll automatisiert geprüft werden und die betroffene Person eine entsprechende Rückmeldung erhalten.

3 Im Verlauf dieser rechtlichen Stellungnahme wird die im datenschutzrechtlichen Sinne betroffene Person entweder als „Nutzer“ oder als „betroffene Person“ bezeichnet.

4 Siehe Studie der Stiftung Datenschutz, Kapitel II. 2.

Entsprechende Vorhaben gab es bereits in der Vergangenheit, wie beispielsweise P3P oder Sticky Policies, an denen sich diese Projekte teilweise orientieren: Bei den so genannten „Sticky Policies“ werden persönliche Daten, die die betroffene Person zuvor im Hinblick auf Zwecke und Konditionen spezifiziert hat, vom System des Datenhalters erfasst, verschlüsselt und diese Vorgaben in eine standardisierte Datenschutzerklärung umgewandelt. P3P verfolgt den Sticky Policy-Ansatz.[5] Die betroffenen Personen nehmen Voreinstellungen bezüglich der von ihnen präferierten Datennutzung vor.[6]

Weiterhin ist „CoMaFeDS“ von dem Wissen abhängig, wo spezifische Datensätze zu finden sind. Um dieses Problem zu lösen, soll eine detaillierte Beschreibung der Datensätze erfolgen. Für jede mögliche Datenquelle soll ein maschinenlesbares Dokument vorliegen, das spezifiziert, wo ein jeweiliges Datum liegt. Außerdem sollen für jeden Datensatz detaillierte Präferenzen verfügbar sein, und zwar bezogen auf die vielfältigen Verarbeitungsprozesse sowie Empfänger. Basierend auf diesen Dokumentationen führt „CoMaFeDS“ interne Konvertierungen durch und die Datenbank- und Datensatzbezogenen Informationen und Spezifikationen werden genutzt, um einen ontologisch-basierten „Wissensgraph“ zu entwickeln. Dieser Graph verschlüsselt das Wissen über den Speicherort und die Zugriffsmöglichkeiten zu den spezifischen Datensätzen („wo diese zu finden sind, um welche Art von Daten es sich handelt und wie diese zu erlangen sind“).

Eine dynamische Einholung der Einwilligungserklärung ist geplant.
Offen, aber besonders interessant ist, ob diese technischen Möglichkeiten mit bereits angebotenen Diensten wie DigiMe (siehe Bestandsaufnahme) oder Konzepten wie MyData (siehe Bestandsaufnahme) zukünftig kombiniert werden können, so dass in Bezug auf mehrere Empfänger ein automatisierter Datenaustausch erfolgen könnte.

B. Ziel und Vorgehensweise

Die Datenschutz-Grundverordnung schafft einen einheitlichen Rechtsrahmen und stellt Anforderungen an die Umsetzung von transparenten Systemen. In Artikel 25 Datenschutz-Grundverordnung wird der Grundsatz „Datenschutz durch Technikgestaltung“ eingeführt. Dementsprechend sind bereits bei der Entwicklung und Gestaltung von technischen Funktionen datenschutzrechtliche Anforderungen zu berücksichtigen.

Zu untersuchen ist daher, ob die unter dem vorangegangen Punkt A. dargestellten Konzepte den rechtlichen Vorgaben der ab Mai 2018 geltenden Datenschutz-Grundverordnung entsprechen, welche Anforderungen bei der Technikgestaltung zu beachten sind und ob insgesamt im Hinblick auf die Einwilligungsvoraussetzungen der einheitliche Rechtsrahmen gewahrt wird. Gemäß Erwägungsgründen 10 und 13 Datenschutz-Grundverordnung sollte das Schutzniveau für die Rechte und Freiheiten von natürlichen Personen bei der Verarbeitung personenbezogener Daten in allen Mitgliedstaaten gleichwertig und es sollten gleichmäßige Kontrollen und gleichwertige Sanktionen gewährleistet sein.

5 Siehe unter https://www.datenschutzzentrum.de/projekte/p3p/P3P_AK-IT.pdf

6 P3P wird jedoch vom Windows-Browser seit der Version Windows 10 nicht mehr unterstützt (siehe in der Bestandsaufnahme der Studie). Bei „CoMaFeDS“ soll allerdings anders als bei „Sticky Policies“ keine vertrauenswürdige Instanz erforderlich, die den Schlüssel für die Entschlüsselung der Datensätze verwahrt und an die interessierte Institutionen ihre Anfrage zur Datennutzung stellen.

Unter dem nachfolgenden Punkt C. erfolgt zunächst die Darstellung der rechtlichen Voraussetzungen und der Anforderungen an eine rechtmäßige Datenverarbeitung. Vergleichend wird hierbei auf die aktuell geltende EU-Datenschutzrichtlinie (95/46/EG) Bezug genommen.[7] Außerdem wird die praktische Umsetzung der so genannten Cookie-Richtlinie anhand von Beispielen erläutert, um damit gleichermaßen die Einwilligungsvoraussetzungen und zugrundeliegenden Rechtsauffassungen näher beleuchten und Empfehlungen aussprechen zu können.

Zudem werden unter Punkt C. die Einwilligungsvoraussetzungen für elektronische Kommunikationsdienste und Dienste der Informationsgesellschaft sowie die Regelungen des Telekommunikations- und des Telemediengesetzes dahingehend diskutiert, ob deren Intentionen weiterhin Geltung beanspruchen können oder durch die Datenschutz-Grundverordnung vollständig abgelöst werden. Dies geschieht zum einen im Hinblick auf Anbieter von elektronischen Telekommunikationsdiensten oder von Diensten der Informationsgesellschaft, bei denen im Zusammenhang mit ihren Dienstleistungen ebenso die Verwendung eines Einwilligungsassistenten denkbar wäre. Zum anderen ist zum jetzigen Zeitpunkt des technischen Entwicklungsstands noch nicht absehbar, ob die in dieser Stellungnahme geprüften Konzepte darüber hinaus als eigenständige Dienste eingestuft werden könnten (im Sinne eines elektronischen Kommunikationsdienstes oder Dienstes der Informationsgesellschaft).

Unter D. wird sodann die Relevanz der unter C. festgestellten Ergebnisse für die so genannten Einwilligungsassistenten geprüft, wobei Empfehlungen in Bezug auf die Auslegung der Regelungen der Datenschutz-Grundverordnung eingebunden sind.

Unter E. werden Fragen der „Verantwortung und Haftung“ behandelt und unter Punkt F. erfolgen Überlegungen zu zukünftigen Problemstellungen von automatisierten Entscheidungen.
Zusammenfassungen zur rechtlichen Bewertung des Einwilligungsassistenten sowie Handlungsempfehlungen werden abschließend in den Punkten G. und H. dargestellt.

7 *Um die Vollharmonisierung ab Inkrafttreten der Datenschutz-Grundverordnung sicherzustellen, sollte frühzeitig mit der Prüfung begonnen werden, ob und in welchem Umfang eine unterschiedliche Interpretation der Datenschutz-Grundverordnung durch die Mitgliedstaaten und Vorgehensweise in der Praxis in Betracht kommen und dem in den Grundsätzen der Datenschutz-Grundverordnung geforderten gleichwertigen Datenschutzniveau entgegenstehen könnte. Die Richtlinie 95/46/EG enthält teilweise identische Begriffe und könnte daher für die Einschätzung hilfreich sein, ob abweichende Definitionen in den einzelnen Mitgliedstaaten auch zukünftig im Hinblick auf die Datenschutz-Grundverordnung zu erwarten sein könnte. Siehe auch Studie zur Umsetzung der Richtlinie 95/46/EG unter http://ec.europa.eu/justice/policies/privacy/docs/lawreport/consultation/technical-annex_en.pdf („Analysis and impact study on the implementation of Directive EC 95/46 in Member States“). Ferner ist der Vergleich aufgrund der Regelung in Erwägungsgrund 171 Datenschutz-Grundverordnung relevant. Danach ist nicht erforderlich, dass die betroffene Person erneut ihre Einwilligung erteilt, wenn die Art der bereits erteilten Einwilligung den Bedingungen der Datenschutz-Grundverordnung entspricht, so dass der Verantwortliche die Verarbeitung nach dem Zeitpunkt der Anwendung der Datenschutz-Grundverordnung fortsetzen kann. Siehe hierzu außerdem Düsseldorfer Kreis, Beschluss vom 13./14.09.2016 zur Fortgeltung bisher erteilter Einwilligungen unter der Datenschutz-Grundverordnung, https://www.ldi.nrw.de/mainmenu_Service/submenu_Entschliessungsarchiv/Inhalt/Beschluesse_Duesseldorfer_Kreis/Inhalt/2016/Fortgeltung_bisher_erteilter_Einwilligungen_unter_der_Datenschutz-_Grundverordnung/Fortgeltung_bisher_erteilter_Einwilligungen_unter_der_Datenschutz-_Grundverordnung1.pdf*

C. Voraussetzungen der Einwilligung

Für die Verarbeitung personenbezogener Daten normiert Artikel 6 Datenschutz-Grundverordnung[8] als allgemeinen Grundsatz das sogenannte Verbotsprinzip mit Erlaubnisvorbehalt. Demnach ist die Verarbeitung von personenbezogenen Daten nur zulässig, wenn eine Einwilligung vorliegt oder eine andere in dieser Vorschrift geregelte Ausnahme vorliegt. Dies entspricht weiterhin den Vorgaben der EU-Datenschutzrichtlinie 95/46/EG.[9] Dort knüpfen Artikel 7 sowie Art. 8 Abs. 1 EG-Datenschutzrichtlinie die Verarbeitung personenbezogener Daten an bestimmte Voraussetzungen. Darüber hinaus sind in Artikel 6 der Datenschutzrichtlinie für elektronische Kommunikation Anforderungen bezüglich der Einwilligung enthalten.[10]

Für das Projekt und vorliegende Gutachten ist insgesamt die Einwilligung als Zulässigkeitsvoraussetzung für eine rechtmäßige Datenverarbeitung von Relevanz. Daher werden im Folgenden die hierfür relevanten Regelungen näher dargestellt.

I. Die Einwilligung im Gemeinschaftsrecht

1. Richtlinie 95/46/EG und Datenschutz-Grundverordnung

Artikel 7a) der EU-Datenschutzrichtlinie 95/46/EG, die gemäß Artikel 94 Datenschutz-Grundverordnung mit Wirkung vom 25. Mai 2018 aufgehoben wird, erlaubt die Verarbeitung personenbezogener Daten unter anderem dann, wenn die betroffene Person „ohne jeden Zweifel ihre Einwilligung gegeben“ hat. Hier sollen die denkbar höchsten Anforderungen an die Zweifelsfreiheit gelten, da diese Formulierung keine relativierenden oder einschränkenden Adjektive enthalte.[11]

Diese Anforderung „ohne jeden Zweifel“ ist in der Datenschutz-Grundverordnung nicht mehr enthalten. Gemäß Artikel 6 Absatz 1a) der Datenschutz-Grundverordnung ist die Datenverarbeitung nunmehr rechtmäßig, „wenn die betroffene Person ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben hat.“

8 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung); http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679&from=DE

9 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, Amtsblatt Nr. L 281 vom 23.11.1995, S. 31 – 50.

10 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation); Amtsblatt Nr. L 201 vom 31.07.2002, S. 37 - 47.

11 Philip Radlanski, Das Konzept der Einwilligung in der datenschutzrechtlichen Realität, S. 43. Siehe außerdem Brühann: in Grabitz/Hilf, Das Recht der Europäischen Union, 40. Auflage 2009, Loseblattsammlung, Stand: Mai 1999 Ergänzungslieferung 13, Artikel 2 Begriffsbestimmungen „Einwilligung der betroffenen Person“ mit dem Hinweis, dass der Bezug auf den ausdrücklichen Charakter der Einwilligung gestrichen wurde, um zu verhindern, dass dies als Erfordernis einer schriftlichen Erklärung ausgelegt werde.

Insgesamt haben sich im Verlauf der Verhandlungen zur Datenschutz-Grundverordnung bei der Definition der Einwilligung weder die ursprünglich geforderte „explizite“[12] oder „ausdrückliche“[13] Willensbekundung noch die Formulierung „ohne jeden Zweifel“[14] durchsetzen können. Die Artikel-29-Datenschutzgruppe hat schon im Verlaufe der Verhandlungen zur Datenschutz-Grundverordnung angemerkt, dass die Beibehaltung von “explicit” im Rahmen der Einwilligung eine wichtige Klarstellung bedeutet, die notwendig ist, um den betroffenen Personen die Ausübung ihrer Rechte zu ermöglichen.[15] Dennoch wurde in der englischen Originalfassung der Datenschutz-Grundverordnung der Begriff „explicit“ in der Endfassung durch „unambiguous“ ersetzt.[16] Lediglich gemäß Erwägungsgrund 32 der Datenschutz-Grundverordnung „sollte“ eine Einwilligung „unmissverständlich“ („unambiguous“) durch eine bestätigende Handlung bekundet sein. Im Verordnungstext selbst (siehe Artikel 6 Absatz 1a) der Datenschutz-Grundverordnung) ist diese Verpflichtung jedoch nicht enthalten. Ergänzend anzumerken ist, dass in der deutschen Fassung des Berichts des LIBE-Ausschusses vom 22.11. der Begriff „explicit“ nicht mehr wie zuvor mit „explizit“, sondern nunmehr mit „ausdrücklich“ übersetzt und als Änderung markiert wurde, obwohl in der Originalfassung weiterhin „explicit“ verwendet und keine begriffliche Abwandlung vorgenommen wurde. Dieser Begriff wurde bereits in der Vergangenheit unterschiedlich übersetzt.[17]

Eine ausdrückliche Einwilligung ist gemäß Artikel 9 Absatz 2a) Datenschutz-Grundverordnung nur bei besonderen Kategorien von personenbezogenen Daten für die Verarbeitung erforderlich.[18]

12 *Siehe Artikel 4 Nr. 8 in Datenschutz-Grundverordnung der EU-Kommission vom 25.1.2012, KOM(2012) 11 endgültig 2012/0011 (COD) - Vorschlag für Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung): http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf*

13 *Siehe Artikel 4 Nr. 8 gemäß LIBE-Ausschuss - Bericht über den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (allgemeine Datenschutzverordnung)(COM(2012)0011 – C7-0025/2012 – 2012/0011(COD), - dieser Vorschlag erfolgte in Kenntnis des Berichts des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres sowie der Stellungnahmen des Ausschusses für Beschäftigung und soziale Angelegenheiten, des Ausschusses für Industrie, Forschung und Energie, des Ausschusses für Binnenmarkt und Verbraucherschutz und des Rechtsausschusses -; http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2013-0402+0+DOC+PDF+V0//DE*

14 *Interinstitutionelles Dossier mit dem Hinweis, dass „explizit“ unrealistisch sei – Siehe Rat der Europäischen Union 31.Mai 2013 10227/13 Interinstitutionelles Dossier 2012/0011 (COD) ; Betr.: Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) – Kernfragen zu den Kapiteln I-IV; http://register.consilium.europa.eu/doc/srv?l=DE&f=ST%2010227%202013%20INIT*

15 *Artikel-29-Datenschutzgruppe, WP 199 “Opinion 08/2012 providing further input on the data protection reform discussions”, adopted on 5 October 2012, S. 7: The Working Party understands that doubts have been raised as to the feasibility of the word “explicit” in the context of consent in Article 4 (8). The Working Party is of the opinion that the inclusion of the word “explicit” is an important clarification in the text, which is necessary to truly enable data subjects to exercise their rights, especially on the Internet where there is now too much improper use of consent. It would be highly undesirable should this important clarification be deleted from the text.*

16 *Siehe http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2013-0402+0+DOC+PDF+V0//EN und http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2013-0402+0+DOC+PDF+V0//DE*

17 *Auf die unterschiedliche Auslegung von „explicit“ wird im Folgenden näher Bezug genommen werden, siehe S. 37 ff.*

18 *Gemäß Artikel 9 Absatz 1 Datenschutz-Grundverordnung (Verarbeitung besonderer Kategorien personenbezogener Daten) ist 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 untersagt. Die Definitionen von genetischen Daten, biometrischen Daten sowie Gesundheitsdaten sind in Artikel 4 Nr. 13, 14 und 15 Datenschutz-Grundverordnung geregelt. Zur näheren Auslegung dieser Daten sind ebenso die Erwägungsgründe 34, 35 und 51 heranzuziehen.*

2. Richtlinie 2002/58/EG

(1) Verkehrsdaten und Standortdaten

Weitere Voraussetzungen einer Einwilligung sind in Artikel 6 Abs. 3 der Richtlinie 2002/58/EG für elektronische Kommunikation hinsichtlich Verkehrsdaten enthalten.[19]

Danach ist die Verarbeitung von Verkehrsdaten[20] zum Zwecke der Bereitstellung von Diensten mit Zusatznutzen oder zum Zwecke der Vermarktung elektronischer Kommunikationsdienste lediglich mit der Einwilligung des betroffenen Nutzers oder Teilnehmers möglich. Die Legaldefinition des öffentlich zugänglichen elektronischen Kommunikationsdiensts regelt Artikel 2 c) Rahmenrichtlinie 2002/21/EG[21].

Dabei handelt es sich um gewöhnlich gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über elektronische Kommunikationsnetze bestehen, einschließlich Telekommunikations- und Übertragungsdienste in Rundfunknetzen, ausgenommen jedoch Dienste, die Inhalte über elektronische Kommunikationsnetze und –dienste anbieten oder eine redaktionelle Kontrolle über sie ausüben. Es gehören keine Dienste der Informationsgesellschaft im Sinne von Artikel 1 der Richtlinie 98/43/EG dazu, die nicht ganz oder überwiegend in der Übertragung von Signalen über elektronische Kommunikationsnetze bestehen. Insgesamt betreffen die Verkehrsdaten daher den Vorgang der Übertragung, nicht den Inhalt der Nachricht, da die Richtlinie 2002/58/EG die telekommunikationsrechtliche Materie regelt.[22]

Der Dienst mit Zusatznutzen, auf den sich Artikel 6 Absatz 3 der Richtlinie 2002/58/EG ebenso bezieht, wird gemäß Artikel 2 g) dieser Richtlinie definiert als „jeder Dienst, der die Bearbeitung von Verkehrsdaten oder anderen Standortdaten als Verkehrsdaten in einem Maße erfordert, das über das für die Übermittlung einer Nachricht oder die Fakturierung dieses Vorgangs erforderliche Maß hinausgeht." Beispielhaft werden hierzu in Erwägungsgrund 18 die Beratung hinsichtlich der billigsten Tarifpakete, Navigationshilfen, Verkehrsinformationen, Wettervorhersage oder touristische Informationen genannt. Die damit verbundenen Standortdaten[23], die keine Verkehrsdaten sind, dürfen gemäß Artikel 9 Absatz 1 der Richtlinie 2002/58/EG nur anonymisiert oder mit der Einwilligung des Nutzers zur Bereitstellung von Diensten mit Zusatznutzen verarbeitet werden.

(2) Informationen, die bereits im Endgerät des Nutzers gespeichert sind

Zudem sieht die Richtlinie 2002/58/EG (in der Fassung 2009/136/EG)[24] für Informationen, die bereits im Endgerät des Nutzers gespeichert sind („Cookies"), folgende Regelung vor (Artikel 5 Absatz 3):

19 *Richtlinie 2002/58/ÆG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation); Amtsblatt Nr. L 201 vom 31.07.2002, S. 37 - 47.*

20 *Siehe Artikel 2b) der Richtlinie 2002/58/ÆG.*

21 *Richtlinie 2002/21/ÆG des Europäischen Parlaments und des Rates vom 7. März 2002 über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste (Rahmenrichtlinie) , Amtsblatt Nr. L 108 vom 24.04.2002 S. 33 – S. 50.*

22 *Siehe hierzu auch die Ausführungen zur Inhaltsneutralität einer Nachricht bei Peukert in: Teplitzky/Pfeifer/Leistner, UWG, Großkommentar zum Gesetz gegen den unlauteren Wettbewerb mit Nebengesetzen, Band 1: Einleitung; 2. Auflage 2013, §§ 1- 3, Rn. 510 (S. 882).*

23 *Siehe Artikel 2c) der Richtlinie 2022/58/ÆG.*

24 *Richtlinie 2009/136/ÆG des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/22/ÆG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/ÆG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz, Amtsblatt Nr. L 337 vom 18.12.2009, S. 11 - 36.*

„Die Mitgliedstaaten stellen sicher, dass die Speiche¬rung von Informationen oder der Zugriff auf Informationen, die bereits im Endgerät eines Teilnehmers oder Nutzers gespeichert sind, nur gestattet ist, wenn der betreffende Teil¬nehmer oder Nutzer auf der Grundlage von klaren und umfassenden Informationen, die er gemäß der Richtlinie 95/46/EG u. a. über die Zwecke der Verarbeitung erhält, seine Einwilligung gegeben hat."

Gemäß Artikel 2f) der Richtlinie 2002/58/EG stellt eine „Einwilligung" eines Nutzers oder Teilnehmers die Einwilligung der betroffenen Person im Sinne von Richtlinie 95/46/EG dar. Die entsprechende Definition der Einwilligung der betroffenen Person regelt die Datenschutzrichtlinie 95/46/EG in Artikel 2h): „Im Sinne dieser Richtlinie bezeichnet der Ausdruck „Einwilligung der betroffenen Person" jede Willensbekundung, die ohne Zwang für den konkreten Fall und in Kenntnis der Sachlage erfolgt und mit der die betroffene Person akzeptiert, dass personenbezogene Daten, die sie betreffen, verarbeitet werden."

II. Die Einwilligung unter Berücksichtigung der Datenschutz-Grundverordnung

1. Elektronische Kommunikationsdienste[25]

(1) Richtlinie 2002/58/EG

Gemäß Erwägungsgrund 173[26] soll die Richtlinie 2002/58/EG entsprechend geändert werden, um das Verhältnis zur Datenschutz-Grundverordnung klarzustellen. Diese Überarbeitung der so genannten e-Privacy-Richtlinie findet zurzeit statt (Stand: Dezember 2016).

Artikel 95 Datenschutz-Grundverordnung regelt dies wie folgt:
„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."

Die Datenschutz-Grundverordnung enthält zur Verarbeitung personenbezogener Daten in Verbindung mit der Bereitstellung elektronischer Kommunikationsdienste keine gesonderten Regelungen. Sie erlaubt den Mitgliedstaaten lediglich hinsichtlich der Voraussetzungen für eine rechtmäßige Datenverarbeitung gemäß Artikel 6 Absatz 2 die Einführung konkreter Bestimmungen in Bezug auf die Verarbeitung zur Erfüllung von Absatz 1c und e.[27]

25 *Aufgrund des jetzigen Entwicklungsstandes ist noch offen, ob der Einwilligungsassistent als (Teil) eines elektronischen Kommunikationsdienstes oder Dienst mit Zusatznutzen qualifiziert werden könnte (bei dem in diesem Falle selbst Verkehrsdaten anfallen könnten), siehe auch Einleitung sowie S. 21 und S. 55.*

26 *Erwägungsgrund 173: Diese Verordnung sollte auf alle Fragen des Schutzes der Grundrechte und Grundfreiheiten bei der Verarbeitung personenbezogener Daten Anwendung finden, die nicht den in der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates (18) bestimmte Pflichten, die dasselbe Ziel verfolgen, unterliegen, einschließlich der Pflichten des Verantwortlichen und der Rechte natürlicher Personen. Um das Verhältnis zwischen der vorliegenden Verordnung und der Richtlinie 2002/58/EG klarzustellen, sollte die Richtlinie entsprechend geändert werden. Sobald diese Verordnung angenommen ist, sollte die Richtlinie 2002/58/EG einer Überprüfung unterzogen werden, um insbesondere die Kohärenz mit dieser Verordnung zu gewährleisten.*

27 *Artikel 6 Absatz 1c Datenschutz-Grundverordnung betrifft die Rechtmäßigkeit der Verarbeitung, zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, der der Verantwortliche unterliegt. Artikel 6 Absatz 1e Datenschutz-Grundverordnung betrifft die Rechtmäßigkeit der Verarbeitung, die für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde.*

Die Rechtmäßigkeit der Verarbeitung durch Einwilligung gemäß Artikel 6 Absatz 1a Datenschutz-Grundverordnung ist von dieser Ausnahme nicht betroffen, so dass die Voraussetzungen der Datenschutz-Grundverordnung im Hinblick auf die Einwilligung eine abschließende Regelung enthalten. Dies entspricht gleichermaßen der Rechtsauffassung des Europäischen Gerichtshofs, die er zu Artikel 7f Richtlinie 95/46/EG in Bezug auf die angestrebte Vollharmonisierung vertreten hat. Gemäß der Intention des Europäischen Gerichthofs dürfen die Mitgliedstaaten weder neue Grundsätze in Bezug auf die Zulässigkeit der Verarbeitung personenbezogener Daten neben Art. 7 der Richtlinie 95/46/EG einführen, noch zusätzliche Bedingungen stellen, die die Tragweite eines der sechs in diesem Artikel vorgesehenen Grundsätze verändern würden.[28] Überträgt man diesen Gedanken auf die geplante Vollharmonisierung des Datenschutzrechts durch die Datenschutz-Grundverordnung -die keine konkreten Regelungen zur Datenverarbeitung in Verbindung mit elektronischen Kommunikationsdiensten enthält- ist daher fraglich, ob das aktuell geltende Telekommunikationsgesetz[29] zusätzliche Pflichten auferlegt bzw. auferlegen darf, die die Tragweite der Anforderungen an eine Einwilligung ändern.

In Bezug auf die inhaltliche Ausgestaltung der Einwilligung müsste hier die Überprüfung der Anforderungen im Rahmen einer elektronischen Einwilligung gemäß § 94 Telekommunikationsgesetz erfolgen und somit der Maßstab der Datenschutz-Grundverordnung sowie der Richtlinie 2002/58/EG zugrunde gelegt werden.[30] Bei dieser Auslegung können ebenso die Regelungen der Richtlinie 95/46/EG unterstützen. Denn Einwilligung bedeutet gemäß Artikel 2 f der Richtlinie 2002/58/EG eine Einwilligung im Sinne der Richtlinie 95/46/EG. Auch wenn letztere gemäß Artikel 94 Datenschutz-Grundverordnung aufgehoben wird, kann sie einen Hinweis dafür geben, was ursprünglich intendiert war oder nun als zusätzliche Verpflichtung bei Aufrechterhaltung der Voraussetzungen des Telekommunikationsgesetzes verstanden werden könnte.

Gemäß Artikel 94 Telekommunikationsgesetz ist eine elektronische Einwilligung möglich, wenn der Diensteanbieter sicherstellt, dass

1. der Teilnehmer oder Nutzer seine Einwilligung bewusst und eindeutig erteilt hat,
2. die Einwilligung protokolliert wird,
3. der Teilnehmer oder Nutzer den Inhalt der Einwilligung jederzeit abrufen kann und
4. der Teilnehmer oder Nutzer die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann.

28 Urteil des Europäischen Gerichtshofs (Dritte Kammer) vom 24.11.2011 bezüglich „Verarbeitung personenbezogener Daten – Richtlinie 95/46/ÆG – Art. 7 Buchst. f – Unmittelbare Wirkung“, in den verbundenen Rechtssachen C 468/10 und C 469/10 betreffend Vorabentscheidungsersuchen nach Art. 267 AEUV, eingereicht vom Tribunal Supremo (Spanien) mit Entscheidungen vom 15. Juli 2010: Die Vorabentscheidungsersuchen betrafen die Auslegung von Artikel 7f EU-Richtlinie 95/46/ÆG. Vom Europäischen Gerichtshof wurde hinsichtlich der Harmonisierung entschieden, dass die nationalen Rechtsvorschriften nicht auf eine Mindestharmonisierung beschränkt sind, sondern zu einer grundsätzlich umfassenden Harmonisierung führen. Art. 7 der Richtlinie 95/46 sehe eine erschöpfende und abschließende Liste der Fälle vor, in denen eine Verarbeitung personenbezogener Daten als rechtmäßig angesehen werden kann. Diese Auslegung werde durch die Formulierung „lediglich erfolgen darf, wenn eine der folgenden Voraussetzungen erfüllt ist“ in Art. 7 der Richtlinie 95/46 bestätigt, die den erschöpfenden und abschließenden Charakter der in diesem Artikel enthaltenen Liste unterstreicht. Der Europäische Gerichtshof hat insgesamt für Recht erkannt, dass dieser Artikel unmittelbare Wirkung hat und dahin auszulegen ist, „dass er einer nationalen Regelung entgegensteht, die für die Verarbeitung personenbezogener Daten, die zur Verwirklichung des berechtigten Interesses, das von dem für diese Verarbeitung Verantwortlichen oder von dem bzw. den Dritten wahrgenommen wird, denen diese Daten übermittelt werden, erforderlich ist, ohne Einwilligung der betroffenen Person nicht nur verlangt, dass deren Grundrechte und Grundfreiheiten nicht verletzt werden, sondern auch, dass diese Daten in öffentlich zugänglichen Quellen enthalten sind, und damit kategorisch und verallgemeinernd jede Verarbeitung von Daten ausschließt, die nicht in solchen Quellen enthalten sind.“

29 Telekommunikationsgesetz vom 22. Juni 2004 (BGBl. I S. 1190), das durch Artikel 9 des Gesetzes vom 26. 07.2016 (BGBl. I S. 1818) geändert worden ist.

30 Zur Verarbeitung von Verkehrsdaten siehe § 96 Telekommunikationsgesetz und die entsprechende Regelung in Artikel 6 der Richtlinie 2002/58/ÆG.

Erwägungsgrund 17 der Richtlinie 2002/58/EG legt fest, dass „für die Zwecke dieser Richtlinie die Einwilligung des Nutzers oder Teilnehmers unabhängig davon, ob es sich um eine natürliche oder eine juristische Person handelt, dieselbe Bedeutung haben sollte wie der in der Richtlinie 95/46/EG definierte und dort weiter präzisierte Begriff „Einwilligung der betroffenen Person. Die Einwilligung kann in jeder geeigneten Weise gegeben werden, wodurch der Wunsch des Nutzers in einer spezifischen Angabe zum Ausdruck kommt, die sachkundig und in freier Entscheidung erfolgt; hierzu zählt auch das Markieren eines Feldes auf einer Internet-Website."

Damit steht die elektronische Form im Einklang mit der Richtlinie 95/46/EG und der Datenschutz-Grundverordnung, da auch in letzterer keine gegenteiligen Anforderungen oder zusätzliche Pflichten enthalten sind.

Die jederzeitige Widerrufbarkeit gemäß § 94 Nr. 3 Telekommunikationsgesetz entspricht zudem Artikel 6 Absatz 3 der Richtlinie 2002/58/EG und legt dem Diensteanbieter damit keine zusätzlichen Pflichten auf.

Allerdings finden sich in der Richtlinie 2002/58/EG keine Anforderungen an die jederzeitige Abrufbarkeit oder die Protokollierung. Lediglich Artikel 5 Absatz 3 der Richtlinie 2002/58/EG regelt die Zulässigkeit der Verarbeitung von Verkehrsdaten im Zusammenhang mit Nachrichten, wenn es zum Nachweis einer kommerziellen Transaktion oder sonstigen geschäftlichen Nachricht geschieht. Eine Protokollierung von Text und Zeitpunkt der Einwilligung kann zwar den erforderlichen Nachweis gemäß Artikel 5 Absatz 2 und Artikel 7 Absatz 1 Datenschutz-Grundverordnung liefern, aber es könnten im Sinne einer europaweiten Vereinheitlichung gegebenenfalls weitere Methoden einer „Rechenschaftsverpflichtung" in Betracht kommen – was gesondert zu prüfen wäre. Daher kann sich an dieser Stelle ebenso die Ausarbeitung von Verhaltensregeln gemäß Artikel 40 Datenschutz-Grundverordnung empfehlen.[31] Wenn die Verarbeitungstätigkeit in mehreren Mitgliedstaaten betroffen ist, hat die Kommission die Möglichkeit, deren allgemeine Gültigkeit in der Union zu beschließen (Artikel 40 Absatz 7 bis Absatz 10 Datenschutz-Grundverordnung).

Fraglich ist daher, ob die Protokollierung und jederzeitige Abrufbarkeit im Telekommunikationsgesetz als zusätzliche Pflichten aufzufassen sind oder ob diese gerade eine erforderliche Transparenz sicherstellen und von den einzelnen Mitgliedstaaten gesetzlich geregelt werden können. Die Anforderungen an die Transparenz lassen sich nicht immer klar von der Einwilligung trennen.

Die ursprüngliche Intention ergibt sich aus Richtlinie 95/46/EG, auf deren Anforderungen die Richtlinie 2002/58/EG derzeit Bezug nimmt. Diese regelt hierzu zum einen, dass die Einwilligung gemäß Artikel 7a Richtlinie 95/46/EG „ohne jeden Zweifel" erteilt sein muss, was dafür sprechen kann, die Protokollierung regeln zu dürfen. Zum anderen sind in Erwägungsgrund 38 Vorgaben zur Transparenz enthalten. Danach setzt eine Datenverarbeitung nach Treu und Glauben voraus, dass die betroffenen Personen in der Lage sind, das Vorhandensein einer Verarbeitung zu erfahren und außerdem ordnungsgemäß und umfassend über die Bedingungen der Erhebung informiert werden, wenn Daten bei ihnen erhoben werden.

31 Verhaltensregeln, die die Anforderungen an die Rechtmäßigkeit der Datenverarbeitung der Datenverarbeitung präzisieren, können durch Verbände und andere Vereinigungen, die Kategorien von Verantwortlichen und Auftragsverarbeitern vertreten, ausgearbeitet werden (Artikel 40 Absatz 2 Datenschutz-Grundverordnung). Entwürfe der beabsichtigten Verhaltensregeln können der zuständigen Aufsichtsbehörde zur Genehmigung vorgelegt werden, die sie in ein Verzeichnis aufnimmt und veröffentlicht.

Im Vergleich dazu muss gemäß Artikel 4 Nr. 11 und Erwägungsgrund 32 der Datenschutz-Grundverordnung die Einwilligung informiert und unmissverständlich sein und nach Artikel 7 Absatz 1 obliegt dem Verantwortlichen der entsprechende Nachweis, ohne jedoch die konkrete Ausführung zu regeln. Gemäß dem aktuellen Verständnis sind Informationen „jederzeit abrufbar“, wenn sie für den Nutzer ohne großen Suchaufwand ständig zur Nutzung bereitgehalten werden.[32]

Die Abrufbarkeit der Information enthält zudem das Recht auf Auskunft, welches in der Datenschutz-Grundverordnung in Artikel 15 geregelt ist. In dieser Regelung findet sich jedoch ebenso wenig eine Verpflichtung der „jederzeitigen“ Abrufbarkeit. Erwägungsgrund 63 regelt vielmehr, dass eine betroffene Person ein Auskunftsrecht hinsichtlich der sie betreffenden personenbezogenen Daten, die erhoben worden sind, besitzen und dieses Recht problemlos und in angemessenen Abständen wahrnehmen können sollte, um sich der Verarbeitung bewusst zu sein und deren Rechtmäßigkeit überprüfen zu können.

Die Frage ist folglich, ob die oben genannten Regelungen des Telekommunikationsgesetzes tatsächlich über die ursprüngliche Intention der Richtlinie 2002/58/EG in Verbindung mit der Richtlinie 95/46/EG hinausgehen und zusätzliche Pflichten auferlegen, die gemäß Artikel 95 Datenschutz-Grundverordnung nicht beabsichtigt sind - unter der Maßgabe, dass diese hinsichtlich der Einwilligungsvoraussetzungen abschließende Regelungen enthält.

Ähnliche Fragestellungen ergeben sich für die Verarbeitung von Standortdaten. § 98 Telekommunikationsgesetz regelt folgendes:
Werden die Standortdaten für einen Dienst mit Zusatznutzen verarbeitet, der die Übermittlung von Standortdaten eines Mobilfunkendgerätes an einen anderen Teilnehmer oder Dritte, die nicht Anbieter des Dienstes mit Zusatznutzen sind, zum Gegenstand hat, muss der Teilnehmer abweichend von § 94 Telekommunikationsgesetz seine Einwilligung ausdrücklich, gesondert und schriftlich gegenüber dem Anbieter des Dienstes mit Zusatznutzen erteilen.

In der Richtlinie 2002/58/EG sind Regelungen über Standortdaten in Artikel 9 enthalten. Ein Dienst mit Zusatznutzen ist in Artikel 2g sowie Erwägungsgrund 18 definiert und umfasst beispielsweise die Beratung hinsichtlich der billigsten Tarifpakete, Navigationshilfen, Verkehrsinformationen, Wettervorhersage oder touristische Informationen.

Dies bedeutet etwa bei einem Dienst, der Standortdaten zum Zwecke einer Wettervorhersage oder touristischen Informationen an Dritte übermittelt, dass vor der ersten Ortung eine ausdrückliche, gesonderte und schriftliche Einwilligung gegenüber dem Ortungsdiensteanbieter erfolgen muss.[33]

Hier ist fraglich, ob diese Regelung nicht eher dem Teilnehmer als betroffener Person eine „zusätzliche Pflicht“ auferlegt und ob dies ebenso von dem Gedanken des Artikel 95 Datenschutz-Grundverordnung umfasst ist. Außerdem könnten die Erteilung der Einwilligung „ohne jeden Zweifel“ gemäß der Richtlinie 95/46/EG sowie „unmissverständlich“ gemäß dem Erwägungsgrund 32 der Datenschutz-Grundverordnung ebenso dafür sprechen, die ausdrückliche und schriftliche Einwilligung beizubehalten und nicht als zusätzliche Pflicht zu sehen.

32 Siehe Spindler/Nink in: Spindler/Schuster, Recht der elektronischen Medien, 3. Auflage 2015, § 13 TMG Rn. 8, jedoch als Auslegung für die sprachlich identische Regelung im Telemediengesetz.

33 Siehe auch „Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit“, Datenschutz und Telekommunikation, 7. Auflage 2015, S. 25; https://www.bfdi.bund.de/SharedDocs/Publikationen/Infobroschueren/INFO5.pdf?__blob=publicationFile&v=6

In Erwägungsgrund 32 ist zudem die Möglichkeit der schriftlichen Einwilligung benannt, die gleichermaßen die Nachweispflicht des Artikel 7 Absatz 1 Datenschutz-Grundverordnung unterstützt. Auf der anderen Seite ist in der Richtlinie 2002/58/EG geregelt (Erwägungsgrund 17), dass die Einwilligung „in jeder geeigneten Weise“ erfolgen kann.

! Fazit Nr. 1

Es empfiehlt sich eine Klarstellung,

- was unter „zusätzlichen Pflichten“ (im Verhältnis zur Richtlinie 2002/58/EG) zu verstehen ist und welche eigenständigen gesetzlichen Regelungen der Mitgliedstaaten einer Vollharmonisierung (dennoch) entsprechen (z. B. jederzeitige Abrufbarkeit und Protokollierung oder in Bezug auf Standortdaten: „ausdrücklich, gesondert und schriftlich“). Zu berücksichtigen ist, dass die Protokollierung eine Form des Nachweises darstellen kann, aber im Sinne einer europaweiten Vereinheitlichung gegebenenfalls auch andere Methoden in Frage kommen, was zu prüfen wäre.

- ob sich der Begriff „zusätzlichen Pflichten“ sowohl auf die betroffene Person als auch auf den Verantwortlichen bezieht.

(2) Richtlinie 2002/58/EG in der Fassung 2009/136/EG

Die Richtlinie 2002/58/EG (in der Fassung 2009/136/EG) enthält in Artikel 5 folgende Regelung:
„(3) Die Mitgliedstaaten stellen sicher, dass die Speicherung von Informationen oder der Zugriff auf Informationen, die bereits im Endgerät eines Teilnehmers oder Nutzers gespeichert sind, nur gestattet ist, wenn der betreffende Teilnehmer oder Nutzer auf der Grundlage von klaren und umfassenden Informationen, die er gemäß der Richtlinie 95/46/EG u. a. über die Zwecke der Verarbeitung erhält, seine Einwilligung gegeben hat. Dies steht einer technischen Speicherung oder dem Zugang nicht entgegen, wenn der alleinige Zweck die Durchführung der Übertragung einer Nachricht über ein elektronisches Kommunikationsnetz ist oder wenn dies unbedingt erforderlich ist, damit der Anbieter eines Dienstes der Informationsgesellschaft, der vom Teilnehmer oder Nutzer ausdrücklich gewünscht wurde, diesen Dienst zur Verfügung stellen kann.“

Erwägungsgrund 17 der Richtlinie 2002/58/EG regelt hierzu näher, dass die Einwilligung dieselbe Bedeutung haben sollte wie der in der Richtlinie 95/46/EG definierte und dort weiter präzisierte Begriff „Einwilligung der betroffenen Person“. Gemäß Artikel 94 Absatz 2 Datenschutz-Grundverordnung gelten Verweise auf die aufgehobene Richtlinie als Verweise auf die Datenschutz-Grundverordnung. Daher ist fraglich, ob Unterschiede in Bezug auf die Einwilligungsvoraussetzungen der Datenschutz-Grundverordnung vorliegen könnten. Hierbei ist gleichermaßen relevant, wie die Richtlinie derzeit umgesetzt wird.

Gemäß der Richtlinien 2002/58/EG und 95/46/EG könne die Einwilligung in jeder geeigneten Weise abgegeben werden, wodurch der Wunsch des Nutzers in einer spezifischen Angabe zum Ausdruck komme, die sachkundig und in freier Entscheidung erfolgt; hierzu zähle auch das Markieren eines Feldes auf einer Internet-Website.

In Bezug auf Cookies enthalten jedoch Erwägungsgründe 24 und 25 der Richtlinie 2002/58/EG gesonderte Regelungen. Es wird zwar einerseits auf das Risiko von Cookies Bezug genommen, welches eine ernsthafte Verletzung der Privatsphäre beinhalten könnte.[34] Gleichzeitig wird aber ebenso die Nützlichkeit als legitimes Hilfsmittel hervorgehoben, um die Wirksamkeit von Website-Gestaltung und Werbung zu untersuchen und die Identität der an Online-Transaktionen beteiligten Nutzer zu überprüfen.[35] In diesem Sinne könnten solche Instrumente, z. B. „Cookies", einem rechtmäßigen Zweck dienen, z. B. der Erleichterung der Bereitstellung von Diensten der Informationsgesellschaft. Daher sollte deren Einsatz auch unter der Bedingung zugelassen werden, dass die Nutzer gemäß der Richtlinie 95/46/EG klare und genaue Informationen über den Zweck von Cookies oder ähnlichen Instrumenten erhalten, d. h., der Nutzer müsse wissen, dass bestimmte Informationen auf dem von ihm benutzten Endgerät platziert werden.

Erwägungsgrund 66 der Richtlinie 2009/136/EG betont gleichermaßen die legitimen Zwecke bei Verwendung von Cookies. Daher sei es wichtig, den Nutzern klare und verständliche Informationen bereit zu stellen. Es sollten ebenso benutzerfreundliche Methoden zur Ablehnung von Cookies gestaltet werden. Ausnahmen von der Informationspflicht und der Einräumung des Rechts auf Ablehnung sollten zudem auf jene Situationen beschränkt sein, in denen die technische Speicherung oder der Zugriff unverzichtbar sind, um die Nutzung eines vom Teilnehmer oder Nutzer ausdrücklich angeforderten Diens¬tes zu ermöglichen. Wenn es technisch möglich sei, könne der Nutzer außerdem seine Einwilligung im Einklang mit den entsprechenden Bestimmungen der Richtlinie 95/46/EG über die Handhabung der entsprechenden Einstellungen eines Browsers oder einer anderen Anwendung ausdrücken. Letzteres sieht die Artikel-29-Datenschutzgruppe allerdings als kritisch an.[36]

In einzelnen Mitgliedsstaaten der Europäischen Union ist die Richtlinie 2002/58/EG (2009/136/EG) jedoch unterschiedlich angewendet worden. Die Ausführungen in den oben genannten Erwägungsgründen zur Rechtmäßigkeit von Cookies zur Webseitengestaltung sind im Jahre 2015 von der niederländischen Regierung im Sinne eines weiten Verständnisses ausgelegt worden, obwohl die Niederlande bislang die engste Interpretation der Richtlinien 95/46/EG sowie 2002/58/EG (2009/136/EG) hatten.

34 *Erwägungsgrund 24 der Richtlinie 2002/58/ÆG: Die Endgeräte von Nutzern elektronischer Kommunikationsnetze und in diesen Geräten gespeicherte Informationen sind Teil der Privatsphäre der Nutzer, die dem Schutz aufgrund der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten unterliegt. Sogenannte „Spyware", „Web-Bugs", „Hidden Identifiers" und ähnliche Instrumente können ohne das Wissen des Nutzers in dessen Endgerät eindringen, um Zugang zu Informationen zu erlangen, oder die Nutzeraktivität zurückzuverfolgen und können eine ernsthafte Verletzung der Privatsphäre dieser Nutzer darstellen. Die Verwendung solcher Instrumente sollte nur für rechtmäßige Zwecke mit dem Wissen der betreffenden Nutzer gestattet sein.*

35 *Erwägungsgrund 25 der Richtlinie 2002/58/ÆG: Solche Instrumente, z. B. so genannte „Cookies", können ein legitimes und nützliches Hilfsmittel sein, um die Wirksamkeit von Website-Gestaltung und Werbung zu untersuchen und die Identität der an Online-Transaktionen beteiligten Nutzer zu überprüfen. Dienen solche Instrumente, z. B. „Cookies", einem rechtmäßigen Zweck, z. B. der Erleichterung der Bereitstellung von Diensten der Informationsgesellschaft, so sollte deren Einsatz unter der Bedingung zugelassen werden, dass die Nutzer gemäß der Richtlinie 95/46/ÆG klare und genaue Informationen über den Zweck von Cookies oder ähnlichen Instrumenten erhalten, d. h., der Nutzer muss wissen, dass bestimmte Informationen auf dem von ihm benutzten Endgerät platziert werden. Die Nutzer sollten die Gelegenheit haben, die Speicherung eines Cookies oder eines ähnlichen Instruments in ihrem Endgerät abzulehnen. Dies ist besonders bedeutsam, wenn auch andere Nutzer Zugang zu dem betreffenden Endgerät haben und damit auch zu dort gespeicherten Daten, die sensible Informationen privater Natur beinhalten. Die Auskunft und das Ablehnungsrecht können einmalig für die Nutzung verschiedener in dem Endgerät des Nutzers während derselben Verbindung zu installierender Instrumente angeboten werden und auch die künftige Verwendung derartiger Instrumente umfassen, die während nachfolgender Verbindungen vorgenommen werden können. Die Modalitäten für die Erteilung der Informationen oder für den Hinweis auf das Verweigerungsrecht und die Einholung der Zustimmung sollten so benutzerfreundlich wie möglich sein. Der Zugriff auf spezifische Website-Inhalte kann nach wie vor davon abhängig gemacht werden, dass ein Cookie oder ein ähnliches Instrument von einer in Kenntnis der Sachlage gegebenen Einwilligung abhängig gemacht wird, wenn der Einsatz zu einem rechtmäßigen Zweck erfolgt.*

36 *Artikel-29-Datenschutzgruppe, WP 171 Stellungnahme 2/2010 zur Werbung auf Basis von Behavioural Targeting, angenommen am 22. Juni 2010, S. 16 ff.*

Nun ist per Gesetz der Einsatz von Cookies auch ohne vorheriges ausdrückliches Einverständnis für Analysezwecke des Webseitenbetreibers erlaubt, die die Privatsphäre des Nutzers nicht wesentlich beeinträchtigen.[37]

In Deutschland gelten für Cookies §§ 12 und 15 Telemediengesetz. Die deutsche Bundesregierung erläutert in ihren Antworten an die Europäische Kommission zur Umsetzung von Artikel 5 Absatz 3 Richtlinie 2002/58/EG, dass „§ 12 Telemediengesetz klarstellt, dass personenbezogene Daten im Zusammenhang mit der Bereitstellung von Telemedien ohne Einwilligung nur verarbeitet werden dürfen, wenn der Gesetzgeber dies ausdrücklich erlaubt. Eine solche gesetzliche Erlaubnis enthalte § 15 Telemediengesetz. Danach dürfen Nutzerdaten bei Inanspruchnahme von Telemedien ohne Einwilligung nur verarbeitet werden, wenn das für diesen Zweck erforderlich ist. Für die Speicherung und den Abruf von Informationen wie z. B. Cookies bedeutet dies, dass solche Verfahren in Deutschland ohne Einwilligung des Nutzers nur zulässig sind, wenn dies aus technischen Gründen für die Inanspruchnahme erforderlich ist. Im Übrigen dürfen solche Verfahren ohne Einwilligung des Nutzers nicht verwendet werden."[38]

Die unabhängige Datenschutzaufsichtsbehörde (ICO) von Großbritannien hat eine Empfehlung für die Verwendung von Cookies veröffentlicht und unterteilt zwischen den erforderlichen Zwecken (etwa für elektronischen Einkauf) ohne Einwilligung und „nützlichen" Zwecken, für die eine Einwilligung erforderlich sein soll. Eine konkludente, bewusste Einwilligung sei möglich:[39]

! You must tell people if you set cookies, and clearly explain what the cookies do and why. You must also get the user's consent. Consent can be implied, but must be knowingly given.

! There is an exception for cookies that are essential to provide an online service at someone's request (e.g. to remember what's in their online basket, or to ensure security in online banking).

The same rules also apply if you use any other type of technology to store or gain access to information on someone's device.[40]

37 *https://www.acm.nl/en/publications/publication/11917/Frequently-asked-questions-about-the-Dutch-cookie-act/; https://zoek.officielebekendmakingen.nl/stb-2015-100.html; http://www.vbk.nl/en/sharing-knowledge/legal-update/new-dutch-cookie-law-is-now-in-force/ Siehe außerdem Artikel-29-Datenschutzgruppe, WP 194, Stellungnahme 04/2012 zur Ausnahme von Cookies von der Einwilligungspflicht, angenommen am 07. Juni 2012, insbesondere S. 11/12 zu den so genannten First-Party-Analysecookies.*

38 *Siehe unter: https://circabc.europa.eu/sd/d/9762ba56-a9b0-48e2-9858-1e25f2ea05cc/COCOM11-20%2520Questionnaire%25 5200n%2520Art.%25205(3)%2520e-Privacy%2520Dir..pdf+&cd=6&hl=de&ct=clnk&gl=de*

39 *https://ico.org.uk/; https://ico.org.uk/media/for-organisations/documents/1545/cookies_guidance.pdf*

40 *https://ico.org.uk/for-organisations/guide-to-pecr/cookies-and-similar-technologies/*

Die Datenschutzaufsichtsbehörde (ICO) vertritt außerdem die Auffassung, dass die Einwilligung nicht ausdrücklich zu erteilen ist[41]:

! Consent does not necessarily have to be explicit 'opt-in' consent. Implied consent can also be valid. If you are relying on implied consent, you need to be confident that your users fully understand that their actions will result in cookies being set. However, in some circumstances (for example, collecting sensitive personal data such as health details) it is likely that explicit opt-in consent is more appropriate.

Des weiteren lässt auch die eigene Webseite der Datenschutzaufsichtsbehörde (ICO) zur „Verbesserung ihrer Webseite" Cookies sowie ein Opt-Out zu. Fraglich ist zudem, was unter „anonymer Form einer Cookie-Sammlung" im Rahmen der Informationen auf der Webseite verstanden wird:

! We have placed cookies on your device to help make this website better.

You can use this tool to change your cookie settings. Otherwise, we´ll assume you are OK to continue.

I'm fine with this

Information and SettingsAbout this tool:
You can use this tool to change your cookie settings. Otherwise, we'll assume you're OK to continue.
Some of the cookies we use are essential for the site to work.

We also use some non-essential cookies to collect information for making reports and to help us improve the site. The cookies collect information in an anonymous form.

To control third party cookies, you can also adjust your browser settings.

Turn cookies off

I'm fine with this

Die Artikel-29-Datenschutzgruppe hat in ihrer Stellungnahme zu Cookies eine solche Unterscheidung nicht vorgenommen und die Richtlinie 2002/58/EG als Spezialgesetz gegenüber der Richtlinie 95/46/EG eingestuft.[42] In diesem Sinne soll die Richtlinie 95/46/EG vollumfänglich anwendbar bleiben mit der Ausnahme der Bestimmungen, die in der Datenschutzrichtlinie für elektronische Kommunikation direkt behandelt werden.

41 https://ico.org.uk/for-organisations/guide-to-pecr/cookies-and-similar-technologies/

42 Artikel-29-Datenschutzgruppe, WP 171 Stellungnahme 2/2010 zur Werbung auf Basis von Behavioural Targeting, angenommen am 22. Juni 2010, S. 11/12.

Dies gelte in erster Linie für die Regelung des Artikels 7 der Richtlinie 95/46/EG zu den Rechtsgrundlagen für die Datenverarbeitung, wobei aber die verbleibenden Bestimmungen der Richtlinie 95/46/EG einschließlich der Grundsätze bezüglich der Datenqualität, der Rechte der betroffenen Personen (wie das Auskunftsrecht, das Recht auf Löschung und das Widerspruchsrecht), der Vertraulichkeit, der Sicherheit der Verarbeitung und der internationalen Datenübermittlungen vollumfänglich anzuwenden seien.[43]

Soweit die Neufassung von Richtlinie 2002/58/EG (2009/136/EG) keine anderweitige Klarstellung schafft, muss dies gleichermaßen im Hinblick auf die Datenschutz-Grundverordnung gelten – mit Ausnahme der Regelungen die den Diensteanbietern zusätzliche Pflichten auferlegen.

Die Artikel- 29-Datenschutzgruppe führt insgesamt aus:
Soweit die Neufassung von Richtlinie 2002/58/EG (2009/136/EG) keine anderweitige Klarstellung schafft, muss dies gleichermaßen im Hinblick auf die Datenschutz-Grundverordnung gelten – mit Ausnahme der Regelungen die den Diensteanbietern zusätzliche Pflichten auferlegen.

! Die Artikel- 29-Datenschutzgruppe führt insgesamt aus:
Aus dem Wortlaut von Artikel 5 Absatz 3 ergibt sich, dass: i) die Einwilligung eingeholt werden muss, bevor der Cookie platziert wird und/oder auf dem Endgerät des Nutzers gespeicherte Informationen gesammelt werden, was üblicherweise als vorherige Einwilligung bezeichnet wird und ii) eine Einwilligung in Kenntnis der Sachlage nur dann eingeholt werden kann, wenn dem Nutzer vorher Informationen über das Versenden und die Zwecke des Cookies erteilt wurden. In diesem Zusammenhang muss berücksichtigt werden, dass eine Einwilligung ungeachtet der jeweiligen Umstände, nur dann gültig ist, wenn sie ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgt ist. Die Einwilligung muss vor Erhebung der personenbezogenen Daten eingeholt werden, damit die betroffenen Personen voll und ganz erkennen, dass sie einwilligen und in was sie einwilligen. Darüber hinaus muss eine Einwilligung zurückziehbar sein.

Einwilligungen über Browserseinstellungen sieht die Artikel-29-Datenschutzgruppe als kritisch an,[44] auch wenn Erwägungsgrund 66 der geänderten Datenschutzrichtlinie für elektronische Kommunikation darauf hinweist, dass die Einwilligung ebenso über Handhabung der entsprechenden Einstellungen eines Browsers oder einer anderen Anwendung, wenn es technisch durchführbar und wirksam ist, im Einklang mit den Bestimmungen der Richtlinie 95/46/EG ausgedrückt werden kann.

Zusammenfassend ist festzuhalten:
In Artikel 5 Absatz 3 der Richtlinie 2002/58/EG (2009/136/EG) wird die Einwilligungspflicht für Cookies normiert. Fraglich ist jedoch, aus welchem Grunde in den Mitgliedstaaten eine unterschiedliche Auslegung erfolgt und ob dies durch die Erwägungsgründe hervorgerufen wird, oder ob tatsächlich ein Vertragsverletzungsverfahren eingeleitet werden müsste.

Für eine unterschiedliche Auslegungsmöglichkeit könnten die nicht eindeutig formulierten Erwägungsgründe sowie die Möglichkeit einer konkludenten Einwilligung sprechen: Erwägungsgrund 66 normiert eine Ausnahme von der Informationspflicht und dem Recht auf Ablehnung für unverzichtbare Cookies.

43 *Artikel-29-Datenschutzgruppe, WP 171 Stellungnahme 2/2010 zur Werbung auf Basis von Behavioural Targeting, angenommen am 22. Juni 2010, S.12.*

44 *Siehe bereits oben, Fn. 34.*

In Erwägungsgrund 25 werden Cookies als legitime und nützliche Hilfsmittel zur Webseiten-Gestaltung und zur Untersuchung von Werbung erläutert. Im Anschlusssatz erfolgt dann die Klarstellung, dass bei Verwendung von Cookies zu einem rechtmäßigen Zweck dem Nutzer klare und genaue Informationen bereitgestellt werden müssen und die Nutzer die Gelegenheit haben, diesen abzulehnen.[45]

Im Übrigen lässt sich bei einem Cookie der Nachweis der Einwilligung (immanent) gemäß Artikel 7 Absatz 1 Datenschutz-Grundverordnung bzw. aufgrund der Darstellung der Webseite leicht erbringen.

! Fazit Nr. 2

Es empfehlen sich europaweite, einheitlich geltende Verhaltensregeln zur Auslegung der Einwilligungsvoraussetzungen, soweit diese aufgrund einer Verarbeitungstätigkeit in mehreren Mitgliedstaaten ausgearbeitet werden können. Aktuell ist in Bezug auf Cookies unklar, ob die Einleitung von Vertragsverletzungsverfahren durch die Kommission versäumt wurde.

Ohne europaweite Verhaltensregelungen läuft außerdem die Nachweispflicht der Einwilligung gemäß Artikel 7 Absatz 1 Datenschutz-Grundverordnung ins Leere bzw. wird den Aufsichtsbehörden in den Mitgliedstaaten überlassen. Schutzniveau und Sanktionen sollten im Sinne einer Harmonisierung gleichwertig sein.

Darüber hinaus empfiehlt sich der Vergleich zwischen der Richtlinie 95/46/EG, der Umsetzung durch die Mitgliedstaaten sowie der Datenschutz-Grundverordnung im Hinblick auf die Anforderungen der Einwilligung. So kann ebenso geprüft werden, ob eine Tendenz für den Inhalt der auszuarbeitenden Verhaltensregeln hergeleitet werden könnte, vor allem dahingehend, was als zusätzliche Pflicht gemäß Artikel 95 Datenschutz-Grundverordnung und was als sinnvolle Ergänzung zu verstehen ist.

Konkret könnte eine Klarstellung dahingehend erfolgen,

- ob die Datenschutz-Grundverordnung grundlegend andere Voraussetzungen an die Einwilligung oder Anonymisierung stellt als die Richtlinie 95/46/EG und ob bislang die Einleitung von Vertragsverletzungsverfahren versäumt wurde,

- welche Grenzen eine konkludente Einwilligung hat, etwa dass eine Weiternutzung des Dienstes gleichzusetzen ist mit „voreingestellte Kästchen“ und dass ein Mehr an Transparenz in diesem Falle nicht die Einwilligung ersetzen kann.

- was unter einer sonstigen eindeutigen bestätigenden Verhaltensweise gemäß Artikel 4 Nr. 11 Datenschutz-Grundverordnung zu verstehen ist.[46]

45 *Siehe Spindler/Nink in: Spindler/Schuster, Recht der elektronischen Medien, 3. Auflage 2015, § 13 TMG Rn. 6 mit dem Hinweis auf nicht hinreichende Bestimmtheit der Richtlinie: „Dem ist entgegen zu halten, dass Bestimmungen aus Richtlinien nach erfolglosem Ablauf der Umsetzungsfrist nur dann unmittelbar in den EU-Mitgliedstaaten gelten, wenn sie derart hinreichend bestimmt sind, dass sie ohne weiteres angewandt werden können. Dies wird jedoch bei der Cookie-Regelung der ePrivacy-Richtlinie gerade kontrovers diskutiert. Denn nach wie vor ist unklar, wie die Umsetzung der Einwilligung in Cookies erfolgen kann. Die Mitgliedstaaten, welche die ePrivacy-Richtlinie bislang ungesetzt haben, implementierten teilweise völlig unterschiedliche Anforderungen an die Einwilligung in den nationalen Gesetzen. Es bestehen daher erhebliche Zweifel, ob die Cookie-Regelung der ePrivacy-Richtlinie tatsächlich hinreichend bestimmt ist.“*

46 *Hier ist die Auffassung der Artikel-29-Datenschutzgruppe zu berücksichtigen, die feststellt, dass ein Opt-Out bei Cookies im Allgemeinen keinen angemessenen Mechanismus in Kenntnis der Sachlage darstellt.*

! Die bisherigen Empfehlungen der Artikel-29-Datenschutzgruppe könnten bei der Ausarbeitung von Verhaltensregeln zugrunde gelegt werden. Hierzu gehört ebenso die Stellungnahme WP 194 zur Ausnahme von Cookies von der Einwilligungspflicht[47], die unter anderem Leitlinien zu „erforderlichen" Cookies und Cookies für eigene Analysezwecke des Dienstanbieters enthält, die nach Ansicht der Artikel-29-Datenschutzgruppe kaum ein Datenschutzrisiko darstellen, wenn sie ausschließlich für die aggregierten Statistiken des Erstanbieters genutzt werden. In diesem Zusammenhang sollten darüber hinaus jedoch klare Kriterien entwickelt werden, unter welchen Voraussetzungen „keine erhebliche Persönlichkeitsrechtsverletzung" der Nutzer oder „kaum ein Datenschutzrisiko" vorliegt, was aufgrund der (zukünftig) noch unbekannten Verknüpfungsmöglichkeiten von persönlichen Daten mit Schwierigkeiten verbunden sein könnte. Entsprechendes gilt für Cookies zur Webseitengestaltung und Werbung. Insoweit sind die Erwägungsgründe der Richtlinie 2002/58/EG nicht eindeutig, die Cookies zur Webseitengestaltung und Werbung als legitimes Mittel betrachten.

2. Dienste der Informationsgesellschaft

Die Datenschutz-Grundverordnung lässt gemäß Artikel 2 Absatz 4 die Anwendbarkeit der Richtlinie 2000/31/EG unberührt.[48] Gegenstand dieser Richtlinie sind Dienste der Informationsgesellschaft. Gemäß Artikel 1 Nr. 2 der Richtlinie 98/34/EG in der Fassung von der Richtlinie 98/48/EG bedeutet Dienst der Informationsgesellschaft jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung.[49] Allerdings enthält diese Verordnung keine speziellen Regelungen zur Einwilligung und Transparenz. Artikel 5 der Richtlinie 2000/31/EG enthält zwar Regelungen zu Impressumsangaben, Artikel 6 Maßnahmen im Hinblick auf kommerzielle Kommunikation und Artikel 10 verbraucherschutzrechtliche Bestimmungen bezüglich der Abgabe einer Bestellung unter Inanspruchnahme eines Dienstes der Informationsgesellschaft. Es werden jedoch weder allgemeine Pflichten im Hinblick auf die Informiertheit bei Erteilung der Einwilligung noch konkrete Anforderungen an die Einwilligung festgelegt.

47 *Artikel-29-Datenschutzgruppe, WP 194, Stellungnahme 04/2012 zur Ausnahme von Cookies von der Einwilligungspflicht, angenommen am 07. Juni 2012, insbesondere S. 11/12 zu den so genannten First-Party-Analysecookies.*

48 *Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr") (Amtsblatt Nr. L 178 vom 17.7.2000, S. 1 – S. 16). Das Telemediengesetz dient der Umsetzung der Richtlinie 2000/31/EG.*

49 *Richtlinie 98/48/EG des Europäischen Parlaments und des Rates vom 20. Juli 1998 zur Änderung der Richtlinie 98/34/EG über ein Informationsverfahren auf dem Gebiet der Normen und technischen Vorschriften*
Amtsblatt Nr. L 217 vom 05.08.1998 S. 18 – S. 26.
Im Sinne dieser Definition bezeichnet der Ausdruck
- ´im Fernabsatz erbrachte Dienstleistung' eine Dienstleistung, die ohne gleichzeitige physische Anwesenheit der Vertragsparteien erbracht wird;
- ´elektronisch erbrachte Dienstleistung' eine Dienstleistung, die mittels Geräten für die elektronische Verarbeitung (einschließlich digitaler Kompression) und Speicherung von Daten am Ausgangspunkt gesendet und am Endpunkt empfangen wird und die vollständig über Draht, über Funk, auf optischem oder anderem elektromagnetischem Wege gesendet, weitergeleitet und empfangen wird;
- ´auf individuellen Abruf eines Empfängers erbrachte Dienstleistung' eine Dienstleistung, die durch die Übertragung von Daten auf individuelle Anforderung erbracht wird.
Zur Auslegung eines Dienstes mit Zusatznutzen im deutschen Recht anhand der Frage, ob es sich um einen Telemediendienst mit Anwendbarkeit des Telemediengesetzes handelt oder ob die Regelungen des Telekommunikationsgesetzes abschließend anwendbar sind: Schnabel, Datenschutz bei profilbasierten Location-based Services, Die datenschutzadäquate Gestaltung von Service-Plattformen zur Mobilkommunikation, S. 275, 276 ff. Außerdem Janner/Holst/Kopp, Social Media im Kulturmanagement, S. 109 mit dem Hinweis, dass sich die Verwendung von Standortdaten für Telekommunikationsdiensteanbieter nicht nach dem Telemediengesetz, sondern nach §§ 96 und 98 Telekommunikationsgesetz richtet.

Im Hinblick auf die Transparenz (Informations- und Auskunftspflichten) sowie die Einwilligung sind daher die Datenschutz-Grundverordnung sowie die Richtlinie 2002/58/EG (2009/136/EG) zugrunde zu legen, soweit letztere den Umgang mit „Informationen, die im Endgerät des Kunden gespeichert sind“ oder „Dienste mit Zusatznutzen“ regelt.[50]

Daher müssen im Hinblick auf die Vorgaben für Transparenz und Einwilligung die Regelungen der Datenschutz-Grundverordnung herangezogen werden, anhand derer auch die datenschutzrechtlichen Regelungen des Telemediengesetzes für elektronische Informations- und Kommunikationsdienste zu prüfen sind:

Die Datenschutz-Grundverordnung regelt in Artikel 12 ff. die Modalitäten der Transparenz, in Artikel 13 dazu näher die Informationspflichten, sofern personenbezogene Daten bei der betroffenen Person erhoben werden. Diesbezüglich enthält die Datenschutz-Grundverordnung außerdem keine generelle Öffnungsklausel für Regelungen durch die Mitgliedstaaten. Beschränkungen dieser Rechte und Pflichten dürfen allenfalls unter den Voraussetzungen des Artikel 23 Datenschutz-Grundverordnung erfolgen. Daher müssen auch die datenschutzrechtlichen Regelungen des Telemediengesetzes mit diesen Anforderungen vereinbar sein: Im Hinblick auf die Informiertheit ist § 13 Telemediengesetz einschlägig, bezüglich der elektronischen Einwilligung enthält § 13 Absatz 2 Telemediengesetz eine zu § 94 Telekommunikationsgesetz inhaltsgleiche Regelung. Für letztere gelten die obigen Ausführungen entsprechend,[51] so dass im Hinblick auf die elektronische Einwilligung gemäß § 13 Absatz 2 Telemediengesetz fraglich ist, ob die Regelungen zur inhaltlichen Ausgestaltung der Einwilligung, nämlich „jederzeit abrufbar und protokolliert“, aufrechterhalten werden können.

Die Datenschutz-Grundverordnung verlangt bezüglich der vorformulierten Einwilligung gemäß Erwägungsgrund 42 lediglich die leicht zugängliche Form. § 13 Absatz 2 Nr. 3 Telemediengesetz enthält allerdings bereits jetzt eine insoweit konforme Regelung, als auch in Artikel 7 Absatz 3 Datenschutz-Grundverordnung vorgegeben ist, dass die betroffene Person vor Abgabe der Einwilligung von der Widerrufsmöglichkeit in Kenntnis zu setzen ist.

50 Zur Auslegung eines Dienstes mit Zusatznutzen im deutschen Recht anhand der Frage, ob es sich um einen Telemediendienst mit Anwendbarkeit des Telemediengesetzes handelt oder ob die Regelungen des Telekommunikationsgesetzes abschließend anwendbar sind: Schnabel, Datenschutz bei profilbasierten Location-based Services, Die datenschutzadäquate Gestaltung von Service-Plattformen zur Mobilkommunikation, S. 275, 276 ff. Außerdem Janner/Holst/Kopp, Social Media im Kulturmanagement, S. 109 mit dem Hinweis, dass sich die Verwendung von Standortdaten für Telekommunikationsdiensteanbieter nicht nach dem Telemediengesetz, sondern nach §§ 96 und 98 Telekommunikationsgesetz richtet.

51 Siehe S. 9 ff.

Hinsichtlich der grundsätzlichen Transparenz der Datenverarbeitung und Informiertheit besteht gemäß § 13 Absatz 1 Satz 3 Telemediengesetz außerdem die Verpflichtung des Diensteanbieters, dass der Inhalt der Unterrichtung für den Nutzer jederzeit abrufbar sein muss. In der Datenschutz-Grundverordnung ist zwar nun der Grundsatz der Transparenz ausdrücklich benannt (siehe Artikel 5 Absatz 1a, Artikel 12). Eine Verpflichtung, dass Informationen für den Nutzer jederzeit abrufbar sein müssen, ist jedoch nicht enthalten. Im Gegensatz zu den in Artikel 5 der Richtlinie 2000/31/EG geregelten Impressumsangaben, nach denen die Mitgliedstaaten sicherstellen müssen, dass der Diensteanbieter den Nutzern des Dienstes die dort aufgeführten Informationen leicht, unmittelbar und ständig verfügbar machen muss, ist im Hinblick auf die datenschutzrechtlichen Informationspflichten eine solche ständige Verfügbarkeit nicht verlangt.[52] Aus der Datenschutz-Grundverordnung (Artikel 15 und Erwägungsgrund 63) kann eine solche Verpflichtung ebenso wenig unmittelbar hergeleitet werden.[53]

Für die Dienste der Informationsgesellschaft ergibt sich im Vergleich zwischen Telemediengesetz und Datenschutz-Grundverordnung ein weiterer Unterschied dahingehend, dass gemäß § 13 Absatz 1 Telemediengesetz die Unterrichtung eines Nutzers über Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten zu Beginn des Nutzungsvorgangs erfolgen muss.[54] Hiervon abweichend regelt Artikel 13 Absatz 1 Datenschutz-Grundverordnung, dass die Informationspflichten seitens des Verantwortlichen gegenüber den betroffenen Personen zum Zeitpunkt der Erhebung der personenbezogenen Daten zu erfüllen sind.[55]

Der Zeitpunkt „zu Beginn des Nutzungsvorgangs“ gemäß § 13 Telemediengesetz kann „vom Zeitpunkt der Erhebung“ der Daten gemäß Artikel 13 Datenschutz-Grundverordnung grundsätzlich abweichen. Für die Einwilligung gilt jedoch (immer), dass diese auf (vorher) informierter Basis stattfinden muss. Im Übrigen ist in Bezug auf die grundsätzliche Informiertheit der Datenverarbeitung zu erwähnen, dass „zum Zeitpunkt der Erhebung“ den Schluss auf eine Zeitgleichheit nahe legt. Die Fassung des Teledienstedatenschutzgesetzes (TDDSG) von 1997 nahm auf den „Zeitpunkt vor Erhebung der Daten“ Bezug, seit dem Teledienstegesetz (TDDSG 2001) stellt der deutsche Gesetzgeber auf den Beginn des Nutzungsvorgangs ab. Hintergrund dafür sei, dass bereits beim ersten Webseitenbesuch personenbezogene Daten erhoben werden können.[56]

52 *Gemäß Erwägungsgründen 39 sowie 58 der Datenschutz-Grundverordnung setzt der Grundsatz der Transparenz lediglich 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. Erwägungsgrund 42 regelt speziell für die Einwilligung mit Bezug zum Verbraucherschutz, dass gemäß der Richtlinie 93/13/EWG des Rates eine vom Verantwortlichen vorformulierte Einwilligungserklärung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zur Verfügung gestellt werden und keine missbräuchlichen Klauseln beinhalten sollte.*

53 *Siehe bereits die Ausführungen zum Telekommunikationsgesetz, S. 7 ff.*

54 *Das Telemediengesetz dient der Umsetzung der Richtlinie 2000/31/EG.*

55 *Gemäß Artikel 13 Absatz 1 Datenschutz-Grundverordnung bestehen die Informationspflichten aus folgendem: den Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters; gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten; die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung; wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden; gegebenenfalls die Empfänger oder Kategorien von Empfängern und gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln.*

56 *Spindler/Nink in: Spindler/Schuster, Recht der elektronischen Medien, 3. Auflage 2015, § 13 TMG Rn. 3. Dieselben: „Diese Unterrichtungspflicht diene letztlich der Ermöglichung der aktiven Mitwirkung des Betroffenen an der Preisgabe seiner Daten, wobei sich die Unterrichtungspflicht von der in § 4a Abs. 1 Satz 2 BDSG verankerten Hinweispflicht insofern unterscheide, dass der Hinweis in § 4a Abs. 1 Satz 2 BDSG immer vor der Einwilligung erfolgen muss, während die Unterrichtungspflicht von der Einwilligung völlig unabhängig ist, wobei beide aber zeitlich zusammenfallen könnten.“ Zu berücksichtigen könnte jedoch ebenso sein, ob sich der Dienst an Nutzer in mehreren Mitgliedstaaten richtet.*

! Fazit Nr. 3:

Eine „jederzeitige Abrufbarkeit“ der Information ist nach der Datenschutz-Grundverordnung nicht gefordert, auch die „Protokollierung“ der Einwilligung wird nicht ausdrücklich benannt und die Anforderungen an einen Nachweis inhaltlich nicht definiert. Zu berücksichtigen ist auch hier, dass die Protokollierung eine Form des Nachweises darstellen kann, aber im Sinne einer europaweiten Vereinheitlichung gegebenenfalls auch andere Methoden in Frage kommen, was zu prüfen wäre.

Daher empfiehlt sich bei Diensten der Informationsgesellschaft die Ausarbeitung einer europaweiten Verhaltensregel, welche Maßnahmen zukünftig gefordert, gewünscht und weiterhin in praktischer Hinsicht für die Unternehmen umsetzbar sind, ebenso im Hinblick auf den geforderten Nachweis der Einwilligung (vgl. auch Artikel 24 Absatz 3, Artikel 40 Datenschutz-Grundverordnung). Es könnte erläutert werden, ob „leicht zugänglich“ mit „jederzeit abrufbar“ gleichzusetzen ist und einem jederzeitigen Auskunftsanspruch gleichsteht. Dies steht unter der Voraussetzung, dass diese aufgrund einer Verarbeitungstätigkeit in mehreren Mitgliedstaaten ausgearbeitet werden können, wobei hier die grundsätzliche „weltweite“ Abrufbarkeit zu berücksichtigen ist.[57]

Anders als bezüglich der Impressumsangaben ist in der Richtlinie 2002/31/EG keine „ständige Verfügbarkeit“ gefordert.

Fraglich ist stets, ob eine europaweit geltende Verhaltensregel mit Schwierigkeiten oder einer langen Zeitdauer behaftet sein könnte, da sich gemäß Artikel 40 Datenschutz-Grundverordnung die Verhaltensregel auf Verarbeitungstätigkeiten in mehreren Mitgliedstaaten beziehen muss und von der zuständigen Aufsichtsbehörde dem Europäischen Datenschutzausschuss vorzulegen ist, bevor die Kommission ihre allgemeine Gültigkeit in der Union erklären kann.

Daher empfiehlt sich bereits zum jetzigen Zeitpunkt die Benennung und Prüfung von offenen Punkten, für die Verhaltensregeln ausgearbeitet werden sollten und deren Klärung für eine auch in praktischer Hinsicht notwendige Harmonisierung des Datenschutzrechts erforderlich ist. Die deutschen Aufsichtsbehörden könnten bereits zum jetzigen Zeitpunkt mit der Förderung der Ausarbeitung von Verhaltensregeln beginnen und klärungsbedürftige Fragen erstellen, die sich auf Verarbeitungstätigkeiten in mehreren Mitgliedstaaten beziehen, verbunden mit der Aufforderung an Verbände, diese zu prüfen und Vorschläge zu unterbreiten.

D. Einwilligungsassistent

In der Einführung A. dieser Stellungnahme (S. 4 ff. | Anhang 1) wurde bereits darauf hingewiesen, dass sich die Konzepte und Verwendungszwecke derzeit in der Entwicklung befinden. Sofern Anbieter von elektronischen Kommunikationsdiensten oder Diensten der Informationsgesellschaft zukünftig den Einwilligungsassistenten im Zusammenhang mit ihren Diensten verwenden, müssten die oben dargestellten Überlegungen zum Telekommunikationsgesetz und zum Telemediengesetz mit berücksichtigt werden.

57 Zu berücksichtigen könnte jedoch ebenso sein, ob sich der Dienst an Nutzer in mehreren Mitgliedstaaten richtet.

Die nachfolgende Prüfung muss allerdings unter der Maßgabe erfolgen, dass noch nicht absehbar ist, ob der Einwilligungsassistent „selbst“ als eigenständiger Dienst oder als Bestandteil eines Dienstes (z. B. Dienst der Informationsgesellschaft) rechtlich einzuordnen ist. Möglich ist ebenso die Einstufung als Software-Tool im Einsatzbereich des Nutzers. In diesem Falle stellt sich die Frage, wer Verantwortlicher dieses Systems ist (siehe S. 56 ff.).

Insgesamt ist nach der Datenschutz-Grundverordnung zu berücksichtigen, dass Verantwortlicher gemäß Artikel 4 Nr. 7 Datenschutz-Grundverordnung die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle ist, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

Es muss daher zukünftig entschieden werden, ob ein Einwilligungsassistent „nur“ als Software, oder darüber hinaus als Dienst der Informationsgesellschaft im Sinne eines „Inhaltsdienstes“ gemäß der Richtlinie 2000/31/EG[58] oder „inhaltsneutral“ als (Bestandteil eines) elektronischen Kommunikationsdienstes gemäß den Richtlinien 2002/21/EG, 2002/58/EG(2009/136/EG)[59] lediglich den Vorgang der Übertragung betrifft oder als Dienst mit Zusatznutzen[60] verstanden werden kann. Die Frage ist, ob die Installation einer Hilfesoftware tatsächlich als eigener Online-Dienst betrachtet werden kann, so dass der Empfänger der Daten auch zum Dienstanbieter wird und damit ebenso zum Verantwortlichen. Dies hängt ebenso davon ab, wer den Einwilligungsassistenten einsetzt und in welcher Weise „betreibt.“ Möglich wäre sogar ein zwischengeschalteter „weiterer Anbieter“, etwa ein Anbieter von Telekommunikationsdiensten, der einen solchen Dienst zur Verfügung stellt.

Insgesamt muss bei dieser Beurteilung beachtet werden, ob der Einwilligungsassistent vorwiegend nur die Übertragung sicherstellt oder „mehr“ kann, so dass bereitgestellte Inhalte im Vordergrund stehen. Sofern die betroffene Person den Assistenten lediglich als Tool dezentral in ihrem Bereich einsetzt, um den Selbstdatenschutz zu stärken, so kann lediglich eine unterstützende Software in Betracht kommen, für die der Nutzer allein verantwortlich ist. Außerdem wäre denkbar, dass der Einsatz beim Empfänger der Daten nicht als eigenständiger Dienst, sondern als die Datenverarbeitung unterstützende Softwarelösung verstanden wird. In diesem Sinne wäre er zwar Verantwortlicher, aber nicht im Sinne eines (Online)Dienstanbieters.

Diese Frage kann abschließend erst zu dem Zeitpunkt beantwortet werden, wenn nähere Details über die Technik und geplanten Einsatzzweck vorliegen.

Unabhängig davon sind für das Vorliegen einer wirksamen Einwilligung jedoch stets die folgenden Überlegungen und Voraussetzungen zu berücksichtigen:

58 Gemäß Artikel 1 Nr. 2 der Richtlinie 98/34/ÆG in der Fassung von der Richtlinie 98/48/ÆG bedeutet Dienst der Informationsgesellschaft jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung.

*59 Richtlinie 2002/21/ÆG des Europäischen Parlaments und des Rates vom 7. März 2002 über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste (Rahmenrichtlinie)
Artikel 2c) „elektronische Kommunikationsdienste“: gewöhnlich gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über elektronische Kommunikationsnetze bestehen, einschließlich Telekommunikations- und Übertragungsdienste in Rundfunknetzen, jedoch ausgenommen Dienste, die Inhalte über elektronische Kommunikationsnetze und -dienste anbieten oder eine redaktionelle Kontrolle über sie ausüben; nicht dazu gehören die Dienste der Informationsgesellschaft im Sinne von Artikel 1 der Richtlinie 98/34/ÆG, die nicht ganz oder überwiegend in der Übertragung von Signalen über elektronische Kommunikationsnetze bestehen.*

60 Dienst mit Zusatznutzen wird gemäß Artikel 2 g) der Richtlinie 2002/58/ÆG definiert als „jeder Dienst, der die Bearbeitung von Verkehrsdaten oder anderen Standortdaten als Verkehrsdaten in einem Maße erfordert, das über das für die Übermittlung einer Nachricht oder die Fakturierung dieses Vorgangs erforderliche Maß hinausgeht.“ Beispielhaft werden hierzu in Erwägungsgrund 18 die Beratung hinsichtlich der billigsten Tarifpakete, Navigationshilfen, Verkehrsinformationen, Wettervorhersage oder touristische Informationen genannt.

I. Willensbekundung und Einverständnis

1. Definition

Gemäß Artikel 2h) der Richtlinie 95/46/EG stellt eine Einwilligung eine Willensbekundung des Betroffenen dar.

Eine Willensbekundung ist eine nach außen tretende, vom Adressaten erkennbare Handlung, die bei objektiver Würdigung als Ausdruck der Zustimmung zu verstehen ist.[61] Der Betroffene muss positiv eine bestimmte Meinung zum Ausdruck gebracht haben.[62] Allerdings ist umstritten, ob eine konkludente Einwilligung ausreicht.[63] Gemäß § 4a Absatz 1 Satz 3 Bundesdatenschutzgesetz bedarf die Einwilligung der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Damit ist gemäß der Intention des Bundesdatenschutzgesetzes eine konkludente Einwilligung grundsätzlich unzulässig. Die Artikel-29-Datenschutzgruppe führt aus, dass eine „Willensbekundung" darauf hindeute, dass eine Handlung nötig ist (im Gegensatz zu einer Situation, in der eine Einwilligung aus dem Ausbleiben einer Handlung gefolgert werden kann).[64]

Gemäß Artikel 4 Nr. 11 Datenschutz-Grundverordnung ist eine Einwilligung ebenfalls eine Willensbekundung, und zwar 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 („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").

Erwägungsgrund 32 regelt dazu näher, dass die Einwilligung durch eine eindeutige bestätigende Handlung erfolgen sollte („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 kann gleichermaßen 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. Ausdrücklich als Willensbekundung ausgeschlossen ist dagegen (Still-)Schweigen („Silence"), bereits angekreuzte Kästchen oder Untätigkeit der betroffenen Person.

61 *Dammann/Simitis, EG-Datenschutzrichtlinie – Kommentar, Baden-Baden 1997, Artikel 2 Nr. 22.*

62 *Brühann: in Grabitz/Hilf, Das Recht der Europäischen Union, 40. Auflage 2009, Loseblattsammlung, Stand: Mai 1999 Ergänzungslieferung 13, A30, Artikel 2 Rn. 27.*

63 *Zur Richtlinie 95/46/EG bejahend: Dammann/Simitis, EG-Datenschutzrichtlinie, Baden Baden 1997, Artikel 2 Nr. 22; dagegen: Brühann: in Grabitz/Hilf, Das Recht der Europäischen Union, 40. Auflage 2009, Loseblattsammlung, Stand: Mai 1999 Ergänzungslieferung, A30, Artikel 2 Rn. 27. Siehe außerdem die Studie zur Umsetzung der Richtlinie 95/46/EG unter http://ec.europa.eu/justice/policies/privacy/docs/lawreport/consultation/technical-annex_en.pdf („Analysis and impact study on the implementation of Directive EC 95/46 in Member States") und dort zur Umsetzung der Einwilligungsvoraussetzungen, S. 4/5: "Neither the French nor the UK and Irish laws define the concept of 'consent' at all. It appears that under UK and also Finnish law in some cases implied consent may be valid but not if the data is sensitive data, so the character of the data gathered is significant in this regard."*

64 *Artikel-29-Datenschutzgruppe, WP 187, Stellungnahme 15/2011 zur Definition von Einwilligung, angenommen am 13. Juli 2011, S. 13.*

Die Frage ist daher, ob eine konkludente Willensbekundung nach der Datenschutz-Grundverordnung möglich ist.[65] Zu berücksichtigen ist, dass gemäß Wortlaut eine „Erklärung“ oder „sonstige bestätigende Handlung“ denkbar ist. Insgesamt kann Erwägungsgrund 32 als Auslegungshilfe herangezogen werden: Eine Person muss eindeutig ihr Einverständnis mit der beabsichtigten Verarbeitung ihrer personenbezogenen Daten signalisieren und ihr Einverständnis unmissverständlich bekunden. Eine konkludente Willenserklärung erfüllt grundsätzlich diese Voraussetzungen und ist nicht mit „Schweigen“ gleichzusetzen. Hier kann sich aus den Gesamtumständen eine Einwilligung ergeben, wobei es nach deutschem Recht nicht auf das tatsächlich Erklärte, sondern auf den objektiven Empfängerhorizont ankommt. Maßstab sind §§ 133, 157 BGB, wonach eine Willenserklärung nach Treu und Glauben auszulegen ist.

Bloßes Schweigen kann kein Einverständnis darstellen. Allerdings gibt es die so genannte „stillschweigende“ Willenserklärung, die in einem schlüssigen bzw. konkludenten Verhalten bestehen kann und nicht in einem reinen Schweigen. Insoweit ist der Begriff „stillschweigend“ missverständlich. Willenserklärungen können grundsätzlich konkludent abgegeben werden, es sei denn, es bestehen besondere Formvorschriften. Ausdrückliche und konkludente Willenserklärungen sind im Zivilrecht als gleichwertig zu betrachten. Bei letzterer findet das Gewollte nicht unmittelbar in einer Erklärung Ausdruck, sondern der Erklärende nimmt Handlungen vor, die mittelbar einen Schluss auf einen bestimmten Rechtsfolgewillen zulassen.[66] Sofern die Person kein entsprechendes Erklärungsbewusstsein hat („Trierer Weinversteigerungsfall“), gelten nach deutschem Recht die Regelungen der Auslegung gemäß §§ 133, 157 BGB und der Anfechtung gemäß §§ 119 ff. BGB.[67] Es wird außerdem zum Bundesdatenschutzgesetz vertreten, dass „konkludent“ derselbe Wert zukomme wie „ausdrücklich“.[68]

Da sich aus der Historie der Datenschutz-Grundverordnung ergibt, dass das im ersten Entwurf vorgesehene Merkmal „explizit“ oder „ausdrücklich“ gestrichen wurde bzw. sich nicht durchsetzen konnte,[69] ist fraglich, ob die Möglichkeit einer konkludenten Einwilligung angenommen werden kann. – unabhängig davon, dass der Diensteanbieter für deren Vorliegen gemäß Artikel 7 Absatz 1 Datenschutz-Grundverordnung nachweispflichtig ist. Für die grundsätzliche Zulässigkeit einer konkludenten Einwilligung könnte sprechen, dass die Datenschutz-Grundverordnung in Artikel 4 Nr. 11 formuliert, dass die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist. Die Artikel-29-Datenschutzgruppe vertritt in Bezug auf die Richtlinie 95/46/EG die Auffassung, dass das Verfahren zur Einholung und Erteilung der Einwilligung keinen Zweifel an der Einwilligungsabsicht der betroffenen Person lassen darf.[70] Die für die Datenverarbeitung Verantwortlichen seien damit zur Schaffung stabiler Verfahren gezwungen und könnten entweder eine klare, ausdrückliche Einwilligung anstreben oder sich auf Verfahren verlassen, die die eindeutige, konkludente

65 Für die Möglichkeit einer konkludenten Einwilligung (allerdings noch im Hinblick auf den ersten Entwurf der Datenschutz-Grundverordnung) siehe Rogosch, Die Einwilligung im Datenschutzrecht, S. 62 (und die dortigen Verweise). Gemäß Wortlaut des ersten Entwurfs der Datenschutz-Grundverordnung (2012) bedeutete Einwilligung “ any freely given specific, informed and explicit indication of his or her wishes…“). Hier ist wichtig, in welchem Sinne „explicit“ zu verstehen ist. In anderem Kontext wurde dieser Begriff von den Mitgliedstaaten unterschiedlich ausgelegt (siehe hierzu S. 34 ff.). „Explicit“ kann jedoch gleichermaßen eine konkludente Einwilligung sein, sofern dies wie im Rahmen der Zweckbestimmung („explicit purposes“, Artikel 5 Absatz 1b) Datenschutz-Grundverordnung) mit „eindeutig“ und nicht mit „ausdrücklich“ übersetzt wird und ein objektiver Maßstab zugrunde gelegt wird. Die aktuelle Fassung der Datenschutz-Grundverordnung enthält die Formulierung „unambigous indication“, was mit „unmissverständlich“ übersetzt wird und daher auch in einem konkludenten Sinne verstanden werden kann.

66 Siehe Ellenberger in: Palandt, Bürgerliches Gesetzbuch, 76. Auflage 2017, Einführung vor § 116 BGB Rn. 6/7.

67 Siehe Ellenberger in: Palandt, Bürgerliches Gesetzbuch, 76. Auflage 2017, Einführung vor § 116 BGB Rn. 6.

68 Zum BDSG: Steidle, Multimedia-Assistenten im Betrieb, S. 205 mit Verweis auf die gegenteiligen Ansichten. Gegenteilige Ansicht etwa Simitis in: Simitis, Bundesdatenschutzgesetz, 8. Auflage 2014, § 4a Rn. 78, dass konkludente Erklärungen nicht den gesetzlichen Anforderungen entsprechen.

69 Siehe Anhang 3. „Historie Einwilligung und Transparenz unter der EU-Datenschutz-Grundverordnung“ der Studie der Stiftung Datenschutz.

70 Artikel-29-Datenschutzgruppe, WP 187, Stellungnahme 15/2011 zur Definition von Einwilligung, angenommen am 13. Juli 2011, S. 25.

Einwilligung der Person übermitteln.[71] Es kann also grundsätzlich ebenso ein Verhalten sein, aus dem zu Recht die Einwilligung geschlossen werden kann.[72]

Die Artikel-29-Datenschutzgruppe führt weiterhin klarstellend aus, dass sowohl in der Offline- als auch in der Online-Welt dieselben Anforderungen gelten, und zwar einschließlich der Einwilligung „ohne jeden Zweifel", wobei allerdings das Risiko einer missverständlichen Einwilligung in der Online-Welt größer sei.[73] Dennoch sei es möglich, unter manchen Umständen eine Einwilligung „ohne jeden Zweifel" aus bestimmten Handlungen zu schließen. Dazu müssten jedoch die einschlägigen Informationen über die Datenverarbeitung gegeben worden sein, so dass die betroffene Person wirklich eine Entscheidung treffen könne (wer ist der für die Datenverarbeitung Verantwortliche, was sind die Zwecke der Verarbeitung usw.).[74]

Im Hinblick auf die Datenschutz-Grundverordnung wären diese Ausführungen unter der Maßgabe der oben dargestellten Einwilligungsvoraussetzungen anzuwenden, so dass eine solche Einwilligung nicht in der irreführenden Bezeichnung „stillschweigende Willenserklärung" zu verstehen ist, sondern vielmehr im Sinne eines unterstellten „Tuns" in der Erklärung.

Zu berücksichtigen ist ebenso, dass bei einer Beeinträchtigung des grundrechtlich anerkannten Persönlichkeitsschutzes (Recht am eigenen Bild, Recht am gesprochenen Wort) eine Einwilligung konkludent erteilt werden kann. Hier kann es nach dem Bundesverfassungsgericht gleichermaßen darauf ankommen, ob „ein bestimmtes Verhalten in einem solchen Maße üblich und geradezu selbstverständlich ist, dass entsprechend dem Grundgedanken des § 157 BGB nach Treu und Glauben und mit Rücksicht auf die Verkehrssitte vernünftigerweise nur von einer Zustimmung des Betroffenen ausgegangen werden kann, sofern er dem Verhalten nicht widerspricht."[75] [76]

Die Frage ist allerdings, was bei einem interaktiven Dialog zwischen Betroffenem und Diensteanbieter unter einem solchen „Tun" zu verstehen ist, ob - etwa bei entsprechender transparenter Darstellung und Information - die bloße Weiternutzung des Dienstes einer solchen Handlung entspricht und mit Rücksicht auf die „Verkehrssitte" vernünftigerweise von einer Zustimmung des Betroffenen ausgegangen werden kann. Hier kann beispielhaft auf die Vorgehensweise der Datenschutzaufsichtsbehörde von Großbritannien in Bezug auf Cookies verwiesen werden. Es muss jedoch im Einzelfall stets geprüft werden, ob ein Erklärungsakt vorliegt.
Insgesamt ist Vorsicht geboten, ob tatsächlich ein Mehr an Transparenz ein Weniger an Einwilligung aufwiegen kann, da der Erklärungsempfänger (hier der Diensteanbieter) bei digitalen Diensten nicht

71 Artikel-29-Datenschutzgruppe, WP 187, Stellungnahme 15/2011 zur Definition von Einwilligung, angenommen am 13. Juli 2011, S. 25.

72 Artikel-29-Datenschutzgruppe, WP 187, Stellungnahme 15/2011 zur Definition von Einwilligung, angenommen am 13. Juli 2011, S. 13/14.

73 Artikel-29-Datenschutzgruppe, WP 187, Stellungnahme 15/2011 zur Definition von Einwilligung, angenommen am 13. Juli 2011, S. 27.

74 Artikel-29-Datenschutzgruppe, WP 187, Stellungnahme 15/2011 zur Definition von Einwilligung, angenommen am 13. Juli 2011, S. 27.

75 BVerfG, Beschluss des Ersten Senats vom 09. Oktober 2002 - 1 BvR 1611/96 - Rn. (1-63), http://www.bverfg.de/e/rs20021009_1bvr161196.html

76 BVerfG, Beschluss der 1. Kammer des Ersten Senats vom 02. April 2003 - 1 BvR 215/03 - Rn. (1-10), http://www.bverfg.de/e/rk20030402_1bvr021503.html: „Eine stillschweigende Einwilligung lässt sich zwar nicht allein aus der faktischen Verbreitung von Mithöreinrichtungen und dem Fehlen eines Widerspruchs gegen deren Benutzung herleiten. Anders liegt es aber, wenn entsprechend dem Grundgedanken des § 157 BGB nach Treu und Glauben und mit Rücksicht auf die Verkehrssitte vernünftigerweise nur von einer Zustimmung des Betroffenen ausgegangen werden kann, sofern er dem Verhalten nicht widerspricht"; siehe außerdem Gola, Handbuch zum Arbeitnehmerdatenschutz, Rn. 776 und 795, letzteres zu der Frage, ob ein Arbeitnehmer seine Einwilligung zu Kontrollmaßnahmen der privaten Nutzung von Telekommunikationstechniken inzident erklären kann, wenn er Kenntnis von diesen hat.

im Sinne eines tatsächlichen „Gegenüberstehens“ handelt und damit nicht in gleichem Maße schutzwürdig ist. Er gibt schließlich die Bedingungen vor. Fraglich ist, welche (besonders hohen) Anforderungen einer transparenten Information erfüllt sein müssen, um letztendlich eine konkludente, aber unmissverständliche und freiwillige Einwilligung unterstellen zu können. Entsprechend den allgemeinen Grundsätzen muss der Erklärungsempfänger schutzbedürftig sein. Er darf Vertrauen auf einen bestimmten Erklärungsinhalt haben. Ansonsten ist zu prüfen, ob er mit dem Fehlen des Erklärungsbewusstseins rechnen musste.[77]

Bei der Bewertung muss gleichermaßen folgendes berücksichtigt werden: Gemäß der Richtlinie 95/46/EG muss die betroffene Person die Datenverarbeitung akzeptieren.[78] Die Datenschutz-Grundverordnung regelt in Artikel 4 Nr. 11 hingegen, dass die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

Diese Änderung des Wortlauts könnte dafür sprechen, dass inhaltlich nun weniger auf die innere Haltung, sondern eher auf den objektiven Empfängerhorizont Bezug genommen wird (was wiederum für eine konkludente Einwilligung sprechen könnte). Insgesamt scheint daher eine Verlagerung von Betroffenensicht auf die Empfängersicht einzutreten.

Dies bedeutet aber auch, dass sich hier die Anforderungen an die Einwilligung im Laufe der Zeit auch ändern können, da an den verständigen Durchschnittsverbraucher zukünftig andere Maßstäbe angelegt werden könnten als zur jetzigen Zeit, entsprechend dem Vergleich zu Zeiten der Verabschiedung der Richtlinie 95/46/EG zu dem heutigen Wissen des „Durchschnittsbetroffenen“. Hierzu hat die Artikel-29-Datenschutzgruppe bereits ausgeführt, dass ein regelmäßiger/durchschnittlicher Nutzer dazu in der Lage sein sollte, die Einwilligung zu verstehen.[79] Auch wenn sich dies auf die Qualität von verständlichen Informationen bezieht, ist fraglich, wie zukünftig der durchschnittliche Nutzer im Netz aussieht und welche Verhaltensweise man ihm (entsprechend dem „Trierer Weinversteigerungsfall“) als Willensbekundung unter dem Gesichtspunkt des Vertrauensschutzes unterstellen kann.

77 Ellenberger in: Palandt, Bürgerliches Gesetzbuch, 76. Auflage 2017, Einführung vor § 116 BGB Rn. 17.

78 Gemäß Artikel 2h) der Richtlinie 95/46/EG ist eine Einwilligung der betroffenen Person“ jede Willensbekundung, die ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgt und mit der die betroffene Person akzeptiert, dass personenbezogene Daten, die sie betreffen, verarbeitet werden.

79 Artikel-29-Datenschutzgruppe, WP 187, Stellungnahme 15/2011 zur Definition von Einwilligung, angenommen am 13. Juli 2011, S. 23.

! Fazit Nr. 4

Die Datenschutzaufsichtsbehörden in Deutschland sollten bereits zum jetzigen Zeitpunkt gemeinsam klare Anforderungen für die Gestaltung einer Einwilligungserklärung formulieren.[81] Damit könnten vorausschauend Leitlinien festgelegt werden, vor allem im Hinblick auf die zukünftige Ausarbeitung von Verhaltensregeln sowie auf die Formulierung, dass der Ausdruck „Einwilligung" ebenso „eine sonstige eindeutige bestätigende Handlung bezeichnet, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist" (siehe auch die vorangegangenen Fazits). In diesem Zusammenhang kann gleichermaßen dazu Stellung genommen werden, ob auch im Datenschutzrecht eine konkludente Einwilligung möglich ist, womit im besonderen Maße berücksichtigt werden muss, ob ein „Mehr" an Transparenz ein „Weniger" an Einwilligung aufwiegen kann.

Aufgrund der in der Vergangenheit unterschiedlichen Auslegung durch die Mitgliedsstaaten und Aufsichtsbehörden (siehe Cookies), sollte der Europäische Datenschutzausschuss zukünftig eine Leitlinie hinsichtlich der Einwilligungskriterien formulieren, um die einheitliche Anwendung der Datenschutz-Grundverordnung sicherzustellen oder die bereits vorhandenen Empfehlungen der Artikel-29-Datenschutzgruppe als bewährtes Verfahren bekräftigen.

Der Europäische Datenschutzausschuss könnte im besonderen Maße die Ausarbeitung von Verhaltensregeln durch Verbände und andere Vereinigungen bezüglich der Einwilligungskriterien fördern und durch eine Leitlinie klarstellen, unter welchen Voraussetzungen eine Verarbeitungstätigkeit im Zusammenhang mit der Bereitstellung von Webinhalten und einer damit verbundenen elektronischen Einwilligung aufgrund der grundsätzlichen weltweiten Abrufbarkeit regelmäßig „mehrere Mitgliedstaaten" betrifft.

2. Relevanz für den Einwilligungsassistenten

(1) Aktives Tun

Der Einwilligungsassistent könnte diese Unklarheiten für den Betroffenen insoweit beseitigen, wenn dieser im Vorhinein die Datenverarbeitung selbstständig durch seine Voreinstellung bestimmen kann und sich damit die Frage einer konkludenten Einwilligung nicht stellt.

Dazu müsste der Nutzer durch aktives Anklicken von einzelnen Daten, Zwecken und Empfängern seinen Willen im Sinne eines „Tuns" ausdrücklich vornehmen können. Die Artikel-29-Datenschutzgruppe hat bereits im Jahre 2005 die Verwendung von leeren Kästchen empfohlen, die die Betroffenen zur Bekundung der vorherigen Einwilligung auf Websites ankreuzen können. Die Verwendung von bereits angekreuzten Kästchen erfülle die Voraussetzung nicht, dass die Einwilligung eine klare und eindeutige Willensbekundung sein muss.[82]

81 Siehe hierzu auch Düsseldorfer Kreis, „Orientierungshilfe zur datenschutzrechtlichen Einwilligungserklärung in Formularen", März 2016.

82 Artikel-29-Datenschutzgruppe, WP 114, Arbeitspapier der Artikel-29-Datenschutzgruppe über eine Gemeinsame Auslegung des Artikels 26 Absatz 1 der Richtlinie 95/46/EG vom 24. Oktober 1995, Arbeitspapier vom 25. November 2005, S. 12.

Eine bewusste und eindeutige Einwilligung könne nicht über eine Opt-Out-Lösung erlangt werden, bei dem der Nutzer erst die entsprechende Voreinstellung abwählen muss, indem er z. B. ein bereits aktiviertes Kreuzchen deaktivieren müsse.[83]

Zu berücksichtigen ist allerdings (insbesondere bei einer automatischen und maschinenlesbaren Erstellung einer Einwilligungsliste für unterschiedliche Daten und Zwecke durch Abgleich mit den Datenschutzhinweisen des Empfängers bzw. Vertragspartners/Dienstanbieters), inwieweit tatsächlich eine Einwilligung für unterschiedliche Daten und Zwecke eingeholt werden muss oder diese Verarbeitung nicht bereits durch eine andere Legitimationsgrundlage abgedeckt ist. Die Artikel-29-Datenschutzguppe führt hierzu aus, dass entweder die Verarbeitung für die Erfüllung eines Vertrags notwendig ist oder die Einwilligung (ohne Zwang) eingeholt werden muss, wobei bei einigen Transaktionen gleichzeitig eine Reihe von Rechtsgrundlagen Anwendung finden könnten[84]: Das schließe zwar die gleichzeitige Anwendung mehrerer Rechtsgrundlagen nicht aus, aber diese müssten auch im richtigen Zusammenhang genutzt werden. Angeführt wird das Beispiel eines Autokaufs, bei welchem einige Datenerhebungen und Weiterverarbeitungen möglicherweise gemäß dem Vertrag mit der betroffenen Person erforderlich sind, andere Verarbeitungen könnten als Ergebnis einer rechtlichen Verpflichtung notwendig sein, andererseits könnte die Erhebung zusätzlicher Informationen eine gesonderte Einwilligung erfordern oder sogar unter dem Ausgleich der Interessen zulässig sein.[85]

Dies bedeutet für den Einwilligungsassistenten gleichermaßen, dass hier gegebenenfalls eine automatisierte Erstellung einer Einwilligungsliste durch Abgleich und Übersetzung der Datenschutzhinweise (d.h. der Information über die geplante Datenverarbeitung) mit Schwierigkeiten verbunden sein könnte, da die rechtliche Bewertung immer für den Einzelfall vorgenommen werden muss. Hier kommt es darauf an, inwieweit die rechtlichen Vorgaben überhaupt automatisiert technisch berücksichtigt werden können. Zu berücksichtigen ist jedoch, dass bei Einholung einer Einwilligung immer auch das Widerspruchsrecht gemäß Artikel 7 Absatz 3 Datenschutz-Grundverordnung gilt.

(2) Standortdaten

Der Einwilligungsassistent könnte im Rahmen von Arbeitsverhältnissen eingesetzt werden, wo es nach den Erwägungen der Artikel-29-Datenschutzgruppe erforderlich ist, dass der Arbeitnehmer bei Fahrzeugen, die ihm auch für den privaten Gebrauch zur Verfügung gestellt werden, mit einem System ausgestattet werden, das es dem Arbeitnehmer erlaubt, die Standortbestimmungsfunktion auszuschalten.[86]

In Bezug auf Standortdaten ist insgesamt besonders zu berücksichtigen, dass Artikel 9 der Richtlinie 2002/58/EG entweder die Anonymisierung oder die Einwilligung verlangt. Dies kann der Einwilligungsassistent durch vorheriges Anklicken der Verwendung von Standortdaten für bestimmte Zwecke sicherstellen. Ansonsten ist zu berücksichtigen, dass wie oben dargestellt - anders als im Sinne von § 98 Telekommunikationsgesetz und der Intention von § 4a BDSG - eine konkludente Einwilligung ausreichend sein könnte und nicht mehr wie bisher sogar eine schriftliche Einwilligung erforderlich ist,

83 *Düsseldorfer Kreis, S. 15 -Orientierungshilfe- Datenschutzanforderungen an App-Entwickler und App-Anbieter vom 16.06.2014.*

84 *Artikel-29-Datenschutzgruppe, WP 187, Stellungnahme 15/2011 zur Definition von Einwilligung, angenommen am 13. Juli 2011, S. 9.*

85 *Artikel-29-Datenschutzgruppe, WP 187, Stellungnahme 15/2011 zur Definition von Einwilligung, angenommen am 13. Juli 2011, S. 9.*

86 *Artikel-29-Datenschutzgruppe, WP 115, Stellungnahme 5/2005 der Gruppe 29 zur Nutzung von Standortdaten für die Bereitstellung von Diensten mit Zusatznutzen, angenommen am 25. November 2005, S.11.*

wenn die Standortdaten für einen Dienst mit Zusatznutzen verarbeitet werden, der die Übermittlung von Standortdaten eines Mobilfunkendgerätes an einen anderen Teilnehmer oder an Dritte, die nicht Anbieter des Dienstes mit Zusatznutzen sind, zum Gegenstand hat.

Der Düsseldorfer Kreis verweist außerdem darauf, dass es bei Standortdaten häufig nicht notwendig ist, dass der Standort des Nutzers metergenau erhoben wird.[87] Auch die Speicherdauer ist von besonderer Relevanz und muss sich für jedes personenbezogene Datum am Grundsatz der Erforderlichkeit messen lassen.[88]

(3) IP-Adresse

Bei der Inanspruchnahme von Webangeboten fällt notwendigerweise ebenso die IP-Adresse an.
In Bezug auf die IP-Adresse ist zu berücksichtigen, dass die automatisierte Erstellung einer Einwilligungsliste durch Abgleich mit den Datenschutzhinweisen zu einem Widerspruchsrecht gemäß Artikel 7 Absatz 3 Datenschutz-Grundverordnung führen könnte, wenn dadurch eine Einwilligung für die Verarbeitung der IP-Adresse durch einen Anbieter eines Dienstes der Informationsgesellschaft eingeholt werden würde: In Datenschutzhinweisen wird regelmäßig auch über die Verarbeitung der IP-Adressen informiert, aber in vielen Fällen ist eine Rubrik „Datenschutz“ zu finden, in welcher sämtliche Verarbeitungstätigkeiten beschrieben werden. Der Einwilligungsassistent müsste also in der Lage sein, zwischen „einwilligungsbedürftig“ und „nur informationspflichtig“ innerhalb der Datenschutzerklärung zu unterscheiden, sofern ein automatisierter Abgleich erfolgt. Anderenfalls muss ein Anbieter im Vorhinein auf die entsprechende Unterscheidung achten.

In Bezug auf IP-Adressen ist das Urteil des Europäischen Gerichtshofs vom 19.10.2016 zu berücksichtigen, nach dem eine Verarbeitung personenbezogener Daten (wozu auch eine IP-Adresse gehören kann) gemäß Artikel 7f der Richtlinie 95/46/EG rechtmäßig sein kann, wenn sie zur Verwirklichung des berechtigten Interesses des für die Verarbeitung Verantwortlichen erforderlich ist, sofern nicht das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person überwiegen.[89] Damit kann die Funktionsfähigkeit eines Online-Medium grundsätzlich gegen das Interesse oder die Grundrechte oder die Grundfreiheiten der Nutzer abgewogen werden. Diesbezüglich erscheint es schwierig, eine solche Interessenabwägung automatisiert durchzuführen.

Diese Erwägungen müssen gleichermaßen für die Datenschutz-Grundverordnung und Artikel 6f gelten. Zu berücksichtigen ist, dass die Voraussetzungen der Einwilligung nicht mit dem Widerspruchsrecht verwechselt werden dürfen: Eine Einwilligung muss vor Datenverarbeitung eingeholt werden, erst dann dürfen die Daten verarbeitet werden. Nur gemäß Artikel 6f Datenschutz-Grundverordnung dürfen die Daten verarbeitet werden (wenn die entsprechenden Voraussetzungen nach Interessenabwägung vorliegen), wenn die betroffene Person der Datenverarbeitung nicht widersprochen hat.[90]

87 *Düsseldorfer Kreis, S. 17 -Orientierungshilfe- Datenschutzanforderungen an App-Entwickler und App-Anbieter vom 16.06.2014.*

88 *Düsseldorfer Kreis, S. 17 -Orientierungshilfe- Datenschutzanforderungen an App-Entwickler und App-Anbieter vom 16.06.2014.*

89 *Urteil des Europäischen Gerichtshofs vom 19.10.2016 C-582/14; http://curia.europa.eu/juris/document/document.jsf?text=&docid=184668&pageIndex=0&doclang=de&mode=lst&dir=&occ=first&part=1&cid=780392 sowie Urteilsberichtigung vom 06.12.2016 http://curia.europa.eu/juris/document/document.jsf?text=&docid=186141&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1 . Siehe ebenso Pressemitteilung des Europäischen Gerichtshofs http://curia.europa.eu/jcms/upload/docs/application/pdf/2016-10/cp160112de.pdf*

90 *Siehe hierzu bzw. zu den Voraussetzungen von Artikel 7a und 7f der Richtlinie 95/46/EG die Ausführungen der Artikel-29-Datenschutzgruppe, WP 187, Stellungnahme 15/2011 zur Definition von Einwilligung, angenommen am 13. Juli 2011, S. 11.*

(4) Cookies

Aufgrund der Ausführungen zur konkludenten Einwilligung sowie der beispielhaften Darstellung der Vorgehensweise in den Niederlanden sowie der Datenschutzaufsichtsbehörde von Großbritannien stellt sich die Frage, ob in Cookies nicht ausdrücklich eingewilligt werden muss und ob die Voreinstellungen eines verwendeten Einwilligungsassistenten unterstützend zur Wahrung der Selbstbestimmungsrechte der Nutzer eingesetzt werden könnten.

Die Artikel-29-Datenschutzgruppe steht -wie oben bereits ausgeführt- den Einstellungsmöglichkeiten durch Browser kritisch gegenüber. Zu prüfen ist daher, ob es andere technische Verfahren gibt oder solche entwickelt werden können, die die betroffenen Personen besser in ihrer informationellen Selbstbestimmung unterstützen und ob der Einwilligungsassistent ein solches technisches Verfahren bewerkstelligen kann. Dabei sind folgende Erwägungen zu berücksichtigen:

Die Artikel-29-Datenschutzgruppe ist weiterhin der Ansicht, dass Cookie-basierte Opt-Out-Mechanismen im Allgemeinen keinen angemessenen Mechanismus zur Einholung der Einwilligung in Kenntnis der Sachlage darstellen. In den meisten Fällen werde die Einwilligung des Nutzers impliziert, wenn er von der Opt-Out-Möglichkeit nicht Gebrauch mache. Tatsächlich machten aber nicht deshalb nur so wenige Leute von der Opt-out-Möglichkeit Gebrauch, weil sie sich in Kenntnis der Sachlage für eine Einwilligung in die Werbung auf Basis des Behavioural Targeting entschieden haben, sondern weil sie nicht wissen, dass eine Verarbeitung stattfindet und erst recht nicht, wie sie von dem Opt-out Gebrauch machen könnten.[91]

Außerdem wird nochmals die Wichtigkeit von Privacy by Design betont.[92]

In ihrer Stellungnahme zur verhaltensorientierten Online-Werbung stellt die Artikel-29-Datenschutzgruppe klar, dass im Sinne einer gültigen und wirksamen Einwilligung Browser oder andere Einstellungen die betroffenen Personen auffordern müssten, durch eine bejahende Handlung sowohl das Setzen eines Cookies als auch die fortdauernde Übermittlung von in den Cookies enthaltenen Informationen zu akzeptieren.[93]

Ein Einwilligungsassistent könnte dies sinnvoll unterstützen. Dies gilt insbesondere vor dem Hintergrund, dass gemäß der obigen Ausführungen (s. S. 19 ff.) die betroffene Person gemäß Artikel 13 Datenschutz-Grundverordnung bei Erhebung der Daten und nicht entsprechend § 13 Telemediengesetz zu Beginn des Nutzungsvorgangs informiert werden muss. Die Schutzfunktion der Einwilligung wäre also gewahrt, da die betroffene Person vor der übereilten Preisgabe ihrer personenbezogenen Daten bewahrt werden könnte. Lässt man hier Voreinstellungen zu, um diese anschließend mit den Datenschutzhinweisen der Webseite abzugleichen, wäre der Übereilungsschutz unter der Voraussetzung erfüllt, dass der Webseitenbetreiber tatsächlich erst dann Cookies erhebt, wenn die Einstellungen dies zulassen. Dies erfordert aber gleichermaßen eine technische Zusammenarbeit, die etwa bei P3P (siehe Bestandsaufnahme) in der Vergangenheit nicht funktioniert hatte. Im Hinblick auf die Information gilt zudem aktuell gemäß § 13 Absatz Satz2 Telemediengesetz, dass die Unterrichtungspflicht auch

91 Artikel-29-Datenschutzgruppe, WP 171 Stellungnahme 2/2010 zur Werbung auf Basis von Behavioural Targeting, angenommen am 22. Juni 2010, S. 29.

92 Artikel-29-Datenschutzgruppe, WP 171 Stellungnahme 2/2010 zur Werbung auf Basis von Behavioural Targeting, angenommen am 22. Juni 2010, S. 29.

93 Artikel-29-Datenschutzgruppe, WP 188 Stellungnahme 16/2011 zur Best-Practice-Empfehlung von EASA und IAB zu verhaltensorientierter Online-Werbung, angenommen am 8. Dezember 2011; S. 11/12

dann greift, wenn die Daten zunächst ohne Personenbezug erhoben werden, ein solcher aber jederzeit hergestellt werden kann.[94] Je nachdem, wie der Zeitpunkt der Unterrichtung zukünftig definiert wird, wäre auch dieser Umstand zu beachten.

Zu berücksichtigen sind hierbei außerdem die obigen Ausführungen: Nach der Intention der Richtlinie 2002/58/EG dürfen erforderliche Cookies (etwa für den Warenkorb oder zur technischen Funktionsfähigkeit der Webseite) ohne Einwilligung des Nutzers erhoben werden. Der Einwilligungsassistent sollte daher in Bezug auf solche Cookies keine Einwilligung einholen, sondern es müsste eine transparente Information sichergestellt sein, dass diese Cookies erhoben werden. Anderenfalls würden dem Nutzer bei jeder Einwilligung auch Widerrufsrechte gemäß Artikel 7 Absatz 3 Datenschutz-Grundverordnung zustehen.

! Fazit Nr. 5

Der Einwilligungsassistent sollte die Übersetzung der Datenschutzhinweise in eine maschinenlesbare Form durch die Darstellung von leeren Kästchen vornehmen, die der Nutzer aktiv ankreuzen muss.
Eine konkludente Einwilligung ist damit ausgeschlossen.

In Bezug auf Standortdaten muss im besonderen Maße die Möglichkeit „einer anderen Verhaltensweise“ und konkludenten Einwilligungsmöglichkeit kritisch geprüft werden. Hier gelten die Anforderungen der Richtlinie 2002/58/EG. Das Telekommunikationsgesetz muss entsprechend angepasst werden.

Bei einer automatisierten Erstellung einer Einwilligungserklärung anhand der Übersetzung der Datenschutzhinweise[95] des Dienstanbieters muss beachtet werden, dass die zur Vertragserfüllung erforderlichen Daten nicht der Einwilligung unterliegen. Wird eine Einwilligung dennoch eingeholt, steht der betroffenen Person auch ein entsprechendes Widerspruchsrecht gemäß Artikel 7 Absatz 3 Datenschutz-Grundverordnung zu. Zu prüfen wäre, ob es in diesem Falle sogar unbillig wäre, wenn sich der Dienstanbieter im Nachhinein auf andere Gründe der rechtmäßigen Datenverarbeitung berufen würde (Erforderlichkeit oder berechtigtes Interesse), so dass die Datenverarbeitung vollständig unterbleiben müsste.
Die transparente Information über die Datenverarbeitung aufgrund anderer Rechtsgrundlagen muss somit klar von der Einwilligung abgegrenzt werden. Es muss berücksichtigt werden, inwieweit eine Darstellung und Prüfung insgesamt automatisiert erfolgen kann. Anderenfalls müssten die Datenschutzhinweise entsprechend angepasst werden. Dies bezieht sich auch auf die Verarbeitung der IP-Adresse, sofern über ihre Verarbeitung in den Datenschutzhinweisen informiert wird (an ihrer Verarbeitung könnte der Diensteanbieter ein berechtigtes Interesse haben, was im Einzelfall zu prüfen ist).

Zu berücksichtigen ist, dass die Voraussetzungen der Einwilligung nicht mit dem Widerspruchsrecht verwechselt werden dürfen: Eine Einwilligung muss vor Datenverarbeitung eingeholt werden, erst dann dürfen die Daten verarbeitet werden. Nur gemäß Artikel 6f Datenschutz-Grundverordnung dürfen die Daten verarbeitet werden (wenn die entsprechenden Voraussetzungen nach Interessenabwägung vorliegen), wenn die betroffene Person der Datenverarbeitung nicht widersprochen hat.
Auch vor dem Hintergrund, dass nach der Datenschutz-Grundverordnung eine Information des Nutzers

94 *Spindler/Nink in: Spindler/Schuster, Recht der elektronischen Medien, 3. Auflage 2015, § 13 TMG Rn. 3: Dies werde durch § 13 Abs. 1 Satz 2 deutlich, der auch die Erhebung in einem automatisierten Verfahren erfasse, welches die Verwendung personenbezogener Daten vorbereitet, wobei automatisierte Verfahren solche sind, die programmgesteuert, ohne auf einer individuellen Entscheidung des Verantwortlichen zu beruhen, initiiert werden.*

95 *Siehe hierzu die Beschreibung unter „Technische Konzepte“, S. 3 ff.*

! nicht zu Beginn des Nutzungsvorgangs sondern erst bei Erhebung der Daten erfolgen muss, sollten die Entwickler prüfen, ob der von Ihnen geplante Einwilligungsassistent in sinnvoller und für die Nutzer überschaubarer Weise für Cookies in Betracht kommen kann. Hier ist erforderlich, dass insgesamt die technischen Voraussetzungen geschaffen werden und die Systeme kompatibel sind. Daher hat die Artikel-29-Datenschutzgruppe ebenso vorgeschlagen, dass Entwickler und Webseitenbetreiber zur Zusammenarbeit bei Privacy by Design ermutigt werden sollten.[96] Beachtet werden muss dabei stets, dass für „erforderliche Cookies" keine Einwilligung eingeholt werden muss.

Im Sinne einer Vollharmonisierung des Datenschutzrechts sollte frühestmöglich ein einheitliches Verständnis über die Einwilligungsvoraussetzungen (auch bezüglich Cookies) erfolgen, selbst wenn die Tendenz in Deutschland eher in der Umsetzung eines aktiven Verhaltens bei der Einwilligung besteht. Hier ist die Formulierung in der Datenschutz-Grundverordnung entscheidend, nach der eine Einwilligung auch eine andere Verhaltensweise darstellen kann, mit der die betroffene Person in dem jeweiligen Kontext eindeutig ihr Einverständnis mit der beabsichtigten Verarbeitung ihrer personenbezogenen Daten signalisiert. Die Formulierung einheitlicher Verhaltensregeln kann von Nutzen sein, so dass Sanktionen für den mangelnden Nachweis der Einwilligung besser greifen können. Dies sollte europaweit erfolgen, soweit Verhaltensregeln aufgrund einer Verarbeitungstätigkeit in mehreren Mitgliedstaaten ausgearbeitet werden können.

II. „Für den bestimmten Fall in informierter Weise"

1. Allgemeine Voraussetzungen

(1) Bestimmter Fall

Artikel 2h der Richtlinie 95/46/EG regelt, dass die betroffene Person im Zeitpunkt der Willensbekundung die Sachlage und den konkreten Fall kennen muss. Dabei müssen alle Voraussetzungen der gesetzlichen Informationspflichten erfüllt sein.

Nach Artikel 4 Nr. 11 der Datenschutz-Grundverordnung ist eine für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung gefordert.

Es ist nun nicht mehr ein „konkreter", sondern ein „bestimmter" Fall genannt. Erwägungsgrund 32 der Datenschutz-Grundverordnung nimmt allerdings wiederum auf den „konkreten" Fall Bezug, so dass diese Begriffe synonym zu verwenden sind. In Erwägungsgrund 42 wird zudem die „Kenntnis der Sachlage" wieder aufgegriffen, auch wenn diese nicht unmittelbar im Verordnungstext steht. In diesem Sinne sollte die betroffene Person mindestens wissen, wer der Verantwortliche ist und für welche Zwecke ihre personenbezogenen Daten verarbeitet werden sollen.

Ein Unterschied zwischen der Richtlinie 95/46/EG und der Datenschutz-Grundverordnung ergibt sich jedoch hinsichtlich der Voraussetzungen der Datenverarbeitung. Nach Erwägungsgrund 28 der Richtlinie 95/46/EG müssen die Zwecke eindeutig sowie rechtmäßig sein und bei der Datenerhebung festgelegt werden. Die Verarbeitung personenbezogener Daten muss gegenüber den betroffenen Personen nach Treu und Glauben erfolgen. Die Zweckbestimmungen der Weiterverarbeitung nach der Erhebung dürfen nicht mit den ursprünglich festgelegten Zwecken unvereinbar sein. In der Datenschutz-Grundver-

96 *Artikel-29-Datenschutzgruppe, WP 171 Stellungnahme 2/2010 zur Werbung auf Basis von Behavioural Targeting, angenommen am 22. Juni 2010, S. 29*

ordnung wird diese Vorgabe insoweit abgeschwächt, dass gemäß Erwägungsgrund 39 die bestimmten Zwecke, zu denen die personenbezogenen Daten verarbeitet werden, eindeutig und rechtmäßig sein sollten (und nicht „müssen“!) und zum Zeitpunkt der Erhebung der personenbezogenen Daten feststehen sollten. Diese begriffliche Änderung darf jedoch nicht dazu führen, die Zwecke zukünftig flexibler zu gestalten. Hierfür spricht ebenso Erwägungsgrund 43 Datenschutz-Grundverordnung, der klarstellt, dass zu verschiedenen Verarbeitungsvorgängen von personenbezogenen Daten eine gesonderte Einwilligung erteilt werden soll, wenn dies im Einzelfall angebracht ist. Allerdings ist nicht eindeutig definiert, was „ein“ Verarbeitungsvorgang darstellt. Ist dies mit der Festlegung des Zwecks gleichzusetzen?

! Hierzu gilt folgendes:

Verarbeitung bedeutet nach Artikel 4 Nr. 2 Datenschutz-Grundverordnung 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.

! Die Artikel-29-Datenschutzgruppe nimmt zu Verarbeitungstätigkeiten wie folgt Stellung:[97]

Damit sie für den konkreten Fall ist, muss die Einwilligung verständlich sein: sie sollte sich eindeutig und genau auf den Anwendungsbereich und die Folgen der Datenverarbeitung beziehen. Sie kann nicht für Verarbeitungsaktivitäten gelten, die in keiner Weise eingegrenzt sind. Das heißt mit anderen Worten, dass der Kontext, in dem die Einwilligung gilt, eingeschränkt ist.

Weiter führt die Artikel-29-Datenschutzgruppe aus, dass die Einigung auf den angemessenen Erwartungen der Parteien basieren sollte, wobei die Anforderung der Granularität der Einwilligung in Bezug auf die verschiedenen Elemente, die die Datenverarbeitung ausmachen, zu berücksichtigen sei. Eine Einwilligung könne nicht „alle rechtmäßigen Zwecke“ abdecken, die der für die Datenverarbeitung Verantwortliche verfolgt, so dass sich die Einwilligung auf die Verarbeitung beziehen sollte, die in Bezug auf den Zweck angemessen und erforderlich ist.[98]

Allerdings ist im Sinne der Rechtauffassung der Artikel-29-Datenschutzgruppe zu berücksichtigen, dass es ausreichen soll, wenn der für die Datenverarbeitung Verantwortliche die Einwilligung einmal für verschiedene Verarbeitungstätigkeiten einholt, sofern die betroffene Person diese Tätigkeiten vernünftigerweise erwarten kann.[99] In einem vor dem Europäischen Gerichtshof verhandelten Fall (auf den sich auch die Artikel-29-Datenschutzgruppe in ihren Ausführungen bezogen hat), konnte die Einwilligung des Betroffenen aufgrund der eindeutigen Formulierung des Zwecks gleichzeitig die Weitergabe an unterschiedliche Empfänger abdecken.

97 *Artikel-29-Datenschutzgruppe, WP 187, Stellungnahme 15/2011 zur Definition von Einwilligung, angenommen am 13. Juli 2011, S. 20.*

98 *Artikel-29-Datenschutzgruppe, WP 187, Stellungnahme 15/2011 zur Definition von Einwilligung, angenommen am 13. Juli 2011, S. 20.*

99 *Artikel-29-Datenschutzgruppe, WP 187, Stellungnahme 15/2011 zur Definition von Einwilligung, angenommen am 13. Juli 2011, S. 21.*

Konkret ging es darum, dass das Bundesverwaltungsgericht in einem Vorabentscheidungsersuchen gemäß Artikel 267 AEUV dem Europäischen Gerichtshof die Klärung der Frage vorgelegt hatte, ob im Sinne des Artikel 12 der Richtlinie 2002/58/EG eine erneute Einwilligung des Betroffenen erforderlich ist, wenn dessen Daten durch andere Anbieter öffentlich zugänglicher Telefonauskunftsdienste und Teilnehmerverzeichnisse verwendet werden, obwohl der Betroffene in die Aufnahme seiner Daten in einen Auskunftsdienst bereits eingewilligt hat. Der Europäische Gerichtshof hat dies mit Verweis auf die Verarbeitung für dieselben Zwecke verneint.[100]

Im Sinne der Sicherung der Datenhoheit des Betroffenen sollte diese Entscheidung nicht in dem Sinne verallgemeinert werden, dass nun die Datenempfänger nicht mehr angegeben werden müssten. Ansonsten würde dies zu einer freien Verwendbarkeit von Daten führen.[101] Daher wird es bei der Ausgestaltung eines granularen, aber auch übersichtlichen Einwilligungskonzepts insgesamt davon abhängen, inwieweit der (eingeschränkte) Kontext eine Einwilligung für mehrere Verarbeitungsvorgänge hergibt. Hierfür sollten Verhaltensregeln aufgestellt werden.

Außerdem ist für den Verantwortlichen der Datenverarbeitung stets die Nachweispflicht gemäß Artikel 7 Absatz 1 Datenschutz-Grundverordnung zu berücksichtigen. In einem solchen Falle müsste ein Verantwortlicher daher nachweisen können, dass eine betroffene Person vernünftigerweise mit verschiedenen Verarbeitungstätigkeiten rechnen konnte. In Bezug auf elektronische Patientenakten hat die Artikel-29-Datenschutzgruppe etwa entschieden, dass sich sie Einwilligung „für den konkreten Fall“ auf eine genau umrissene konkrete Situation beziehen müsse, in der die Verarbeitung der medizinischen Daten erfolgen soll. Eine „pauschale Zustimmung“ der betroffenen Person, beispielsweise zur Erfassung ihrer medizinischen Daten in einer elektronischen Patientenakte und zur anschließenden Weitergabe dieser medizinischen Daten an in die Behandlung eingebundenen medizinischen Fachkräfte, wäre keine Einwilligung.[102] In diesem Zusammenhang verweist die Artikel-29-Gruppe auf die entsprechende Auslegung der Einwilligungsvoraussetzungen für Standortdaten. Danach könne die Einwilligung nicht im Zuge der Annahme der allgemeinen Bedingungen für die Nutzung der angebotenen elektronischen Kommunikationsdienste erteilt werden:[103] Abhängig von der Art der angebotenen Dienste könne sich die Einwilligung jedoch auf einen spezifischen Vorgang beziehen oder sie könne die Zustimmung zu einer kontinuierlichen Standortbestimmung darstellen. Die Bereitstellung eines Dienstes, der die automatische Standortbestimmung einer Person erfordert (z. B. die Möglichkeit, eine bestimmte Nummer anzurufen, um eine Wettervorhersage für den jeweiligen Standort zu erhalten), sei zulässig, sofern die Nutzer im Voraus vollständige Informationen über die Verarbeitung ihrer Standortdaten erhalten. In diesem Fall würde das Anrufen der entsprechenden Nummer bedeuten, dass die Einwilligung zur Standortbestimmung erteilt wird.[104]

Ergänzend ist hier außerdem auf die obigen Ausführungen zu verweisen (s. S. 19 ff.), dass zukünftig unklar ist, ob die Protokollierungspflicht (im deutschen Recht) in ihrer derzeitigen Form aufrechterhalten wird oder ob die Art und Weise der Erbringung des Nachweises gemäß Artikel 7 Absatz 1 (aber ebenso Artikel 5 Absatz 2 Datenschutz-Grundverordnung dem Verantwortlichen obliegt.

100 Urteil des Gerichtshofs vom 5. Mai 2011, Deutsche Telekom AG (Rechtssache C-543/09).

101 Siehe hierzu auch Radlaski, Das Konzept der Einwilligung in der datenschutzrechtlichen Realität, S. 49.

102 Artikel-29-Datenschutzgruppe, WP 187, Stellungnahme 15/2011 zur Definition von Einwilligung, angenommen am 13. Juli 2011, S. 21 mit Verweis auf WP 131, Arbeitspapier Verarbeitung von Patientendaten in elektronischen Patientenakten (EPA), 15. Februar 2007.

103 Artikel-29-Datenschutzgruppe, WP 187, Stellungnahme 15/2011 zur Definition von Einwilligung, angenommen am 13. Juli 2011, S. 21 mit Verweis auf WP 115, Stellungnahme 5/2005 der Gruppe 29 zur Nutzung von Standortdaten für die Bereitstellung von Diensten mit Zusatznutzen, angenommen am 25. November 2005, S. 6.

104 Artikel-29-Datenschutzgruppe, WP 115, Stellungnahme 5/2005 der Gruppe 29 zur Nutzung von Standortdaten für die Bereitstellung von Diensten mit Zusatznutzen, angenommen am 25. November 2005, S. 6.

Die Protokollierung kann eine Form des Nachweises sein, aber es könnte gegebenenfalls andere hilfreiche Methoden geben, was näher zu prüfen wäre. Hier empfehlen sich (genehmigte) Verhaltensregeln gemäß Artikel 24 Absatz 3, Artikel 40 Datenschutz-Grundverordnung.

(2) Bestimmter Zweck

Gemäß den obigen Ausführungen sollte sich die Einwilligung also auf die Verarbeitung(stätigkeit) beziehen, die in Bezug auf den Zweck angemessen und erforderlich ist. Auch Erwägungsgrund 32 der Datenschutz-Grundverordnung nimmt „auf einen oder mehrere Zwecke“ Bezug, zu welchen die betroffene Person ihre Einwilligung erteilen sollte, und Erwägungsgrund 39 regelt darüber hinaus, dass die personenbezogenen Daten für die Zwecke, zu denen sie verarbeitet werden, angemessen und erheblich sowie auf das für die Zwecke ihrer Verarbeitung notwendige Maß beschränkt sein sollten. Eine Zweckänderung wäre nur unter den Voraussetzungen des Artikels 6 Absatz 4 Datenschutz-Grundverordnung zulässig.
Durch Artikel 17 Datenschutz-Grundverordnung wird die Zweckbindung außerdem gestärkt, da nun gemäß Absatz 1a dieser Regelung die Daten zu löschen sind, wenn sie für die Zwecke, für die sie erhoben wurden, nicht mehr erforderlich sind.

Hier ist jedoch im europäischen Kontext darauf zu achten, dass die Mitgliedstaaten den Zweckbindungsgrundsatz der Richtlinie 95/46/EG bislang unterschiedlich ausgelegt haben und die Artikel-29-Datenschutzgruppe aus diesem Grunde Kriterien festgelegt hat.[105]

Um zukünftig diese Unterschiede zu vermeiden, ist nun erneut der Vergleich zwischen der Richtlinie 96/46/EG und Datenschutz-Grundverordnung hilfreich, um zu prüfen, ob hier Auslegungsspielräume einer Vollharmonisierung entgegenstehen könnten:
Erwägungsgrund 39 der Datenschutz-Grundverordnung regelt, dass die bestimmten Zwecke, zu denen die personenbezogenen Daten verarbeitet werden, eindeutig und rechtmäßig sein sollten und zum Zeitpunkt der Erhebung der personenbezogenen Daten feststehen sollten.

In der englischen Fassung heißt es: “In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data.”

Auf diesen Unterschied in der Zweckbestimmung hat bereits die Artikel-29-Datenschutzgruppe verwiesen:[106]
Sie führt im Hinblick auf die Richtlinie 95/46/EG aus, dass das Wort „explicit“ in die unterschiedlichen Sprachen nicht identisch übersetzt wurde. Erwägungsgrund 28 der Richtlinie 95/46/EG regelt: “whereas, in particular, the data must be adequate, relevant and not excessive in relation to the purposes for which they are processed; whereas such purposes must be explicit and legitimate and must be determined at the time of collection of the data”. Gemäß der Stellungnahme der Artikel-29-Datenschutzgruppe liege die Anforderung teilweise darin, den Fokus auf das Endergebnis zu legen, darauf, dass die Zwecke unzweifelhaft sein müssten und von allen Beteiligten in der gleichen Weise verstanden werden müssten (im Zweifel kann also der Zweck durch Auslegung ermittelt werden). In anderen Übersetzungen liege der Fokus dagegen mehr darauf, wie dieses Endergebnis erreicht werden könne, nämlich dass die Zwecke klar ausgedrückt und erklärt werden müssten.

105 Artikel-29-Datenschutzgruppe, „Opinion 03/2013 on purpose limitation“, WP 203 adopted on 2 April 2013, insbesondere S. 5.

106 Artikel-29-Datenschutzgruppe, „Opinion 03/2013 on purpose limitation“, WP 203 adopted on 2 April 2013, S. 17.

Zur näheren Erläuterung verweist die Artikel-29-Datenschutz-Gruppe auf die lateinische Wurzel von „explicit“ und darauf, dass in Deutschland dies mit „eindeutig“ übersetzt werde und dass hier der Fokus auf dem Ergebnis und nicht in der geäußerten und erklärenden Form liege.[107]

Die Artikel-29-Datenschutzgruppe führt im Übrigen aus, dass die Flexibilität der Regelungen zur Zweckbestimmung zu unterschiedlichen Anwendungen in den Mitgliedstaaten geführt habe und dass die Anforderung an „explicit purposes“ von der Bekanntmachung dieses Zwecks an die betroffene Person oder der Benachrichtigung der Datenschutzaufsichtsbehörden (Artikel 18 Richtlinie 95/46/EG) zu unterscheiden sei.[108] Die Mitteilung der Zwecke (gemäß Artikel 6 (1) (b) Richtlinie 96/46/EG) könne auf unterschiedliche Weise durchgeführt werden. So seien in manchen Mitgliedstaaten die „Zwecke“ sehr weit definiert worden und überdies variiere die Herangehensweise im Hinblick auf die Darstellung eines „expliziten“ Zwecks.[109] Teilweise könne dies durch eine Beschreibung der Zwecke in einer Benachrichtigung an die Datenschutzaufsichtsbehörde oder in einer Mitteilung an die betroffene Person umgesetzt werden, bei anderen Mitgliedstaaten genüge eine interne Information an den Datenschutzbeauftragten, wohingegen wieder andere sowohl Mitteilungen als auch Benachrichtigungen als ausreichendes Mittel betrachten, allerdings mit dem Hinweis, dass dies nicht die einzigen Möglichkeiten im Hinblick auf die Anforderungen an eine „explizite Zweckbestimmung“ (im Sinne von „making the purposes of the processing explicit“) sind.[110] Gemäß der Ausführungen der Artikel-29-Datenschutzgruppe kann die schriftliche Spezifizierung sowie die Erstellung einer angemessenen Dokumentation hilfreich sein, wobei im Einzelfall sogar auf die Notwendigkeit der schriftlichen Spezifizierung, etwa bei komplexer Datenverarbeitung, Bezug genommen wird.[111]

In der deutschen Fassung der Datenschutz-Grundverordnung wird „explicit“ in Artikel 9 Datenschutz-Grundverordnung zwar mit „ausdrücklich“ übersetzt, aber im Rahmen der Zweckbestimmung des Artikel 5 Absatz 1b Datenschutz-Grundverordnung mit „eindeutig“, so dass nicht unbedingt die Erklärung des Zwecks verlangt wird. Die von der Artikel-29-Datenschutzgruppe benannte „schriftliche“ Spezifizierung stellt im Übrigen keine Voraussetzung dar.

Die Frage ist, wie die übrigen Mitgliedstaaten im Hinblick auf die Datenschutz-Grundverordnung die Begrifflichkeiten verwenden werden, ob die Zweckbestimmung immer noch in einem weiten Verständnis definiert wird und ob die erklärende Form durch eine andere Übersetzung des Erwägungsgrunds 39 Datenschutz-Grundverordnung hätte erreicht werden können, etwa: „Die näher beschriebenen/einzelnen Zwecke sollten genau/ausdrücklich angegeben und rechtmäßig sein und zum Zeitpunkt der Erhebung festgelegt werden.“

107 Artikel-29-Datenschutzgruppe, „Opinion 03/2013 on purpose limitation“, WP 203 adopted on 2 April 2013, S. 17: “The same Latin root is used in several languages including English, Italian and French as ‚explicit‘, ‚explicite‘ and ‚esplicite‘. The original Latin verb from which these adjectives all originate is ‚explicare‘, with the meaning of ‚unfold, unravel, explain‘, and thus appears to imply a requirement that the purposes must be expressed and explained in some form. Other language versions focus on the requirement of the end-result, that the specification of the purposes must be unambiguous. See, for example, the German ‚eindeutig‘ and the Hungarian ‚ egyértelmű‘, which can be translated as ‚unambiguous‘, and do not necessarily require that the purposes must also be ‚expressed‘ in any way. However, the Dutch ‚uitdrukkelijk omschreven‘ is again similar to ‚explicit‘.

108 Vgl. Artikel-29-Datenschutzgruppe, „Opinion 03/2013 on purpose limitation“, WP 203 adopted on 2 April 2013, S. 10, 18.

109 Vgl. Artikel-29-Datenschutzgruppe, „Opinion 03/2013 on purpose limitation“, WP 203 adopted on 2 April 2013, S. 10. An dieser Stelle wird ebenso darauf verwiesen, dass sich Unterschiede auch für die Zweckänderung ergeben.

110 Vgl. Artikel-29-Datenschutzgruppe, „Opinion 03/2013 on purpose limitation“, WP 203 adopted on 2 April 2013, S. 18.

111 Vgl. Artikel-29-Datenschutzgruppe, „Opinion 03/2013 on purpose limitation“, WP 203 adopted on 2 April 2013, S. 18.

Für die Auslegung von Artikel 5 Datenschutz-Grundverordnung ist dies ebenso relevant:
Artikel 5 Absatz 1b der Fassungen im Vergleich:

⇢ “Personal data shall be:
collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes”

⇢ „Personenbezogene Daten müssen:
für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden“
Der Begriff „specified“ wird im Sinne von „determine“ verwendet und „explicit“ mit „eindeutig“ übersetzt.

Auch hier empfiehlt sich daher die Vorabprüfung, ob die übrigen Mitgliedstaaten das gleiche Verständnis haben und ob sich Auslegung und Anforderungen ändern, wenn die deutsche Fassung voraussetzen würde, dass personenbezogene Daten für näher aufgeführte, genau angegebene/ausdrücklich benannte und rechtmäßige Zwecke erhoben werden müssen.

Gleichwohl sollte insgesamt berücksichtigt werden, dass die Artikel-29-Datenschutzgruppe darauf hinweist, dass manchmal sogar der Kontext und die Verkehrssitte ausreichend sein können, wenn die Datenverarbeitung für alle Beteiligten ausreichend klar ist.[112] In einfachen Fällen sei die Bereitstellung detaillierter Informationen nicht unbedingt erforderlich.[113]

Unter Berücksichtigung dieser Auffassung könnte sich in Bezug auf Artikel 5 Absatz 1b Datenschutz-Grundverordnung daher eine Verhaltensregel dahingehend empfehlen, ob die schriftliche Bereitstellung des expliziten Zwecks an die betroffene Person erforderlich ist und in welchen Fallgestaltungen eine ausdrückliche und detaillierte Benennung des Zwecks nicht erforderlich sein könnte.

Diese Überlegungen müssten im Übrigen gleichermaßen im Hinblick auf Cookies und bei der Auslegung der Richtlinien 2002/58/EG und 2009/136/EG berücksichtigt werden. Sofern die Artikel-29-Datenschutzgruppe First-Party-Analysecookies für rechtmäßig erachtet, da sie ein geringes Datenschutzrisiko darstellen,[114] sollte der Anbieter seine Vorgehensweise genau beschreiben, damit die betroffene Person tatsächlich eine freie Entscheidung treffen kann. „Specified“ meint, dass der Verarbeitungsprozess begrenzt sein muss,[115] und dass unklare Formulierungen wie „IT-Sicherheitszwecke“ nicht ausreichen.[116] Entsprechendes muss für die Formulierung „Webanalyse-Cookies“ des Anbieters gelten. Auch hier bedarf es einer näheren Erläuterung des Zwecks und der Durchführung. Dies ist bei Anwendung und Auslegung des Erwägungsgrunds 25 der Richtlinie 2002/58/EG sowie Erwägungsgrunds 66 der Richtlinie 2009/136/EG zu bedenken, wenn es um Cookies als legitime Hilfsmittel geht.

Die gerade dargestellten Erwägungen wirken sich unmittelbar auf die unter den Punkten (3) und (4) aufgeführte Transparenz und „Kenntnis der Sachlage“ aus. Zunächst muss Einigung darüber bestehen, wie die Zweckbestimmung und damit zusammenhängend der Begriff „explicit“ zu verstehen ist.

112 Vgl. Artikel-29-Datenschutzgruppe, „Opinion 03/2013 on purpose limitation“, WP 203 adopted on 2 April 2013, S. 18.

113 Vgl. Artikel-29-Datenschutzgruppe, „Opinion 03/2013 on purpose limitation“, WP 203 adopted on 2 April 2013, S. 18.

114 Artikel-29-Datenschutzgruppe, WP 194, Stellungnahme 04/2012 zur Ausnahme von Cookies von der Einwilligungspflicht, angenommen am 07. Juni 2012, S. 12.

115 Artikel-29-Datenschutzgruppe, „Opinion 03/2013 on purpose limitation“; WP 203 adopted on 2 April 2013, S. 12.

116 Artikel-29-Datenschutzgruppe, „Opinion 03/2013 on purpose limitation“; WP 203 adopted on 2 April 2013, S. 15/16.

Ist nicht die erklärende Form umfasst, sondern das Ergebnis entscheidend, könnte letztendlich der Inhalt der Information abweichend sein. Um einen gemeinsamen Nenner zu finden, hat die Artikel-29-Datenschutzgruppe in Bezug auf die Richtlinie 95/46/EG vorgeschlagen, dass so viel wie nötig ausdrücklich erklärt werden muss, um ein einheitliches Verständnis über den Zweck zu erreichen.[117] Wenn der Fokus auf dem Ergebnis liegt, muss für den eindeutigen und unmissverständlichen Zweck, der nach außen hin auch zum Ausdruck gebracht wurde, der Empfängerhorizont entscheidend sein. Sofern der Zweck mangelhaft kommuniziert wurde, können nach Auffassung der Artikel-29-Datenschutzgruppe unterschiedliche Faktoren herangezogen werden, etwa das allgemeine Verständnis und die vernünftigen Erwartungen der betroffenen Person.[118]

(3) Kenntnis der Sachlage

Hinsichtlich der Kenntnis der Sachlage sind die Auslegung und Verknüpfung der Begriffsbestimmungen von „explicit und specified purposes“ sowie „einer Verarbeitungstätigkeit“ (siehe oben unter (1)) relevant, die gemäß der obigen Ausführungen der Artikel-29-Datenschutzgruppe in einem eingeschränkten Kontext verstanden werden sollte. Die Einwilligung müsse sich auf eine genau umrissene konkrete Situation beziehen. In diesem Sinne sollte daher Erwägungsgrund 32 Datenschutz-Grundverordnung zukünftig verstanden werden, der auf „eine andere Erklärung oder Verhaltensweise“ Bezug nimmt, „mit der die betroffene Person in dem jeweiligen Kontext eindeutig ihr Einverständnis mit der beabsichtigten Verarbeitung ihrer personenbezogenen Daten signalisiert.“

Die Datenverarbeitung wird umfangreicher und komplizierter, es gibt immer mehr Auswertungsmethoden. Bei vielen Diensten, z. B. Smart-Grid oder Smart-TV, können außerdem unterschiedliche Akteure einbezogen und Verarbeitungsvorgänge betroffen sein. Ist es hier der betroffenen Person überhaupt möglich, in dem jeweiligen Kontext eindeutig ein Einverständnis zu signalisieren? Der Durchschnittsverbraucher wird die komplexe Datenverarbeitung oftmals nicht mehr nachvollziehen können, so dass die Zwecke und Empfänger in seinem Sinne klar benannt werden müssten. In diesem Sinne wäre eine Auslegung nicht mehr notwendig. Anderenfalls müsste bei einer Auslegung des „Signals eines Einverständnisses der betroffenen Person in dem jeweiligen Kontext“ sehr genau geprüft werden, welche Maßnahmen etwa bei der Erstellung einer persönlichen Senderliste (Smart-TV) oder des Verbrauchs per Zeitintervall (Smart-Grid) ohne weitere gesonderte Einwilligung erfasst sein dürften. Der betroffenen Person müsste außerdem technisch von vorneherein ermöglicht werden, Verarbeitungstätigkeiten im Einzelfall auszuschließen, ohne auf den kompletten Dienst verzichten zu müssen.[119]

Bei der Kontextbestimmung muss jedoch eine weite Auslegung ausgeschlossen sein, so dass nicht - wie bei der Direktwerbung im Wettbewerbsrecht - die Möglichkeit besteht, einen „ähnlichen“ Zweck als rechtmäßig zu unterstellen. Wenn im Rahmen eines laufenden Vertragsverhältnisses die Möglichkeit besteht, nicht nur zur Vertragserfüllung erforderliche, sondern freiwillige, einwilligungsbedürftige Leistungen (unterschiedlich beteiligter Vertragspartner) in Anspruch zu nehmen, sollte aus Transparenzgründen die Datenverarbeitung klar dargestellt sein und eine Interpretation des Kontexts nicht möglich sein.[120] In analoger Anwendung des geschilderten „Telekom-Falls“ ist zudem sehr genau zu prüfen, ob die betroffene Person außerdem vernünftigerweise mit unterschiedlichen Empfängern (die bei Bereitstellung der Dienstleistung beteiligt sind) rechnen konnte.

117 Artikel-29-Datenschutzgruppe, „Opinion 03/2013 on purpose limitation“; WP 203 adopted on 2 April 2013, S. 18.

118 Artikel-29-Datenschutzgruppe, „Opinion 03/2013 on purpose limitation“; WP 203 adopted on 2 April 2013, S. 19, 39.

119 Zum Kopplungsverbot siehe S. 49 ff.

120 Siehe zur Werbung die Ausführungen auf S. 44 ff.

Entscheidend müssen stets gemäß der Empfehlungen der Artikel-29-Datenschutzgruppe die „vernünftigen Erwartungen“ sein, wobei zu bedenken ist, dass sich diese im Laufe der zukünftigen Entwicklung immer offener gestalten könnten. Für die Beibehaltung der Datenhoheit bei der betroffenen Person sollten die Zwecke und Empfänger daher ausdrücklich erklärt werden (müssen).

Der Nachweis der Einwilligung gemäß Artikel 7 Absatz 1 Datenschutz-Grundverordnung ist in diesem Falle im Übrigen nur dann hilfreich, wenn dafür europaweit einheitliche Kriterien festgelegt werden, auch um gleichartige Wettbewerbsbedingungen zu schaffen.

Es sollten daher insgesamt klare Verhaltensregeln oder Leitlinien aufgestellt werden, um eine faire und transparente europaweite Datenverarbeitung sicherzustellen, die ebenso zur Gewährleistung eines einheitlichen Wettbewerbs beitragen könnten.

Zudem sind einheitliche Kriterien wichtig, um eine klare Abgrenzung von einer Zweckänderung gemäß Artikel 6 Absatz 4 Datenschutz-Grundverordnung vorzunehmen. Die Voraussetzungen in Erwägungsgrund 50 und Artikel 6 Absatz 4 Datenschutz-Grundverordnung entsprechen den Ausführungen der Artikel-29-Datenschutzgruppe zur Zweckbestimmung, vor allem der Zusammenhang von ursprünglichen und dem späteren Verwendungszweck, die vernünftigen Erwartungen der betroffenen Personen, die Auswirkung der geänderten Verwendung auf die betroffenen Personen sowie die Schutzmaßnahmen, wie etwa Pseudonymisierung.[121] Aber es wird gleichermaßen im Sinne eines Kompatibilitätstests vertreten, dass diese Faktoren unterschiedlich gewichtet und eine erhöhte oder nachgewiesene Transparenz berücksichtigt werden könnte, wenn dem Betroffenen ein Widerspruchsrecht eingeräumt oder eine funktionale Trennung vorgenommen werde.[122]

Im Ergebnis könnten also geeignete Schutzmaßnahmen durchaus größere oder überraschende Zweckänderungen legitimieren.[123] Verbindet man diesen Gedanken mit der Möglichkeit, dass nun ebenso die datenverarbeitende Stelle durch eine organisatorische Trennung die Pseudonymisierung durchführen kann,[124] bedarf es hier im Besonderen klarer Verhaltensregeln für die Datenverarbeitung. Zu beachten ist stets: Gemäß Artikel 13 Absatz 3 sowie Erwägungsgrund 61 Datenschutz-Grundverordnung muss der Verantwortliche Informationen über den geänderten Zweck vor Weiterverarbeitung zur Verfügung stellen. Dies ist jedoch von der grundsätzlichen Bewertung der Zulässigkeit der Zweckänderung unabhängig, die ohne erneute Einwilligung durchgeführt werden könnte (bei Vorliegen der entsprechenden Voraussetzungen).

Insgesamt muss zukünftig eine weite Auslegung von Zweck und Empfängern vermieden werden. Die Gefahr besteht anhand der oben dargestellten Formulierungen „Signal des Einverständnisses in dem jeweiligen Kontext“ in Verbindung mit der unterschiedlichen europaweiten Auslegung des Begriffs „explicit“ und der darüber hinaus bestehenden Möglichkeit einer Zweckänderung, der bereits zum jetzigen Zeitpunkt teilweise ein weites Verständnis zugrunde liegt.

121 Vgl. Artikel-29-Datenschutzgruppe, „Opinion 03/2013 on purpose limitation“; WP 203 adopted on 2 April 2013, siehe insbesondere zur Kompatibilität, Vorhersehbarkeit und Nutzerkontrolle S.12-S.14.

122 Helbig, K&R 2015, S. 145, 147.

123 Helbig, K&R 2015, S. 145, 147.

124 Erwägungsgrund 29 Datenschutz-Grundverordnung regelt, dass „um Anreize für die Anwendung der Pseudonymisierung bei der Verarbeitung personenbezogener Daten zu schaffen, sollten Pseudonymisierungsmaßnahmen, die jedoch eine allgemeine Analyse zulassen, bei demselben Verantwortlichen möglich sein, wenn dieser die erforderlichen technischen und organisatorischen Maßnahmen getroffen hat, um — für die jeweilige Verarbeitung — die Umsetzung dieser Verordnung zu gewährleisten, wobei sicherzustellen ist, dass zusätzliche Informationen, mit denen die personenbezogenen Daten einer speziellen betroffenen Person zugeordnet werden können, gesondert aufbewahrt werden.“

Nur wenn ein einheitliches Verständnis herrscht, kann auch die Information oder Unterrichtung über den zugrundeliegenden Zweck sinnvoll und einheitlich umgesetzt werden (siehe den folgenden Punkt „Informiertheit“).

(4) Informiertheit und Transparenz

Gemäß der Ausführungen der Artikel-29-Datenschutzgruppe bezieht sich eine zweite Dimension der Einwilligung auf die Information als Transparenz gegenüber der betroffenen Person. Dies wurde gerade unter Punkt (3) „Kenntnis der Sachlage“ dargestellt, deckt aber regelmäßig auch alle Informationen ab, die in Artikel 13 Datenschutz-Grundverordnung enthalten sind.[125]

Die Einwilligung muss damit auf informierter Basis erfolgen, was die Artikel-29-Datenschutzgruppe bereits für die Anforderungen nach der Richtlinie 95/46/EG festgestellt hat (Artikel 10 und 11 der Richtlinie 95/46/EG). Obwohl die Informationspflicht eine eigenständige Pflicht darstellt, sei sie mit der Einwilligung verbunden: Vor ihrer Bereitstellung könne keine Einwilligung erteilt werden,[126] wobei in vielen Fällen die Einwilligung zum Zeitpunkt der Erhebung der personenbezogenen Daten erhalten wird, wenn die Verarbeitung beginnt, so dass in diesem Fall die bereitzustellende Information mit den in Artikel 10 der Richtlinie aufgeführten Punkten übereinstimme.[127]

Diese Ausführungen müssen ebenso hinsichtlich der Datenschutz-Grundverordnung gelten.
Insgesamt enthält die Datenschutz-Grundverordnung Regelungen zur Informiertheit und Transparenz in Artikel 12, 13 und 14: Der Nutzer muss stets präzise, leicht zugänglich und verständlich sowie in klarer und einfacher Sprache, insbesondere über Verarbeitungszwecke, Rechtsgrundlage der Verarbeitung, Empfänger der personenbezogenen Daten, informiert sein und ein entsprechendes Auskunftsrecht gemäß Artikel 15 ausüben können.

125 *Siehe auch Artikel-29-Datenschutzgruppe, WP 187, Stellungnahme 15/2011 zur Definition von Einwilligung, angenommen am 13. Juli 2011, S. 11 mit dem folgenden Hinweis: „Um gültig zu sein, muss die Einwilligung in Kenntnis der Sachlage erfolgen. Das bedeutet, dass alle erforderlichen Informationen dann zu erteilen sind, wenn die Einwilligung gefordert wird und dass sie alle wesentlichen Aspekte der Verarbeitung ansprechen, die durch die Einwilligung legitimiert werden sollen. Das würde normalerweise alle Informationen abdecken, die in Artikel 10 der Richtlinie aufgeführt sind. Es hängt aber auch davon ab, wann und unter welchen Umständen die Einwilligung gefordert wird. Unabhängig davon, ob die Einwilligung gegeben wird oder nicht, ist die Transparenz der Datenverarbeitung eine Bedingung der Fairness, die auch nach Bereitstellung der anfänglichen Informationen ihren Wert hat“.*

126 *Artikel-29-Datenschutzgruppe, WP 187, Stellungnahme 15/2011 zur Definition von Einwilligung, angenommen am 13. Juli 2011, S. 22/23.*

127 *Artikel-29-Datenschutzgruppe, WP 187, Stellungnahme 15/2011 zur Definition von Einwilligung, angenommen am 13. Juli 2011, S. 23.*

Diese Informations- und Auskunftsrechte umfassen ebenso

- die Dauer der Verarbeitung,
- die Darlegung der berechtigten Interessen gemäß Artikel 6 Absatz 1f (sofern etwa eine Verarbeitung der personenbezogenen Daten nicht auf der Einwilligung beruht oder zur Vertragserfüllung erforderlich ist),
- Widerspruchsrechte gemäß Artikel 21,
- Beschwerderecht bei der Aufsichtsbehörde,
- Informationen über die öffentlichen zugänglichen Quellen, sofern Daten daraus erhoben wurden
- sowie das Bestehen einer automatisierten Entscheidungsfindung (Artikel 22).

Die Artikel-29-Datenschutzgruppe unterscheidet zwischen Qualität einerseits sowie Zugänglichkeit und Sichtbarkeit der Information andererseits. Qualität (bezogen auf „in Kenntnis der Sachlage“) meint, dass ein regelmäßiger/durchschnittlicher Nutzer in der Lage sein sollte, sie zu verstehen.[128] In der Datenschutz-Grundverordnung wird in Erwägungsgrund 42 zusätzlich die Einhaltung von verbraucherschutzrechtlichen Vorgaben verlangt. Garantien sollten sicherstellen, dass die betroffene Person weiß, dass und in welchem Umfang sie ihre Einwilligung erteilt hat. Eine vom Verantwortlichen vorformulierte Einwilligungserklärung sollte keine missbräuchlichen Klauseln enthalten und in verständlicher und leicht zugänglicher Form sowie in einer klaren und einfachen Sprache zur Verfügung gestellt werden (unter Verweis auf die Richtlinie 93/13/EWG des Rates).

Entsprechendes hat die Artikel-29-Datenschutzgruppe bereits in ihrer Stellungnahme WP 187 empfohlen („Informationen sollten deutlich sichtbar (Art und Größe der Schrift), auffällig und verständlich sein“).[129]

Der Grundsatz der Transparenz setzt gemäß der deutschen Fassung des Erwägungsgrunds 39 Datenschutz-Grundverordnung zwar außerdem voraus, dass alle Informationen und Mitteilungen zur Verarbeitung dieser personenbezogenen Daten leicht zugänglich und verständlich und in klarer und einfacher Sprache verfasst sein müssen. Fraglich ist jedoch (wie oben ausführlich dargestellt) hinsichtlich des Zwecks, „wie“ zu informieren ist bzw. ob entsprechend der Problematik bei Anwendung der Richtlinie 95/46/EG ebenso bei der Datenschutz-Grundverordnung unterschiedliche Sprachverständnisse über „explicit“ und „specified“ bestehen, sich dadurch für die Rechte der betroffenen Personen in den einzelnen Mitgliedstaaten Unterschiede ergeben und einer Vollharmonisierung des Datenschutzrechts entgegenstehen könnten (siehe hierzu die obigen Ausführungen und zur Erinnerung den Wortlaut des Erwägungsgrunds 39 „In particular, the specific purposes for which personal data are processed should be explicit…“).

128 *Artikel-29-Datenschutzgruppe, WP 187, Stellungnahme 15/2011 zur Definition von Einwilligung, angenommen am 13. Juli 2011, S. 23.*

129 *Artikel-29-Datenschutzgruppe, WP 187, Stellungnahme 15/2011 zur Definition von Einwilligung, angenommen am 13. Juli 2011, S. 23. S. 24: Je schwieriger es für den Durchschnittsbürger wird, alle Elemente der Datenverarbeitung zu überblicken und zu verstehen, desto größer sollten die Anstrengungen des für die Datenverarbeitung Verantwortlichen sein, zu zeigen, dass die Einwilligung basierend auf verständlichen Informationen für den konkreten Fall erteilt wurde.*

Die englische Originalfassung regelt zudem in Artikel 13 Datenschutz-Grundverordnung folgendes:
„Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:
...

(c)
the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;"

Die deutsche Fassung übersetzt "provide with information" mit "mitteilen". Der Zweck muss demnach aufgrund der Regelung des Artikel 13 Datenschutz-Grundverordnung gegenüber der betroffenen Person erklärt werden. Gemäß dem oben Gesagten ist jedoch zum einen offen, „wie" der Zweck (vorher) festgelegt und formuliert sein muss. Zum anderen wäre europaweit zu vergleichen, ob sich gegebenenfalls durch abweichende Übersetzungen von „provide with" Unterschiede ergeben könnten und die Verantwortlichen in den übrigen Mitgliedstaaten die Informationen immer „mitteilen" im Sinne von „erklären" müssen.

Bei einer elektronischen Einwilligung sind zudem die oben dargestellten Ausführungen zu beachten (s. S. 9 ff. und S. 19 ff.). Hier muss zukünftig klargestellt werden, ob die Informationen „jederzeit abrufbar" oder nur „leicht zugänglich" sein müssen oder ob beide Begrifflichkeiten synonym zu verwenden sind.

! Fazit Nr. 6

Zwecke müssen gemäß Artikel 5 Absatz 1b Datenschutz-Grundverordnung festgelegt, eindeutig und legitim sein, aber fraglich ist, ob damit auch europaweit das Verständnis verbunden wird, die Zwecke klar auszudrücken und zu erklären und inwieweit die Zweckbestimmung in einem weiten Verständnis definiert wird (siehe Artikel-29-Datenschutzgruppe WP 203).

Es kann sich daher ein aktueller Vergleich der Übersetzungen noch vor Inkrafttreten der Datenschutz-Grundverordnung im Hinblick darauf empfehlen, inwieweit ein einheitliches, europaweites Verständnis über die Auslegung von „explicit", „specified" und „provide with" besteht. Dabei sollte berücksichtigt werden, ob unterschiedliche Auslegungen Auswirkung auf die Betroffenenrechte im Sinne eines einheitlichen Schutzniveaus haben könnten.

Die bisherigen Ausführungen der Artikel-29-Datenschutzgruppe zur Zweckbestimmung könnten für die Ausgestaltung einer Verhaltensregel herangezogen oder vom zukünftigen Europäischen Datenschutzausschuss bekräftigt werden. Im Sinne des Betroffenenschutzes und im Rahmen der Zweckbestimmung sollten Zwecke klar ausgedrückt und erklärt werden (trotz oder gerade aufgrund komplexer Datenverarbeitungsprozesse). Dies ist insbesondere im Hinblick auf Big Data-Anwendungen und zentrale Datenspeicherungslösungen, bei welchen mehrere Beteiligte eingebunden sind, von Bedeutung.

! Es muss genau geprüft werden, was von einer Verarbeitungstätigkeit sinnvollerweise und vernünftigerweise umfasst sein kann. Hierfür sind das allgemeine Verständnis und die Betroffenensicht entscheidend, die sich jedoch im Laufe der Zeit verändern können. Die rasante technische Entwicklung spielt hierbei eine Rolle. Es muss dementsprechend die Sichtweise und das technische Verständnis eines „Durchschnittsbetroffenen" zum „jeweiligen Zeitpunkt" ermittelt werden.[130]
Die Datenschutzaufsichtsbehörden in Deutschland sollten bereits zum jetzigen Zeitpunkt klare Anforderungen an geeignete Schutzmaßnahmen für eine Zweckänderung formulieren, insbesondere vor dem Hintergrund von Big Data-Anwendungen. Es kann sich ein Negativkatalog empfehlen, etwa inwieweit Transparenz und Pseudonymisierung tatsächlich eine Zweckänderung ermöglichen oder erleichtern kann. Zukünftig bedarf es hierfür im europäischen Kontext klarer Leitlinien für die Datenverarbeitung.

2. Relevanz für den Einwilligungsassistenten

(1) Granularität

Der Verantwortliche muss sicherstellen, dass die betroffene Person die gerade unter 1. (4) aufgelisteten Informationen vor Erteilung der Einwilligung erhält, da die Einwilligung auf informierter Basis erfolgen muss. Dabei ist ebenso zu berücksichtigen, ob der zukünftige Einsatz eines Einwilligungsassistenten einen selbstständigen Dienst der Informationsgesellschaft darstellt, so dass dieser ebenfalls einer Verpflichtung zur Bereitstellung von Informationen unterliegt.[131]

In Bezug auf die Einwilligungsvoraussetzungen hat die Artikel-29-Datenschutzgruppe in ihrer Stellungnahme „Online-Informationsmittel" erwähnt, die besonders in Bezug auf soziale Netzwerkdienste hilfreich sein sollen, um eine ausreichende Granularität und Klarheit der Privatsphären-Einstellungen zu bieten. Auch mehrschichtige Hinweise könnten als ein hilfreiches Mittel dazu beitragen, die richtigen Informationen auf eine einfach zugängliche Weise bereitzustellen.[132] Diese Überlegungen sollten ebenso für die Konzeption des Einwilligungsassistenten herangezogen werden, damit dieser für die betroffene Person ausreichend klare Elemente hinsichtlich Einwilligung und Information anbietet.

Für den Einwilligungsassistenten ist jedoch fraglich, ob er den notwendigen Detaillierungsgrad und die Unterscheidung von Zwecken sowie vernünftigen Erwartungen und Empfängern automatisiert durchführen kann oder vielmehr eine rechtliche Bewertung des Einzelfalls erforderlich bleibt.[133] Der in der Einführung geschilderte automatisierte Abgleich der Datenschutzbestimmungen mit anschließender Übersetzung in ein Formular, welches die Daten, Zwecke und Empfänger für die betroffene Person in einem übersichtlichen Dokument darstellt, müsste ausreichend detailliert sein.

130 *Hier kann geprüft werden, ob es hilfreich ist, die Auffassung des Bundesgerichtshofs zur WLan-Haftung heranzuziehen, und -im Sinne des Betroffenenschutzes- bei einem laufenden Dienstleistungsverhältnis den Zeitpunkt der Kenntnis auf den Zeitpunkt des ursprünglichen Abschlusses festzulegen. Bundesgerichtshof, Urteil vom 24.11.2016 - I ZR 220/15: Der Inhaber eines Internetanschlusses mit WLAN-Funktion ist „nur" zur Prüfung verpflichtet, ob der eingesetzte Router über die im Zeitpunkt seines Kaufs für den privaten Bereich marktüblichen Sicherungen, also einen aktuellen Verschlüsselungsstandard sowie ein individuelles, ausreichend langes und sicheres Passwort, verfügt. Eventuell könnte in Anlehnung an diese Rechtsprechung das technische Verständnis der betroffenen Person zum Zeitpunkt des Vertragsabschlusses bei einem laufenden Vertragsverhältnis zugrunde gelegt werden.*

131 *Siehe hierzu S. 21 und S. 55.*

132 *Artikel-29-Datenschutzgruppe, WP 187, Stellungnahme 15/2011 zur Definition von Einwilligung, angenommen am 13. Juli 2011, S. 24.*

133 *Siehe hierzu bereits S. 26 und S. 28.*

Zur Bewertung können in diesem Zusammenhang etwa die verbundenen Rechtssachen „C-92/09 und C-93/09“ des Europäischen Gerichtshofs herangezogen werden.[134] Hier wurde verlangt, dass der Betroffene die Möglichkeit hat, nicht nur pauschal in die Veröffentlichung von Daten einzuwilligen, sondern im Einzelfall bezüglich der einzelnen Daten unterschieden werden müsse, die veröffentlicht werden sollen. Dies muss bei der Konzeption des Einwilligungsassistenten sichergestellt sein.

Unter Berücksichtigung der obigen Ausführungen hinsichtlich der Einwilligungsvoraussetzungen „bestimmter Fall und Zweck“ stellt sich dennoch die Frage, wie granular die Voreinstellungen vorgenommen werden müssen oder ob sich nicht durch Verwendung von bestimmten Präferenzen gleichzeitig ergeben könnte, dass der Nutzer ebenso mit Verarbeitung von anderen Daten im gleichen Kontext einverstanden ist. In Bezug auf die Darstellung der Einwilligungs“elemente“ könnte fraglich sein, ob es nicht zulässig wäre, die Zwecke weniger detailliert aufzulisten, stets unter der Maßgabe, dass der Verantwortliche sie als „eine“ Verarbeitungstätigkeit versteht. Aber gerade der Einwilligungsassistent kann aufgrund seiner Möglichkeit der Bereitstellung granularer Komponenten zur Transparenz beitragen, so dass seine technische (Fort-)Entwicklung dahingehend erfolgen sollte, die notwendige Granularität und Transparenz sicherzustellen und nicht diese umzukehren.

Beachtet werden muss gleichwohl, dass die Komplexität der Datenverarbeitung zunimmt und der Kontext der Einwilligung auch aus Betroffenensicht nicht überspannt werden darf, so dass tatsächlich im Einzelfall geprüft werden muss, was unter „einer“ Verarbeitungstätigkeit sinnvollerweise verstanden werden muss. Insbesondere bei intelligenten Stromzählern gibt es unter Umständen eine Menge Akteure, bei denen das Erfordernis einer Einwilligung für die einzelne Datenverarbeitung und unterschiedliche Empfänger genau zu prüfen wäre. Darüber hinaus gilt stets, dass anstatt einer Einwilligung eine transparente Information ausreichen könnte, wenn die Datenverarbeitung bereits durch die Ausgestaltung des Vertragsverhältnisses erforderlich ist,[135] so dass abermals die automatische Prüfung der Datenschutzhinweise unter Erstellung einer Einwilligungserklärung einer kritischen Prüfung zu unterziehen ist.

Dies entspricht insgesamt der Auffassung der Artikel-29-Datenschutzgruppe, die zum einen die Notwendigkeit der Granularität bei der Einholung der Einwilligung von Fall zu Fall in Abhängigkeit vom Zweck/den Zwecken oder dem Datenempfänger bewertet wissen möchte, und zum anderen die Unterscheidung zwischen Erforderlichkeit der Datenverarbeitung und freiwilliger Einwilligung betont.[136]

Weiterhin ist bei der Konzeption des Einwilligungsassistenten entscheidend, ob die Daten zentral oder dezentral gespeichert werden:

134 *Siehe den Verweis in Artikel-29-Datenschutzgruppe, WP 187, Stellungnahme 15/2011 zur Definition von Einwilligung, angenommen am 13. Juli 2011, S. 26 auf die Schlussanträge der Generalanwältin Sharpston vom 17. Juni 2010, Volker und Markus Schecke GbR, verbundene Rechtssachen C-92/09 und C-93/09.*

135 *Siehe hierzu etwa auch das Beispiel zu den unterschiedlichen beteiligten Akteuren bei Verbrauchsdatenabrechnung per Zeitintervall im Kontext von „Abrechnung bezogener sowie eingespeister Energie im Bilanzierungssystem“. Hier muss die Erforderlichkeit einer Einwilligung genau geprüft werden und von den erforderlichen Zwecken einer Vertragsdurchführung abgegrenzt werden in der Orientierungshilfe datenschutzgerechtes Smart Metering der Konferenz der Datenschutzbeauftragten des Bundes und der Länder von Juni 2012 „Maßnahmen an Hand von Use Cases“, Fallbeispiel S. 28 http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/Orientierungshilfe_SmartMeter.pdf?__blob=publicationFile*

136 *Artikel-29-Datenschutzgruppe, WP 187, Stellungnahme 15/2011 zur Definition von Einwilligung, angenommen am 13. Juli 2011, S. 21 sowie S. 9, letzteres zur Anwendbarkeit mehrerer Rechtsgrundlagen: Entweder ist die Verarbeitung notwendig für die Erfüllung eines Vertrags oder die Einwilligung (ohne Zwang) muss eingeholt werden.*

- Werden die Daten zentral auf einer Plattform gespeichert -diese Möglichkeit besteht bei CoMaFeDS- muss zwischen dem Verantwortlichen der Plattform und dem jeweiligen (potenziellen) Empfänger der Daten unterschieden werden: Es müsste zum einen sichergestellt sein, dass der Nutzer transparent über die geplante Datenverarbeitung des Empfängers aufgeklärt wird. Zum anderen müsste berücksichtigt werden, wer als Verantwortlicher des „Wissensgraphen" der Plattform einzustufen ist.[137] Wie eingangs dargestellt, sind über die zukünftige geplante Funktionsweise bislang noch keine näheren technischen Details offengelegt. Daher muss sich diese Ausführung auf den allgemeinen Hinweis beschränken, dass hier sowohl die technische Sicherheit zu beachten ist, als auch die Frage beantwortet werden muss, ob der Plattformbetreiber gesondert vom jeweiligen Nutzer eine Einwilligung für die „Datenvermittlung" einholen müsste und wie die „Kenntnis der Sachlage im Einzelfall" sichergestellt ist. Auch hier sollte grundsätzlich die Aktivität stets vom Nutzer ausgehen und es dürfte, gerade unter Berücksichtigung der Zeitdauer, keine pauschale Einwilligung -ohne entsprechende Rückfrage im Einzelfall an den Nutzer- eingeholt werden.

- Im Hinblick auf die dezentrale Speicherung beim Nutzer wird zurzeit nach technischen Lösungen gesucht, die es potenziellen Empfängern erlauben, die erteilte Einwilligung trotz lokaler Speicherung finden zu können. Daher wäre der selbstständige Einsatz beim Nutzer (ohne zentrale Plattform) zukünftig denkbar. Eine solche dezentrale Speicherung ist das Konzept von LETsmart, aber ebenso bei CoMaFeDS in Prüfung und Entwicklung.

Auch wenn Systeme wie LETsmart nach derzeitiger Planung in der Lage sein sollen, nach Wegfall des Verwendungszwecks die Daten automatisiert im dezentral betriebenen System des Nutzers zu löschen, ist nicht ausgeschlossen, dass der Empfänger die Daten, auf die ihm Zugriff gewährt wurde, kopiert und eigenständig verarbeitet. Der jeweilige Empfänger muss also im Sinne der datenschutzrechtlichen Regelungen entweder die Kopie bzw. Speicherung der Daten in seinem System von vorneherein ausschließen oder im Falle einer eigenständigen Speicherung die Löschung der Daten in seinem System sicherstellen. Im Gesamten ist somit wiederum von besonderer Bedeutung, wer Verantwortlicher des Einwilligungsassistenten ist, der sich derzeit weiterhin in der Entwicklung befindet. Entscheidend ist, unter anderem für die Informations- und Löschungspflichten, ob sich der Einwilligungsassistent (ebenso) im „Herrschaftsbereich" des Nutzers befindet oder von einem Anbieter eingesetzt wird.[138]

In diesem Zusammenhang ist auf die übrigen Systeme Bezug zu nehmen, die in der Bestandsaufnahme der Studie dargestellt wurden: Sofern unterschiedliche Daten in einem System zusammengefügt werden (siehe etwa den Dienst DigiMe[139]) und mit einem Einwilligungsassistenten verknüpft würden, ist besonders zu bedenken, inwieweit eine nachträgliche Zweckänderung oder die Formulierung eines Zwecks „in einem Kontext" in Bezug auf andere Empfänger in Betracht kommen kann. Wenn der Nutzer selbst seine persönlichen Daten speichert, Zugriffsberechtigungen vergibt, so dass mehrere Unternehmen darauf Zugriff haben, lässt sich gegebenenfalls einfacher begründen, aus welchem Grunde nun die Formulierung eines Zwecks „in einem Kontext" ausreichen soll, um die Weitergabe an unterschiedliche Empfänger zu begründen oder dies nachträglich zu legitimieren (siehe auch den oben genannten Telekom-Fall).

137 Siehe hierzu auch den Punkt „Verantwortung" auf S. 52 ff.
138 Siehe hierzu auch den Punkt „Verantwortung" auf S. 52 ff.
139 Siehe Kapitel II.2. der Studie der Stiftung Datenschutz.

Dem Nutzer wären die Empfänger in diesem Fall ja sogar bekannt. Hierbei wird zukünftig ganz entscheidend sein, wer im Rahmen der technischen Möglichkeiten als (Mit)Verantwortlicher betrachtet wird und inwieweit sanktionsbehaftete Nachweispflichten gemäß Artikel 7 Absatz 1 Datenschutz-Grundverordnung durchgesetzt werden können.[140]

(2) Exkurs: UWG

In Bezug auf die Einwilligung bei Standortdaten ist bei Verwendung eines Einwilligungsassistenten auf folgendes zu achten: Es ergibt sich zu dem oben dargestellten Telefonanruf im Zusammenhang mit einem Wettervorhersagedienst[141] insofern ein Unterschied, dass die betroffene Person durch Anwählen einer Telefonnummer selbst aktiv tätig wird. Es ist ungewiss, ob tatsächlich an jedem Ort oder bei jeder Hotelankunft eine Restaurantempfehlung oder Wetteransage gewünscht ist. Im Hinblick auf den Einwilligungsassistenten ist daher fraglich, ob im Vorhinein eine informierte Einwilligung für eine automatische Standortbestimmung erfolgen kann: Wird der Nutzer beispielsweise automatisiert bei Ankunft in einem Hotel gefragt, ob er eine Restaurantempfehlung wünscht, wird sein Standort bereits verwendet. Hier spielt außerdem der Zeitablauf einer solchen Einwilligung eine wesentliche Rolle.[142] Dem Nutzer muss bewusst sein, in welchem Falle und zu welchem konkreten Zweck eine automatische Standortbestimmung erfolgt. Weiterhin ist fraglich, ob damit auch „ähnliche“ Zwecke wie die nächstgelegenen Kneipen, Bars oder Tankstellen mit Imbissangebot (Ursprungsdienstleistung: Restaurantempfehlungen) oder Informationen über Schäden, Stromausfälle und Verkehrsbehinderungen (Ursprungsdienstleistung: Wettervorhersage) für einen bestimmten Wintersportort) umfasst sind. In der deutschen Literatur wird beispielsweise vertreten, dass demjenigen , der per E-Mail französischen Rotwein bestellt hat, künftig Werbung für chilenischen Rotwein übersandt werden darf, und wer einen Hotelaufenthalt in Kärnten per E-Mail gebucht hat, dem dürfe eine Werbung für einen Hotelaufenthalt in Sizilien geschickt werden.13[143] Gilt dies ebenso für (entgeltliche) Dienstleistungen wie die gerade genannten und wieweit reicht der datenschutzrechtliche Kontext? Eine solche mutmaßliche Einwilligung wird im Datenschutzrecht abgelehnt,[144] aber bei Direktwerbung innerhalb bestehender Vertragsbeziehungen für eigene ähnliche Produkte gemäß Artikel 13 Absatz 2 und Erwägungsgrund 41 der Richtlinie 2002/58/EG dennoch legitimiert. Dies bezieht sich insgesamt auf die Frage einer zulässigen Zweckänderung nach Artikel 6 Absatz 4 Datenschutz-Grundverordnung oder im Rahmen „derselben“ Einwilligung auf deren „Kontext“ (siehe oben unter (2) und (3)) unter Berücksichtigung des Wettbewerbsrechts. So wird in der deutschen Literatur kritisiert, dass bislang versäumt wurde, eine Homogenisierung der wettbewerbs- und datenschutzrechtlichen Einwilligungen herbeizuführen,[145] und nun muss darüber hinaus eine europaweite Harmonisierung erfolgen.

Gemäß der Rechtslage in Deutschland ist bei Direktwerbung folgendes zu bedenken: Das Bundesdatenschutzgesetz und das Gesetz gegen den unlauteren Wettbewerb (UWG) stehen gleichberechtigt nebeneinander. § 7 Absatz 3 UWG (der Artikel 13 Absatz 2 der Richtlinie 2002/58/EG umsetzt) bietet bei elektronischer Werbung insoweit eine Erleichterung, dass ein Unternehmer, der im Zusammenhang mit dem Verkauf einer Ware oder Dienstleistung von dem Kunden dessen elektronische Postadresse

140 Siehe S. 47 ff.

141 Siehe hierzu S. 31 ff.

142 Siehe hierzu S. 50 ff. und aus wettbewerbsrechtlicher Sicht Köhler in: Köhler/Bornkamm, UWG, 34. Auflage 2016, § 7 UWG Rn. 204b zur zeitlichen Begrenzung.

143 Köhler in: Köhler/Bornkamm, UWG 34. Auflage 2016, § 7 UWG Rn. 205. Siehe hierzu auch die Ausführungen weiter unten in diesem Abschnitt.

144 Rogosch, Die Einwilligung im Datenschutzrecht, S. 68.

145 Rogosch, Die Einwilligung im Datenschutzrecht, S. 125.

erhalten hat, diese zur Direktwerbung für eigene ähnliche Waren oder Dienstleistungen verwenden darf, wenn der Kunde nicht widersprochen hat. Diese Ausnahmeregelung wird von der deutschen Rechtsprechung eng und im Hinblick auf eine bestehende Geschäftsbeziehung ausgelegt.[146] Es wird vertreten, dass sich die Ähnlichkeit auf die bereits gekauften Waren beziehen und dem gleichen typischen Verwendungszweck oder Bedarf des Kunden entsprechen muss.[147] Gegebenenfalls sei es zulässig, Zubehör oder Ergänzungswaren zu bewerben.[148] Die Voraussetzung sei außerdem regelmäßig erfüllt, wenn die Produkte austauschbar sind oder dem gleichen oder zumindest einen ähnlichen Bedarf oder Verwendungszweck dienen.[149]

Umfasst das Geschäftsmodell eines Anbieters etwa das „Angebot von Restaurantempfehlungen aufgrund der Standortbestimmung" an Nutzer, die sich mittels ihrer elektronischen Postadresse[150] registriert haben, könnte unterstellt werden, dass die eigene Zusammenstellung der Empfehlungen auch ein eigenes Produkt des Anbieters darstellt (unter der Voraussetzung, dass der Anbieter die Nutzerdaten nicht an die Restaurantbesitzer weitergibt). Damit könnte er ebenfalls ähnliche Produkte empfehlen. Der Anbieter dieses Geschäftsmodells muss für diesen Dienst selbst Datenschutzhinweise transparent zur Verfügung stellen und hätte die Möglichkeit, gemäß § 7 Absatz 3 UWG ähnliche Dienstleistungen zu empfehlen. Zu beachten ist jedoch, dass der „Verkauf einer Dienstleistung" der Auslegung bedarf.[151] Im Sinne einer Harmonisierung sollte vor allem nicht die Rechtsauffassung zur „Entgeltlichkeit" im europäischen Kontext außer Acht gelassen werden sowie die Frage, wie „eigene Produkte" und „ähnliche Produkte" in anderen Mitgliedstaaten bewertet werden. Datenschutzrechtlich kann sich außerdem stets ein Widerspruch zur Eindeutigkeit der Zweckbestimmung und der klaren Benennung des Zwecks ergeben, sofern „Restaurantempfehlung" auf „ähnliche" Produkte ausgedehnt wird. Die Erforderlichkeit der ausdrücklichen Benennung des Zwecks wird in den Mitgliedstaaten unter Anwendung der Richtlinie 95/46/EG unterschiedlich gehandhabt.[152]

In dieser Stellungnahme kann allerdings keine europaweite Prüfung erfolgen, so dass sich eine zusätzliche Studie dahingehend empfehlen kann, ob sich im Hinblick auf die übrigen Mitgliedstaaten Unterschiede in der Rechtsauffassung ergeben könnten oder eine Harmonisierung des Wettbewerbsrechts bereits vorliegt. Die im Folgenden dargestellten Ausführungen beschränken sich daher weiterhin auf das UWG.

146 *KG, Beschluss vom 18.3.2011, 5 W 59/11.*

147 *OLG Jena, Urteil vom 21. 4. 2010, 2 U 88/10, MMR 2011, 101.*

148 *Köhler in: Köhler/Bornkamm, UWG 34. Auflage 2016, § 7 UWG Rn. 205.*

149 *KG, Beschluss vom 18.3.2011, 5 W 59/11; Köhler in: Köhler/Bornkamm, UWG 34. Auflage 2016, § 7 UWG Rn. 205. Fezer, UWG Lauterkeitsrecht, §§ 5-22, Kommentar, Band 2, München 2005, nimmt auf die Abgrenzungsprobleme und auf das Markenrecht und Kartellrecht als mögliche Auslegungshilfen Bezug (Rn. 136): Aus Sicht des Verbrauchers reichten Äquivalenz und Austauschbarkeit. Wenn also Preissteigerungen bei einem der Produkte zu einer Ausweichbewegung hin zu einem anderen Produkt führe und die Nachfrage bei dem zweiten Produkt steige.*

150 *Siehe Artikel 2h) Richtlinie 2002/58/EG, die ganz allgemein regelt: „elektronische Post" jede über ein öffentliches Kommunikationsnetz verschickte Text-, Sprach-, Ton- oder Bildnachricht, die im Netz oder im Endgerät des Empfängers gespeichert werden kann, bis sie von diesem abgerufen wird.*

151 *Ohly in: Ohly/Sosnitza, Gesetz gegen den unlauteren Wettbewerb, 6. Auflage 2014, § 7 UWG Rn. 73, verweist darauf, dass ein Vertrag tatsächlich zustande gekommen sein muss (Kaufvertrag, Werkvertrag, Reisevertrag, Vertrag über Finanzdienstleistungen) und dass eine konkrete Vertragsanbahnung noch nicht ausreichend ist. Schöler in: Harte-Bavendamm/Henning-Bodewig, UWG, 3. Auflage 2013, § 7 UWG Rn. 351 bezieht sich auf den tatsächlichen „Verkauf" einer Ware oder Dienstleistung, und das bloße Verkaufsgespräche nicht genügen sollen. Fezer, UWG Lauterkeitsrecht. §§ 5-22, Kommentar, Band 2, München 2005 verweist darauf, dass ein vorangegangenes Umsatzgeschäft vorliegen muss (Rn. 122). Unter Rn. 131 nimmt er außerdem auf die unklare Formulierung Bezug, da es den Verkauf von Dienstleistungen nicht gebe und dies in anderen Sprachfassungen leider nicht so deutlich sei. Es sei „mit dem Erbringen einer Dienstleistung" zu lesen.*

152 *Siehe oben S. 34 ff.*

Grundsätzlich wäre gemäß § 7 Absatz 3 UWG denkbar, dass der Vertragspartner ohne Einwilligung Werbung, also Informationen, die nicht für vertragliche Zwecke erforderlich sind, an seinen Kunden versenden dürfte (bei LETsmart ist etwa zunächst ein laufendes Vertragsverhältnis bei Verwendung eines Einwilligungsassistenten angedacht). Im Bundesdatenschutzgesetz gilt bislang für solche Zwecke grundsätzlich ein Einwilligungserfordernis, da das Listendatenprivileg des § 28 Absatz 3 BDSG nicht greift. Erwägungsgrund 47 Datenschutz-Grundverordnung regelt ohne nähere Erläuterung, dass die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden kann. Daher empfehlen sich auch hier entsprechende europaweit einheitliche Verhaltensregeln zur Auslegung dieses Erwägungsgrunds - soweit diese aufgrund einer Verarbeitungstätigkeit in mehreren Mitgliedstaaten ausgearbeitet werden können - oder aber Leitlinien. Datenschutzrechtlich ist außerdem erforderlich, die betroffene Person transparent über die geplante Datenverarbeitung zu informieren und ein Widerspruchsrecht einzuräumen (letzteres verlangt auch das UWG). Der Einwilligungsassistent müsste daher wiederum zwischen Einwilligungserfordernis und („nur“) transparenter Information unterscheiden können.

Hat der Nutzer umgekehrt Interesse an Werbung bzw. fordert diese Informationen ein, könnte eine Wissensplattform wie CoMaFeDS unterstützend eingesetzt werden. Der Plattform ist bekannt, wo welche Datensätze zu finden sind und sie speichert diese Information in verschlüsselter Form. Wie mehrfach erwähnt liegen allerdings noch keine veröffentlichten Details über konkrete Einsatzzwecke und technische Funktionsweise vor. Daher werden im Folgenden anhand eines fiktiven Beispiels mögliche Anforderungen beschrieben:

Plant der Nutzer einen Einkaufsbummel und ist an Angeboten für Kosmetikartikel interessiert, muss beachtet werden, dass gemäß der oben dargestellten Empfehlungen der Artikel-29-Datenschutzgruppe eine pauschale Einwilligung unzulässig ist und die Informiertheit für den bestimmten Fall sichergestellt sein muss. Grundsätzlich müsste in einem Einwilligungsprozess folgendes berücksichtigt werden:

- Der Nutzer gibt an, dass er an Kosmetikangeboten von sämtlichen Geschäften in der Umgebung seines aktuellen Standortes während seines Einkaufbummels interessiert ist. Die Plattform speichert diese Information in verschlüsselter Form. Ein potenzieller Empfänger fragt an, ob für ihn relevante Datensätze vorhanden sind, ohne dass (wie von auch CoMaFeDS geplant) bereits konkrete Daten übermittelt werden. Es erfolgt lediglich eine Beschreibung der Datenstruktur. Datenschutzrechtlich muss sichergestellt sein, dass CoMaFeDS die „Anonymität“ der Nutzer im Hinblick auf die potenziellen Empfänger tatsächlich umsetzen kann. (Nach Offenlegung der technischen Details wäre diese Anforderung zu überprüfen, insbesondere unter Ausschluss von eventuellen Verknüpfungsmöglichkeiten).

- Der Einwilligungsassistent müsste daraufhin in der Lage sein, eine entsprechende granulare Liste mit Auswahlmöglichkeiten von Geschäften (Empfängern) und Kosmetikartikeln automatisiert zum Zwecke der Werbung zu erstellen. Der Nutzer muss die Möglichkeit haben, die einzelnen generierten Felder aktiv anzuklicken. Die Einwilligung und die Verwendung der Standortdaten muss auf die Dauer des Einkaufs begrenzt sein. Es müsste daher ein dynamischer Einwilligungsprozess erfolgen (wie von CoMaFeDS geplant).[153]

153 Die Rechtmäßigkeitsvoraussetzungen sind gesondert zu prüfen.

Der „Kontext“ einer Einwilligung gewinnt somit an Bedeutung, da das Fortschreiten der Technik mehr Möglichkeiten bietet, Daten zu verarbeiten und zu verknüpfen, so dass hier vernünftige Grenzen gefunden werden müssen.

Für Informationen, die als Werbung einzustufen sind wäre im Übrigen in dem oben genannten Beispiel bei Verwendung eines „Wissensgraphen“ (CoMaFeDS) und dynamischer Einwilligung und unter Bezug zum Wettbewerbsrecht zu berücksichtigen, dass bei Erhalt der Daten des Nutzers der Empfänger (Anbieter von Kosmetikartikel) im Sinne von § 7 Absatz 3 UWG noch kein Unternehmer ist, der im Zusammenhang mit dem Verkauf einer Ware oder Dienstleistung von dem Kunden dessen elektronische Postadresse erhalten hat, so dass er diese gerade nicht zur Direktwerbung für eigene ähnliche Waren oder Dienstleistungen verwenden darf. Er muss sich vielmehr an die granularen Vorgaben des Nutzers halten, die dieser aktiv bei Verwendung des Einwilligungsassistenten vorgegeben hat.[154]

! Fazit Nr. 7

Insgesamt kann lediglich eine allgemeinere Betrachtung für den Einwilligungsassistenten erfolgen, da dessen Verwendung, Einsatzzwecke und Betreiben sich bislang in den Anfangsüberlegungen der Entwickler befinden. Diesbezüglich wird ebenso auf die Abschnitte „Zukünftige Fragestellungen“[155] und „Verantwortung“[156] verwiesen.

Festzuhalten ist aber:
Nur wenn Nutzer für den bestimmten Einzelfall eine Vorauswahl der Einwilligungselemente granular aktivieren konnten, kann der Einwilligungsassistent diese Entscheidung überhaupt automatisiert übernehmen. Hier kann es hilfreich sein, wenn sich die Entwickler an der Umsetzung des Projekts „Platform for Privacy Preferences“ (P3P) orientieren, das in der Bestandsaufnahme dargestellt wurde. Damit könnte die Direkterhebung von Daten weiterhin forciert werden, auch wenn diese als Grundsatz in der Datenschutz-Grundverordnung nicht mehr verankert ist.

Bei Unterstützung durch einen Einwilligungsassistenten müssen die unterschiedlichen Rechtsgrundlagen einer Datenverarbeitung (z. B. Erforderlichkeit für vertragliche Zwecke oder berechtigte Interessen) berücksichtigt werden, so dass stets geprüft werden muss, ob eine Einwilligung als Rechtsgrundlage überhaupt in Betracht kommt. Es ist daher zwischen Einwilligungserfordernis und „nur“ transparenter Information über die Datenverarbeitung zu unterscheiden.

Der Einwilligungsassistent kann aufgrund der Möglichkeit der Bereitstellung granularer Komponenten zur Transparenz der Einwilligung beitragen, so dass seine technische Entwicklung dahingehend erfolgen sollte, die Granularität und Transparenz sicherzustellen und nicht diese umzukehren, in dem Verarbeitungsvorgänge oder Zwecke in einem weiten Verständnis ausgelegt werden.

154 *Je nachdem, welche Funktionen geplant sind, könnte zudem die folgenden wettbewerbsrechtlichen Aspekte zu berücksichtigen sein: Das Kammergericht Berlin ist noch von einer möglichen Zulässigkeit der Versendung einer Freundesliste sowie der Versendung von Einladungs-E-Mails ausgegangen mit der Begründung, dass dies dem privaten Nutzer zuzurechnen sei (KG Berlin Urteil vom 24.01.2014, Az.: 5 U 42/12). Der Bundesgerichtshof hat jedoch entschieden, dass die mithilfe der Funktion „Freunde finden“ des Internet-Dienstes „Facebook“ versendeten Einladungs-E-Mails an Personen, die nicht als „Facebook“-Mitglieder registriert sind, eine wettbewerbsrechtlich unzulässige belästigende Werbung darstellen (BGH Urteil vom 14.01.2016, Az.: I ZR 65/14). Überträgt man dies auf den oben genannten Fall, wäre eine Funktion, die Kneipen- oder Restaurantempfehlungen, Einkaufstipps, etc. für „Freunde“ bereitstellt, ebenso kritisch zu beleuchten.*

155 *Siehe S. 56 ff.*

156 *Siehe hierzu auch den Punkt „Verantwortung“ auf S. 52 ff.*

!

In Anlehnung an die Ausführungen der Artikel-29-Datenschutzgruppe muss der Nutzer selbst aktiv werden. Vorstellbar wäre beispielsweise im Hinblick auf Standortdaten ein Tätigwerden unmittelbar vor oder während einer Reise durch aktive Auswahl von Präferenzen, begrenzt auf die Dauer der Reise, für bestimmte Zwecke (z. B. Restaurantempfehlungen oder Wetterinformationen) und für den konkreten Ort. Es ist nicht möglich, eine automatische Standortbestimmung vorzunehmen, wenn der Nutzer zuvor nicht für diesen bestimmten Fall informiert eingewilligt hat. Wichtig wäre bei der Granularität ebenso die Berücksichtigung der Ortungsmöglichkeiten. Eine genaue Standortbestimmung ist nicht immer erforderlich. Unternimmt der Nutzer aber eine Städtereise, möchte er abends bei Ankunft im Hotel gegebenenfalls die Restaurants in unmittelbarer Nähe angezeigt erhalten. Diesen Detaillierungsgrad sollte ein Einwilligungsassistent berücksichtigen.

Konzepte wie CoMaFeDS könnten bei Forschungszwecken unterstützend eingesetzt werden. Gemäß Erwägungsgrund 33 Datenschutz-Grundverordnung kann die betroffene Person ihre Einwilligung für bestimmte Bereiche wissenschaftlicher Forschung geben, d.h. ohne vollständige Angabe des Zwecks. Dies könnte ebenso entsprechend für die Empfänger (im Sinne von Datennehmern) gelten.

Was unter „einer“ Verarbeitungstätigkeit oder dem „Kontext“ einer Einwilligung innerhalb einer komplexen Datenverarbeitung sinnvollerweise verstanden werden kann, muss bei Verwendung eines Einwilligungsassistenten der Einzelfallbetrachtung obliegen. Hier muss kritisch geprüft werden, inwieweit die Erstellung einer automatisierten Einwilligungserklärung anhand der Datenschutzhinweise systemseitig in Betracht kommen kann. Die Einwilligung „in einem Kontext“ und die Zweckänderung nach Artikel 6 Absatz 4 Datenschutz-Grundverordnung benötigen klare Grenzen.

In Bezug auf Werbung ist dabei folgendes zu berücksichtigen: Das Bundesdatenschutzgesetz und das Gesetz gegen den unlauteren Wettbewerb (UWG) stehen aktuell gleichberechtigt nebeneinander. § 7 Absatz 3 UWG bietet allerdings bei elektronischer Werbung insoweit eine Erleichterung, dass ein Unternehmer, der im Zusammenhang mit dem Verkauf einer Ware oder Dienstleistung von dem Kunden dessen elektronische Postadresse erhalten hat, diese zur Direktwerbung für eigene ähnliche Waren oder Dienstleistungen verwenden darf. Die Frage ist, welche Auswirkung dies auf die datenschutzgerechte Gestaltung eines Einwilligungsassistenten und die Übersendung von ähnlichen Dienstleistungsangeboten haben könnte. Datenschutzrechtlich muss die betroffene Person die geänderte Verarbeitungstätigkeit oder den Zweck vernünftigerweise erwarten dürfen. Fraglich ist jedoch, ob dies in einem europaweiten Vergleich stets gleichbedeutend mit „ähnlicher“ Zweck zu verstehen ist. Hier kommt es ebenso darauf an, ob das Markenrecht oder das Kartellrecht als Auslegungshilfen heranzuziehen sind. Im Übrigen empfiehlt sich hier eine europaweite Gesamtschau und entsprechende Harmonisierung im Falle eines unterschiedlichen Verständnisses in Europa. Rechtsunsicherheiten, die sich durch „berechtigte Interessen“ zur Direktwerbung ergeben, lassen sich ebenso durch einheitliche Verhaltensregeln beheben. Eine pauschale Einwilligung ist unwirksam. Entwickler von Konzepten wie CoMaFeDS könnten jedoch die Möglichkeit einer „pauschalen Interessensbekundung“ prüfen. Wird wie hier eine Wissensplattform zentral erstellt, wäre auch denkbar, dass der Nutzer ein Interesse kundtut (etwa: „Ich möchte Informationen über günstige Kosmetikangebote während meines Einkaufs“ oder „Ich nehme an jedem Gewinnspiel teil, bei dem ich einen Fernseher gewinnen kann“). Die Einwilligung, die in Bezug auf einen konkreten Anbieter und ein konkretes Angebot erteilt wird, muss jedoch stets „für den bestimmten Fall in informierter Weise“ erfolgen. Der „Wissensgraph“ müsste daher eine dynamische Einwilligungsmöglichkeit bieten und beim Nutzer eine automatisierte Rückfrage stellen (können), ob dieser mit der konkreten Datenverarbeitung einverstanden ist. Der Nutzer muss auf der Grundlage der Datenschutzbestimmungen des einzelnen Anbieters eine freie und informierte Entscheidung treffen können.

! Bei einer solchen zentralen Datenspeicherung mit Zugriffsmöglichkeiten von unterschiedlichen Empfängern ist vor allem an die Sicherheit des „Wissensgraphen“ (CoMaFeDS) und ausreichende Verschlüsselung zu denken. Außerdem ist die Frage entscheidend, wer Verantwortlicher dieses „Wissensgraphen“ und ob sowie in welcher Form diesbezüglich eine zusätzliche Einwilligung des Nutzers vorliegen muss. Es empfiehlt sich außerdem eine Zertifizierung, da ein Nutzer die technischen Voraussetzungen, technische Sicherheit und die Vorgehensweise einer Datenverarbeitung nicht überblicken kann.[157] Gemäß dem aktuellen Entwicklungsstand enthält die Plattform selbst keine Datensätze, sondern nur das (verschlüsselte) Wissen, wo diese zu finden sind. Ein Nutzer muss jedoch die Gewissheit haben, dass die Verschlüsselung ausreichend, seine Anonymität gegenüber potenziellen Empfängern gewahrt ist und keine Verknüpfungsmöglichkeiten bestehen, insbesondere da diese Plattform großes Potenzial für Big Data-Anwendungen bietet. Ob die erforderliche Sicherheit der Datenverarbeitung umsetzbar ist, muss einer gesonderten technischen Bewertung unterliegen (in dieser Stellungnahme werden lediglich rechtliche Anforderungen geprüft).

III. Freiwilligkeit und Kopplungsverbot

1. Voraussetzungen

Gemäß Artikel 4 Nr. 11 Datenschutz-Grundverordnung muss es sich bei einer Einwilligung um eine freiwillige Willensbekundung handeln. Artikel 7 Absatz 4 Datenschutz-Grundverordnung konkretisiert dies dadurch, dass „bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, dem Umstand in größtmöglichem Umfang Rechnung getragen werden muss, 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.“

Im Vergleich dazu muss im Sinne von Artikel 2h der Richtlinie 95/46/EG eine Willensbekundung ohne Zwang erfolgt sein. Hierzu wird vertreten, dass die Freiwilligkeit nicht mehr gegeben ist, wenn die betroffene Person die Willensbekundung in sozialer oder wirtschaftlicher Schwäche oder Unterordnung erteilt hat oder wenn sie einen Verstoß gegen zwingende Schutznormen darstellen würde.[158] Auch im Arbeitsverhältnis wird die Freiwilligkeit der Einwilligung kritisch gesehen.[159]

157 *Siehe jedoch unter E. Verantwortlichkeit (S. 50 ff.), dass auch bei dezentraler Speicherung beim Nutzer eine Zertifizierung des Systems von außerordentlicher Wichtigkeit sein kann.*

158 *Brühann: in Grabitz/Hilf, Das Recht der Europäischen Union, 40. Auflage, 2009, Loseblattsammlung, Stand: Mai 1999 Ergänzungslieferung 13, A30, Art. 2 Rn. 28.*

159 *Artikel-29-Datenschutzgruppe, Stellungnahme 8/2001 zur Verarbeitung personenbezogener Daten von Beschäftigten, 10. Siehe auch Däubler, Gläserne Belegschaften?, 5. Aufl. Frankfurt 2010, Rn. 150 ff., der unter Rn. 160 ausführt, dass die Freiwilligkeit nur gewahrt ist, wenn die Willensbildung des Betroffenen nicht in unangemessener Weise beeinflusst wurde („Überrumpelung“, zielgerichtete Beratung) und wenn keine vermeidbaren Nachteile oder übermäßigen Vorteile in Aussicht gestellt wurden. Außerdem: Gola, Die Einwilligung als Legitimation für die Verarbeitung von Arbeitnehmerdaten, RDV 2002, S. 109 ff.*

Im Verlaufe der Verhandlungen zur Datenschutz-Grundverordnung konnte sich die Benennung eines „Ungleichgewichts“ im unmittelbaren Verordnungstext nicht durchsetzen. Vielmehr wurde lediglich im Erwägungsgrund 43 formuliert, dass die Einwilligung in besonderen Fällen keine gültige Rechtsgrundlage liefern sollte, nämlich 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. Allerdings wurde der Vorschlag nicht übernommen, die Marktmacht als einen Fall des Ungleichgewichts klar zu benennen[160].

Zum Kopplungsverbot etwa Gola/Schomerus, Bundesdatenschutzgesetz, 11. Auflage 2012, § 28 Rn. 46; Taeger in: Taeger/Gabel, Kommentar zum BDSG (2010), § 28 Rn. 180 ff.

Im deutschen Recht ist die Regelung in § 28 Absatz 3b BDSG zum Kopplungsverbot auf die Fälle der Einwilligung im Bereich Werbung und Adresshandel beschränkt. Außerdem ist diese Regelung sehr weit gefasst: Das Kopplungsverbot soll nur gelten, wenn dem Betroffenen ein anderer Zugang zu gleichwertigen vertraglichen Leistungen ohne die Einwilligung nicht oder nicht in zumutbarer Weise möglich ist. Dies bedeutet, dass die „Freiwilligkeit“ überall dort weiterhin bestehen würde, wo die betroffenen Personen entsprechende Leistungen bei anderen Unternehmen in Anspruch nehmen können. Letztendlich muss das Unternehmen nach überwiegender Meinung also eine Monopolstellung innehaben.[161] Im Sinne dieser Auslegung kann das Kopplungsverbot bei international vorhandenen Dienstleistungen kaum praktische Anwendung finden, da es unwahrscheinlich ist, kein als gleichwertig zu betrachtendes Angebote zu finden.

Der Bundesrat hatte aus diesem Grunde in der Vergangenheit vorgeschlagen,[162] dass die verantwortliche Stelle den Abschluss eines Vertrags nicht von einer Einwilligung des Betroffenen nach Absatz 3 Satz 1 abhängig machen dürfe. Eine solche Einwilligung sei unwirksam. Dies bedeutet, dass die betroffene Person den Dienst dennoch in Anspruch nehmen könnte, was ihr Recht auf informationelle Selbstbestimmung insgesamt stärken würde. Ein solches allgemeines Kopplungsverbot ist nunmehr auch in Artikel 7 Absatz 4 der Datenschutz-Grundverordnung enthalten, jedoch unter der Einschränkung, dass hier keine eindeutige Formulierung wie im Entwurf des Bundesrats vorgesehen ist, sondern lediglich ein Maßstab zur Beurteilung der Freiwilligkeit. Im Erwägungsgrund 43 wird näher präzisiert, dass die Einwilligung nicht als freiwillig erteilt gilt, 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.

160 Siehe Änderungsantrag 20 zu Erwägungsgrund 34 im Berichtsentwurf 2012/0011 (COD) vom 16.01.2013; Entwurf eines Berichts über den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung)

161 Zum Kopplungsverbot etwa Gola/Schomerus, Bundesdatenschutzgesetz, 11. Auflage 2012, § 28 Rn. 46; Taeger in: Taeger/Gabel, Kommentar zum BDSG (2010), § 28 Rn. 180 ff.

162 Bundesrat-Drucksache 55/1/15 vom 16.03.2015 „Entwurf eines Gesetzes zur Verbesserung der zivilrechtlichen Durchsetzung von verbraucherschützenden Vorschriften des Datenschutzrechts“; http://www.bundesrat.de/SharedDocs/drucksachen/2015/0001-0100/55-1-15.pdf?__blob=publicationFile&v=4. Siehe zum Kopplungsverbot auch die Ausführungen von Jan Albrecht unter https://www.janalbrecht.eu/fileadmin/material/Dokumente/Datenschutzreform_Stand_der_Dinge_10_Punkte_070115.pdf“Das Parlament hat ausdrücklich ein Kopplungsverbot vorgesehen, um zu verhindern, dass Dienste nur mit überschießenden Datensammlungen genutzt werden können.“

2. Relevanz für den Einwilligungsassistenten

Der Einwilligungsassistent muss so gestaltet sein, dass die betroffene Person frei zwischen unterschiedlichen Daten, Zwecken und Empfängern wählen kann. In diesem Sinne kann der Einsatz eines solchen Assistenten eine Unterstützung für die betroffene Person darstellen, da dieser in übersichtlicher Weise die Datenverarbeitung auflistet und die betroffene Person sich zwischen den Verarbeitungstatbeständen frei entscheiden kann.

Bei Nichteinwilligung in einzelne Verarbeitungstatbestände dürfen ihr insbesondere ohne finanziellen Druck keine Nachteile entstehen. Die Einwilligung darf in diesem Zusammenhang nicht irreführend sein. Die Artikel-29-Datenschutzgruppe verweist etwa darauf, dass eine Einwilligung des Betreffenden nicht eingeholt werden darf, um die Verarbeitung zu legitimieren, wenn eine medizinische Fachkraft aus medizinisch indizierten Gründen in einer bestimmten Situation nicht anders kann als personenbezogene Daten in einer elektronischen Patientenakte zu verarbeiten. Eine Einwilligung sollte auf die Fälle beschränkt werden, in denen die betreffende Person tatsächlich frei entscheiden kann und anschließend die Einwilligung ohne irgendwelche Nachteile zurückziehen kann.[163]

Es sollte zudem keine Datenverarbeitung legitimiert werden, die bereits durch andere Rechtsgrundlagen abgedeckt ist.[164] In diesem Sinne würde es ebenso an der Freiwilligkeit fehlen. Dieser Umstand könnte nur „geheilt“ werden, wenn deutlich wird, dass sich der Datenverarbeiter bei einem etwaigen Widerruf der Einwilligung nicht zusätzlich auf diese Rechtsgrundlage beruft, um die Datenverarbeitung trotzdem weiter zu verfolgen. Ein solches Verhalten wäre aus datenschutzrechtlicher Sicht unzulässig.

Der Düsseldorfer Kreis hat bereits für Apps entschieden,[165] dass der Nutzer die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen können muss. Es handele sich nicht um eine wirksame Einwilligung, wenn der Nutzer entweder den Dienst „so nehmen müsse, wie er ist“ oder den Dienst nicht in Anspruch nehmen kann und ein Widerruf der „Einwilligung“ nur durch Beendigung des Nutzungsvertrags möglich ist.[166]

Für den Einwilligungsassistenten bedeutet dies, dass bereits bei der Entwicklung zu prüfen ist, inwieweit die Erbringung einer Dienstleistung von einer Einwilligung abhängig gemacht wird, obwohl diese Einwilligung für die Erfüllung nicht erforderlich ist (was auch dem Grundsatz „Datenschutz durch Technikgestaltung“ gemäß Artikel 25 Datenschutz-Grundverordnung entspricht).

Sofern der Nutzer wie bei einer App als Gegenleistung mit seinen Daten bezahlen soll, wäre fraglich, ob diese Daten für die Durchführung der Dienstleistung erforderlich sind.

163 *Artikel-29-Datenschutzgruppe, WP 131, Arbeitspapier Verarbeitung von Patientendaten in elektronischen Patientenakten (EPA), angenommen am 15. Februar 2007; S. 9.*

164 *Siehe Artikel 29-Datenschutz-Gruppe Fn. 122.*

165 *Düsseldorfer Kreis, S. 17 -Orientierungshilfe- Datenschutzanforderungen an App-Entwickler und App-Anbieter vom 16.06.2014: Eine App dürfe zudem nur die erforderlichen Berechtigungen vom Nutzer anfordern und es wird in diesem Zusammenhang dargestellt, dass einige Betriebssysteme Berechtigungen lediglich in festen Kombinationen anbieten, welche neben den erforderlichen auch nicht benötigte Datenzugriffe enthielten, so dass dies bei der Entwicklung zu berücksichtigen sei. Als Beispiel nennt der Düsseldorfer Kreis Android, welches bis zur Version 4.0 den Zugriff auf das Kontaktverzeichnis nicht zugelassen habe, ohne zugleich Zugriffsrechte auf den Anrufverlauf zu bekommen. Insgesamt sei ein Zugriff auf das gesamte Adressbuch des Geräts mit all den darin hinterlegten persönlichen Informationen des Nutzers und seiner Kontakte und deren Verwendung nicht zulässig, wenn lediglich z. B. eine Adresse für die Navigation mit einer App benötigt werde (siehe S. 17)*

166 *Düsseldorfer Kreis, S. 15 Fn. 26 - Orientierungshilfe- Datenschutzanforderungen an App-Entwickler und App-Anbieter vom 16.06.2014.*

Wie oben ausgeführt, hat der Düsseldorfer Kreis die Empfehlung gegeben, dass keine wirksame Einwilligung vorliegen soll, wenn eine wirksame Nutzung nur unter Beendigung des Nutzungsvertrages möglich ist.[167] Der Bundesrat hat in seinem Gesetzesentwurf zum Kopplungsverbot im Bundesdatenschutzgesetz zudem darauf hingewiesen, dass besondere Gefahren erheblicher Verletzungen des Persönlichkeitsrechts unterbunden werden, indem Unternehmen wirksam untersagt wird, Angebote von dem Einverständnis der Kunden in die Datennutzung abhängig zu machen oder auf einen anderen Erlaubnistatbestand zurückzugreifen. Dies gelte umso mehr, als dem Kunden oftmals nicht klar sein wird, welche der Angaben zu seiner Person und zu seinen persönlichen Verhältnissen zu Werbe-, Marketing-, Score- oder anderen erlaubten Zwecken verwendet wird. Wichtig sei, dass der Einwilligende in Kenntnis aller Umstände frei bestimmt, wenn er sich mit der Erhebung und Verwertung seiner persönlichen Daten einverstanden erklärt, also er selbstbestimmt entscheidet, ob er für das Angebot mit Daten oder Euro bezahlen will. Insoweit wird es für erforderlich gehalten, dass die Einwilligung in Datennutzungsrechte nicht mit Vorteilen, die Dritte einräumen, gekoppelt werden dürfe.[168]

Auch wenn dieses Gesetz nicht in Kraft getreten ist, können diese Ausführungen als Auslegungshilfe „für die Wahrung des Persönlichkeitsrechts“ dienen und sollten ebenso für Artikel 7 Absatz 4 Datenschutz-Grundverordnung herangezogen werden. In Bezug auf diesen Punkt könnten die deutschen Datenschutzaufsichtsbehörden bereits zum jetzigen Zeitpunkt Anforderungen festlegen und ihre Auffassung zur Auslegung kundtun, wobei zukünftig europaweit eine Verhaltensregel (soweit diese aufgrund einer Verarbeitungstätigkeit in mehreren Mitgliedstaaten ausgearbeitet werden kann) oder eine Leitlinie durch den Europäischen Datenschutzausschuss erstellt werden sollte, um ein einheitliches Schutzniveau sicherzustellen.

Für den Einwilligungsassistenten bedeutet dies, dass die Freiwilligkeit im Besonderen bei der Gestaltung des Systems zu berücksichtigen ist und bei kostenlosen Diensten, bei denen im Gegenzug Daten bereit gestellt werden sollen, besondere Vorsicht geboten ist. Diese werbefinanzierten Dienste kommen auch bei Smart-TV-Angeboten in Betracht.[169]

Sofern für die unterschiedlichen Zwecke eine Einwilligung eingeholt wird, muss darüber hinaus im besonderen Maße geprüft werden, ob es für die betroffene Person irreführend ist, sich darüber hinaus auf berechtigte Interessen gemäß Artikel 6 f Datenschutz-Grundverordnung zu stützen. Auch bezüglich der berechtigten Interessen obliegen dem Verantwortlichen Informationspflichten nach Artikel 13 Absatz 1 d Datenschutz-Grundverordnung, und zwar bei Erhebung der persönlichen Daten (wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden).

167 *Düsseldorfer Kreis, S. 15 Fn. 26 - Orientierungshilfe- Datenschutzanforderungen an App-Entwickler und App-Anbieter vom 16.06.2014.*

168 *Bundesrat-Drucksache 55/1/15 vom 16.03.2015 „Entwurf eines Gesetzes zur Verbesserung der zivilrechtlichen Durchsetzung von verbraucherschützenden Vorschriften des Datenschutzrechts“; http://www.bundesrat.de/SharedDocs/drucksachen/2015/0001-0100/55-1-15.pdf?__blob=publicationFile&v=4*

169 *Siehe Düsseldorfer Kreis, S. 15 - Orientierungshilfe zu den Datenschutzanforderungen an Smart-TV-Dienste vom 15./16.09. 2015. https://www.datenschutz-hamburg.de/news/detail/article/orientierungshilfe-datenschutzanforderungen-an-smart-tv-dienste.html?tx_ttnews%5BbackPid%5D=203&cHash=ff2c5449bcoeba90ba131dbe32a19db1*

Daher ist der Verantwortliche angehalten, dies klar zu trennen:

- Es geht einerseits um die Verarbeitung, die auf der Einwilligung gemäß Artikel 6 Absatz 1 a Datenschutz-Grundverordnung beruht. Diese muss gemäß Artikel 4 Nr. 11, Artikel 7 und Artikel 13 Absatz 2 c Datenschutz-Grundverordnung in informierter Weise erfolgen (wenn die Verarbeitung auf Artikel 6 Absatz 1 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).

- Plant der Verantwortliche die Datenverarbeitung darüber hinaus auf berechtigte Interessen gemäß Artikel 6 Absatz 1 f Datenschutz-Grundverordnung zu stützen, muss insbesondere beim Einholen einer Einwilligung darauf geachtet werden, dass nicht der Eindruck erweckt wird, dass die Datenverarbeitung sei durch die Einwilligung abschließend abgedeckt. Es muss vielmehr eine transparente Information erfolgen, welche Datenverarbeitung stattfinden soll und auf welcher Rechtsgrundlage diese erfolgt.

Insgesamt muss die Datenverarbeitung fair und nachvollziehbar bleiben (Artikel 5 Absatz 1 a Datenschutz-Grundverordnung).

! Fazit Nr. 8

Die betroffene Person muss darüber informiert werden, ob sie gesetzlich oder vertraglich verpflichtet ist, ihre personenbezogenen Daten preiszugeben oder ob die Bereitstellung für einen Vertragsschluss erforderlich ist. Darüber hinaus ist sie darüber in Kenntnis zu setzen, was die möglichen Folgen einer verweigerten Bereitstellung sind.

Ist die Rechtsgrundlage der Datenverarbeitung die Einwilligung, kann der Einwilligungsassistent durch Zusammenstellung und Auflistung klar beschriebener Zwecke, Empfänger und der verwendeten Daten zur Informiertheit und damit Transparenz bei der Einwilligung beitragen.

Es darf dennoch bei Verwendung eines Einwilligungsassistenten nicht der Eindruck entstehen, dass damit die Datenverarbeitung abschließend abgedeckt ist, wenn beispielsweise darüber hinaus eine Verarbeitung aufgrund berechtigter Interessen geplant ist. In diesem Falle muss besonders auf die Nachvollziehbarkeit für den Betroffenen geachtet werden und Einwilligung und Information über Datenverarbeitung aufgrund anderer Rechtsgrundlagen klar getrennt werden.

Bei der Auslegung des Kopplungsverbots ist im besonderen Maße auf die freie Bestimmung durch die betroffene Person zu achten. Es müssen die Gesamtumstände berücksichtigt werden, ob sie tatsächlich vollständig überblicken kann, für welche Marketing- und/oder Scoringzwecke ihre persönlichen Daten verwendet werden. Diese Selbstbestimmtheit kann im Einzelfall schwierig zu ermitteln sein. Aber je mehr Zwecke miteinander verknüpft sind oder je mehr Datenempfänger involviert sind, desto wahrscheinlicher ist die Unübersichtlichkeit für den Betroffenen.

! Der Gesetzesvorschlag des Bundesrats hinsichtlich eines Kopplungsverbots beinhaltet Hinweise für mögliche Anforderungen zur Wahrung des Persönlichkeitsrechts. Die Ausführungen könnten daher bei der Auslegung von Artikel 7 Absatz 4 Datenschutz-Grundverordnung herangezogen werden. In Bezug auf diesen Punkt könnten die deutschen Datenschutzaufsichtsbehörden bereits zum jetzigen Zeitpunkt Anforderungen festlegen und ihre Auffassung kundtun, wobei zukünftig europaweit eine Verhaltensregel erstellt (soweit diese aufgrund einer Verarbeitungstätigkeit in mehreren Mitgliedstaaten ausgearbeitet werden kann) oder eine Leitlinie durch den Europäischen Datenschutzausschuss bereit gestellt werden sollte.

IV. Dauer der Einwilligung

1. Definition

In den Informationspflichten muss über die Dauer der Einwilligung transparent informiert werden (Artikel 13 Datenschutz-Grundverordnung). Insgesamt ist die Feststellung zu wiederholen, dass die Einwilligung vor Datenverarbeitung einzuholen ist, auch wenn dies weder in der Datenschutz-Grundverordnung noch in der Richtlinie 95/46/EG ausdrücklich fixiert wurde.[170] Damit ist eine Regelung ausgeschlossen, bei der sich eine Person erst gegen die Übermittlung aussprechen kann, nachdem sie bereits stattgefunden hat.[171] Daher darf das Widerspruchsrecht nicht mit der Einwilligung verwechselt werden.[172]

Die Artikel-29-Datenschutzgruppe verweist darauf, dass mit dem Verstreichen der Zeit möglicherweise Zweifel entstehen, ob die Einwilligung, die ursprünglich auf gültigen, ausreichenden Informationen beruhte, immer noch gültig ist, so dass die für die Datenverarbeitung Verantwortlichen den betroffenen Personen die Möglichkeit zur Überprüfung geben sollten.[173]

Hierzu könnten sie diese beispielsweise über ihre aktuelle Wahl informieren und ihnen die Möglichkeit anbieten, sie entweder zu bestätigen oder zu widerrufen, wobei der jeweilige Zeitraum vom Kontext und den Umständen des Falls abhänge.[174]

Die Entscheidungen von Landgerichten, die sich mit der Wirksamkeit von Werbeeinwilligungen befassen, verlangen vom Anbieter nach einer gewissen Zeit die Rückversicherung, dass die Ansprache per Email oder Telefonanruf weiterhin gewünscht ist.[175]

170 Artikel-29-Datenschutzgruppe, WP 187, Stellungnahme 15/2011 zur Definition von Einwilligung, angenommen am 13. Juli 2011, S.11 mit Verweis darauf, dass in deutschem Recht der Begriff „Einwilligung" verwendet werde, was im deutschen Zivilrecht als „vorherige Zustimmung" definiert werde. Siehe auch Überarbeitung von 2002/58/EG: „prior consent".

171 Artikel-29-Datenschutzgruppe, WP 114, Arbeitspapier der Artikel-29-Datenschutzgruppe über eine Gemeinsame Auslegung des Artikels 26 Absatz 1 der Richtlinie 95/46/EG vom 24. Oktober 1995, Arbeitspapier vom 25. November 2005, S. 12. Artikel-29-Datenschutzgruppe, WP 114, Arbeitspapier der Artikel-29-Datenschutzgruppe über eine Gemeinsame Auslegung des Artikels 26 Absatz 1 der Richtlinie 95/46/EG vom 24. Oktober 1995, Arbeitspapier vom 25. November 2005, S. 12.

172 Artikel-29-Datenschutzgruppe, WP 187, Stellungnahme 15/2011 zur Definition von Einwilligung, angenommen am 13. Juli 2011, S. 12.

173 Artikel-29-Datenschutzgruppe, WP 187, Stellungnahme 15/2011 zur Definition von Einwilligung, angenommen am 13. Juli 2011, S. 24: Aus einer Vielzahl von Gründen würden die Leute häufig ihre Meinung ändern, weil ihre ursprünglichen Entscheidungen schlecht waren oder aufgrund einer Änderung der Umstände, beispielsweise wenn ein Kind reifer wird.

174 Artikel-29-Datenschutzgruppe, WP 187, Stellungnahme 15/2011 zur Definition von Einwilligung, angenommen am 13. Juli 2011, S. 24.

175 Siehe LG München Urteil vom 08.04.2010, Az.: 17 HK O 138/10, 17 HKO 138/10 (zu § 7 Absatz 2 Nr. 3 UWG); LG Berlin Beschluss vom 02.07.2004, Az.: 15 O 653/03; LG Hamburg Urteil vom 17.02.2004, Az.: 312 O 645/02.

Wenn bei diesen gerichtlichen Entscheidungen im Werbekontext ein Zeitrahmen von 1,5 bis 2 Jahren angenommen wird, stellt sich in Bezug auf „andere“ Einwilligungen im Einzelfall die Frage, ob die Persönlichkeitsrechte der betroffenen Person stärker betroffen sein könnten als durch den Versand eines Newsletters oder Telefonanrufs, und daher die Überprüfung des Einverständnisses weitaus früher erfolgen muss.[176] In der Literatur wird die Befristung einer datenschutzrechtlichen Einwilligung auf zwei bis drei Jahre befürwortet.[177]

2. Relevanz für den Einwilligungsassistenten

Sofern die betroffene Personen durch entsprechende selbstständige und granulare Einstellungen ihre Einwilligung zu einer bestimmten Datenverarbeitung erteilt, muss sichergestellt sein, dass sie diese nach einer gewissen Zeit überprüfen können oder dass die Einwilligung nur einmalig gilt. Bei der Einwilligung in Verwendung von Standortdaten ist beispielsweise vorstellbar, dass diese für eine Restaurantsuche in einem bestimmten Ort nur einmalig verwendet wird. Ansonsten könnten die Entwickler prüfen, ob ein „technisches Warnsystem“ installiert werden kann, dass nach einem bestimmten Zeitablauf oder in regelmäßigen Abständen die Nutzer automatisiert über erteilte Einwilligungen informiert und die einfache Möglichkeit zur Korrektur bietet. Zu berücksichtigen ist jedoch, dass die Empfänger immer die Möglichkeit haben, Daten der Nutzer in ihr System zu kopieren bzw. zu übertragen, so dass insbesondere zu diesen Systemen eine Rückkopplung der Information erfolgen muss

! Fazit Nr. 9

Die Einwilligung ist auf die Dauer des jeweiligen konkreten Verwendungszwecks zu begrenzen. Konzepte wie LETsmart stellen die automatisierte Löschung nach Wegfall des Verwendungszwecks sicher. Die Empfänger müssen aber gleichermaßen den Widerruf oder die zeitlich befristete Einwilligung berücksichtigen, wenn sie die Daten der Nutzer in ihren eigenen Systemen erfasst haben.
Es sollte entwicklerseitig geprüft werden, ob automatisiert nach einer gewissen Zeitspanne oder regelmäßig eine Information der Nutzer über die erteilte Einwilligungen erfolgen kann, gekoppelt mit der Bereitstellung einer einfachen Widerrufsmöglichkeit.

E. Verantwortlichkeit

Eine besondere Problemstellung bei der Gestaltung eines Einwilligungsassistenten ergibt sich in Bezug auf Haftung und Verantwortlichkeit. Hier sind die technische Entwicklung und der geplante Einsatz zu berücksichtigen, da entschieden werden muss, ob es sich um „nur“ ein Software-Tool in Eigenverantwortung der betroffenen Person handelt und ob der Empfänger damit „nur“ für die im Anschluss folgende Datenverarbeitung nach den allgemeinen Grundsätzen und ohne besondere Verpflichtung für den Einwilligungsassistenten verantwortlich ist,[178] oder ob darüber hinaus eine Einordnung als eigenständiger Dienst, entweder im Sinne eines „Inhaltsdienstes“ gemäß der Richtlinie 2000/31/EG, „inhaltsneutral“ oder als Dienst mit Zusatznutzen in Betracht kommt.

176 *Dies gilt z. B. bei komplexen Datenverarbeitungen, wie sie auch in Zusammenhang mit Smart-TV oder Smart-Grid vorkommen könnten, wenn diese durch Einwilligung legitimiert sind und nicht durch „für zur Vertragserfüllung erforderliche Zwecke“.*

177 *Rogosch, Die Einwilligung im Datenschutzrecht, S. 148.*

178 *Siehe bereits hierzu S. 21.*

Die Frage ist, inwieweit zukünftig die Installation einer Software oder die technische Fortentwicklung des Einwilligungsassistenten als eigener Online-Dienst eingestuft werden kann, so dass der Empfänger der Daten zum Anbieter und damit ebenso zum Verantwortlichen für den Einwilligungsassistenten im Sinne eines Dienstanbieters wird. Möglich wäre ebenso ein zwischengeschalteter „weiterer Anbieter", etwa Anbieter von Telekommunikationsdiensten, der einen solchen Dienst zur Verfügung stellt. In Bezug auf den Empfänger der Daten wäre außerdem denkbar, dass die Verwendung des Einwilligungsassistenten als eine die Datenverarbeitung unterstützende Softwarelösung verstanden wird. In diesem Sinne wäre er zwar Verantwortlicher der ordnungsgemäßen Datenverarbeitung, aber nicht im Sinne eines (Online)Dienstanbieters.

I. Allgemein

Durch die Richtlinie 95/46/EG ist bislang eine generelle Meldepflicht bei den Aufsichtsbehörden vorgesehen, sofern personenbezogene Daten verarbeitet werden.[179]

Die Datenschutz-Grundverordnung geht nun insgesamt von einem risikobasierten Ansatz anstatt einer grundsätzlichen Meldepflicht aus, um zukünftig einen bürokratischen und finanziellen Aufwand zu verhindern. Gemäß Erwägungsgrund 89 der Datenschutz-Grundverordnung sollen die bestehenden unterschiedslosen Meldepflichten nunmehr durch wirksame Maßnahmen ersetzt werden, die sich mit denjenigen Verarbeitungsvorgängen befassen, die aufgrund

- ihrer Art
- ihres Umfangs
- ihrer Umstände
- ihrer Zwecke

wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringen. Zu solchen Arten sollen insbesondere die Verarbeitungsvorgänge zählen, bei denen neue Technologien eingesetzt werden und die neuartig sind und bei denen der Verantwortliche noch keine Datenschutzfolgeabschätzung durchgeführt hat.

Dies bedeutet, dass ein Unternehmen zukünftig eine Risikobewertung vor Verarbeitungsvorgängen durchführen muss. Hierbei ist entscheidend, dass objektive Kriterien gefunden werden, die den Betroffenen in den Fokus der Bewertung stellen und anhand derer die Eintrittswahrscheinlichkeit und Schwere eines Risikos für dessen Rechte und Freiheiten ermittelt werden kann.

Wichtig ist hierbei, dass das Unternehmen gleichzeitig die Maßnahmen und Verfahren im Blick hat, mit denen dieses Risiko eingedämmt werden kann. Die Datenschutz-Grundverordnung nimmt etwa immer wieder Bezug auf die Pseudonymisierung als geeignete Garantie für die Betroffenenrechte.

179 *Bei der Umsetzung dieser Richtlinie in nationales Recht hat Deutschland gemäß § 4d Absatz 2 Bundesdatenschutzgesetz (BDSG) eine Ausnahme der Meldepflicht vorgesehen, wenn ein Beauftragter für den Datenschutz im Unternehmen bestellt ist. Aufgrund der unmittelbaren Geltung der Datenschutz-Grundverordnung in den Mitgliedstaaten der Europäischen Union entfällt damit auch die entsprechende Umsetzung der Richtlinie 95/46/EG in § 4d Absatz Bundesdatenschutzgesetz.*

Eine solche Pseudonymisierung kann nach der Datenschutz-Grundverordnung auch innerhalb der verantwortlichen Stelle (Unternehmen) stattfinden, wenn diese sicherstellt, dass die zusätzlichen Informationen, mit denen die personenbezogenen Daten einer betroffenen Person zugeordnet werden können, gesondert aufbewahrt werden.

Für das Unternehmen ist letztendlich entscheidend, dass die erforderliche Risikobewertung vor der Verarbeitung stattfindet, um zu Beginn der Verarbeitung nachweisen zu können, dass die durchgeführte Verarbeitung personenbezogener Daten rechtmäßig gemäß Artikel 5 Absatz 1a Datenschutz-Grundverordnung erfolgt. Eine solche Nachweispflicht bzw. Rechenschaftsverpflichtung ist in der Datenschutz-Grundverordnung in Artikel 5 Absatz 2 ausdrücklich benannt. An dieser Stelle werden zukünftig genehmigte Verhaltensregeln (Artikel 40 Datenschutz-Grundverordnung) und Zertifizierungen (Artikel 42 Datenschutz-Grundverordnung) eine wichtige Rolle einnehmen.

Die Risikobewertung vor Datenverarbeitung orientiert sich dabei an den Regelungen zur Datenschutz-Folgenabschätzung gemäß Artikel 35 und 36 Datenschutz-Grundverordnung. Die Aufsichtsbehörde muss von dem Unternehmen vor der geplanten Verarbeitung außerdem nur dann konsultiert werden, wenn eine Form der Verarbeitung, insbesondere die 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 hat.

Diese Risikobewertung liegt in der Hand des Unternehmens als Verantwortlichen.[180]

Gemäß Artikel 35 Absatz 7 Datenschutz-Grundverordnung muss eine Datenschutz-Folgenabschätzung zumindest Folgendes enthalten:

- Systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem für die Verarbeitung Verantwortlichen verfolgten berechtigten Interessen.

- Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck.

- Bewertung der Risiken der Rechte und Freiheiten der betroffenen Personen.

180 *Gemäß der in Deutschland geltenden Regelungen ist bislang eine Vorabkontrolle gemäß § 4d Absatz 5 Bundesdatenschutzgesetz von dem betrieblichen Datenschutzbeauftragten durchzuführen, soweit besonders sensible Daten nach § 3 Absatz 9 Bundesdatenschutzgesetz betroffen sind oder die Datenverarbeitung dazu bestimmt ist, die Persönlichkeit des Betroffenen, einschließlich seiner Fähigkeiten, Leistungen oder seines Verhaltens zu bewerten. Zukünftig ist jedoch ein Datenschutzbeauftragter gemäß Artikel 37 Datenschutz-Grundverordnung nur noch in Ausnahmefällen zu bestellen. Artikel 37 regelt eine grundsätzliche Verpflichtung zur Bestellung eines Datenschutzbeauftragten für öffentliche Stellen, ansonsten nur, wenn*
- 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
- die Kerntätigkeit des Verantwortlichen oder Auftragsverarbeiters in der umfangsreichen Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 besteht.
Sofern die deutsche Gesetzgebung gemäß der Öffnungsklausel in Artikel 37 Absatz 4 von der Möglich Gebrauch macht und in einem Anpassungsgesetz zum Bundesdatenschutzgesetz (entsprechend den Vorgaben der Datenschutz-Grundverordnung) die Regelungen zur Bestellung eines Datenschutzbeauftragten beibehält, ist dieser bei einer Risikoabschätzung zwar um Rat zu fragen. Dies ist aber insoweit abweichend von einer Vorabkontrolle gemäß § 4d Absatz 5 Bundesdatenschutzgesetz, für die der Datenschutzbeauftragte zuständig ist.

- Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht werden soll, dass die Bestimmungen dieser Verordnung eingehalten werden, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen werden soll.

Bei der Risikobewertung sollen gemäß Erwägungsgrund 77 der Datenschutz-Grundverordnung mögliche physische, materielle und immaterielle Schäden berücksichtigt werden. Auch hier wird es zukünftig maßgeblich davon abhängen, ob genehmigte Verhaltensregeln, genehmigte Zertifizierungsverfahren oder Leitlinien des Ausschusses diesbezüglich eine Anleitung enthalten. Die Aufsichtsbehörde soll zudem Listen von Verarbeitungsvorgängen erstellen, für die Datenschutz-Folgenabschätzungen erforderlich oder gerade nicht erforderlich sind (Artikel 35 Absatz 4 und Absatz 5 Datenschutz-Grundverordnung). Dies bedeutet, dass die Intention der Datenschutz-Grundverordnung ist, Unternehmen - auch wenn sie zukünftig keinen Datenschutzbeauftragten bestellt haben – Orientierungshilfen bei der Durchführung der Datenschutz-Folgenabschätzungen von staatlicher Seite zur Verfügung zu stellen.

Gemäß Artikel 30 ist außerdem ein Verzeichnis der Verarbeitungstätigkeiten zu erstellen, und zwar ebenso von Auftragsverarbeitern, in schriftlicher oder elektronischer Form. Der Aufsichtsbehörde ist dieses Verzeichnis nur auf Anfrage zu Verfügung zu stellen. Eine Ausnahme soll hierbei für Unternehmen mit weniger als 250 Mitarbeitern gelten. Diese sind zunächst von der Verpflichtung befreit, ein Verzeichnis der Verarbeitungstätigkeiten zu führen (nicht aber von der Risikobewertung). Allerdings müssen ebenso Unternehmen mit einer Mitarbeiterzahl von weniger als 250 dennoch ein solches Verzeichnis führen, wenn die Verarbeitung ein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt, ebenso wenn sie nicht nur gelegentlich erfolgt.

Da an dieser Stelle im Verordnungstext jedoch nicht ein hohes Risiko verlangt wird, kann unterstellt werden, dass zukünftig bei nahezu jeder dauerhaften Verarbeitung personenbezogener Daten ein Verzeichnis der Verarbeitungstätigkeiten zu führen ist (es sei denn dies würde durch eventuelle Verhaltensregeln gemäß Artikel 40 Datenschutz-Grundverordnung präzisiert).

Ein Verzeichnis der Verarbeitungstätigkeiten soll ebenso eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Datenschutz-Grundverordnung enthalten. Die dort genannten Schutzziele „Integrität, Vertraulichkeit, Verfügbarkeit“ entsprechen den Gewährleistungszielen des Datenschutz-Standard-Schutzmodells (als die drei Risiken der Informationssicherheit).[181] Neu ist der Begriff der Belastbarkeit, der zukünftig ebenso noch der Auslegung bedarf.

Artikel 4 Nr. 2 Datenschutz-Grundverordnung definiert die Verarbeitung als Vorgang oder Vorgangsreihe.[182] Für die Auslegung, was unter einer Verarbeitungstätigkeit zu verstehen ist, die in einem Verzeichnis zu führen ist, sind inhaltlich Artikel 30 Absatz 1 b, c und d Datenschutz-Grundverordnung entscheidend.

181 *Siehe Konzept der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder zur Datenschutzberatung und –prüfung auf der Basis einheitlicher Gewährleistungsziele vom 30.09./01.10.2015. https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2015/10/SDM-Handbuch_V09a.pdf*

182 *Artikel 4 Nr. 2 Datenschutz-Grundverordnung: Im Sinne dieser Verordnung bezeichnet der Ausdruck „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*

Danach sind neben einer Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten sowie der Kategorien von Empfängern, die Zwecke der Verarbeitung anzugeben. Die Frage ist daher, ob mehrere Zwecke einer Verarbeitung in einem Verarbeitungsvorgang oder einer Vorgangsreihe von Verarbeitungen nicht nur sinnvoll verbunden werden können, sondern ob diese Verbindung der Zwecke auch für die betroffene Person im Sinne der Sicherstellung der Transparenz in einer nachvollziehbaren Weise erfolgen und von ihr vernünftigerweise erwartet werden kann.[183]

II. Relevanz für den Einwilligungsassistenten

Eingangs wurde bereits die Problematik dargestellt, dass die Frage der Verantwortlichkeit im Hinblick auf den Einwilligungsassistenten zum jetzigen Zeitpunkt noch nicht abschließend entschieden werden kann. Der Empfänger der Daten ist zwar immer für die Datenverarbeitung verantwortlich. Aber hier geht es vielmehr um den Prozess davor, um die Verantwortung und Haftung für das eingesetzte Tool, welches die betroffene Person bei ihrer Einwilligung unterstützt. Wer führt für dieses System die Datenschutz-Folgenabschätzung durch und ist damit im Sinne der Datenschutz-Grundverordnung Verantwortlicher?

Verantwortlicher ist gemäß Artikel 4 Nr. 7 Datenschutz-Grundverordnung die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet.

Installiert der Nutzer das System als zusätzliche Software auf seinem Rechner, eigenverantwortlich und in seinem Herrschaftsbereich stellt sich die Frage, inwieweit ein Dritter (Empfänger) als Verantwortlicher angesehen werden kann und im Sinne des Gesetzes über die Verarbeitung zumindest mit entscheidet. Ist ein Softwareanbieter tatsächlich „Mitentscheider“? Fraglich ist auch, ob der Empfänger stets dadurch zum Mitentscheider wird, da die Technik auf beiden Seiten (Nutzer und Empfänger) kompatibel sein muss.

Sollte dem Nutzer eine (Mit-)Verantwortung für das eingesetzte System obliegen, muss in diesem Falle ebenso berücksichtigt werden, ob er in dem Sinne „alleingelassen“ werden der Software vertrauen kann? Wer haftet, wenn seine Daten nicht im Sinne der Datenschutz-Grundverordnung ordnungsgemäß verarbeitet werden?

Hier geht es um mehr als nur um die Installation eines technischen Werkzeuges, sondern es geht um die Nachvollziehbarkeit einer Entscheidungsfindung.

Das Forum Privatheit hat etwa auf die Möglichkeit einer wissenschaftlichen Datenschutz-Folgeabschätzung Bezug genommen. Eine wissenschaftlich orientierte Datenschutz-Folgeabschätzung könnte für den Bereich der Forschung und Entwicklung sinnvoll sein, auch wenn sie nicht unbedingt die Anforderungen an eine Datenschutz-Folgeabschätzung im Sinne der Datenschutz-Grundverordnung erfüllt. Dadurch könnten ebenso Fragen des Datenschutzes in das Risikomanagement der Hersteller und Systembetreiber integriert werden.[184] Müsste eine solche auch hier erfolgen, wenn der Nutzer alleine für das Management des Einwilligungsassistenten verantwortlich wäre?

183 *Siehe hierzu bereits die Ausführungen zur Zweckbestimmung, S. 34 ff.*

184 *Siehe hierzu die Ausführungen des Forum Privatheit im White Paper Datenschutz-Folgeabschätzung https://www.forum-privatheit.de/forum-privatheit-de/texte/veroeffentlichungen-des-forums/themenpapiere-white-paper/Forum_Privatheit_White_Paper_Datenschutz-Folgenabschaetzung_2016.pdf, S. 35.*

Eine konkrete Datenschutz-Folgeabschätzung der für die Datenverarbeitung Verantwortlichen (wie in Artikel 35 Datenschutz-Grundverordnung verlangt), könnte im Übrigen ebenso auf einer solchen generischen (wissenschaftlichen, forschungsorientierten) Datenschutz-Folgeabschätzung aufbauen.[185]

Bei einer zentralen Datenspeicherung mit mehreren zugriffsberechtigten Empfängern stellt sich gleichermaßen die Frage nach der Verantwortung sowie zusätzlich nach einer vertrauenswürdigen Instanz.[186] Sofern hier im Sinne einer Wissensplattform große Datenmengen vorhanden sind, ist zu überlegen, wer hier als zertifizierte Stelle die Verantwortung für diese Plattform übernimmt. Diese rechtliche Bewertung könnte sogar mit der Fragestellung verknüpft werden, welche Auswirkungen auf die Gesellschaft zu erwarten sind.[187]

Wenn der Einwilligungsassistent Teil eines Dienstleistungsangebots ist, müssen die Dienstanbieter eine solche Datenschutz-Folgenabschätzung gemäß Artikel 35 Datenschutz-Grundverordnung übernehmen. Wenn jedoch die betroffene Person das Tool in Eigenverantwortung installiert , um mehr Selbstbestimmung über die Daten zu erhalten, sind zwar in Bezug auf die übertragenen Daten die Empfänger die verantwortliche Stelle, in Bezug auf das Tool sind jedoch nur die Hersteller bzw. Entwickler Ansprechpartner. Es besteht einerseits nach der Datenschutz-Grundverordnung die Verpflichtung zur Entwicklung datenschutzfreundlicher Technik gemäß Erwägungsgrund 78, aber andererseits keine Haftung für die Hersteller oder Entwickler.[188] Hinsichtlich „vernetzter Autos“ gibt es allerdings eine gemeinsame Erklärung vom Verband der Autoindustrie und Datenschutzbehörden, dass die Hersteller Ansprechpartner für die Datenschutzbehörden bleiben.[189] Eine weitergehende Verantwortung der Hersteller wird jedoch nicht diskutiert.

Daher stellt sich die Frage, ob Zertifizierungen überhaupt ausreichend sind oder der Gesetzgeber für noch mehr Verantwortung der Hersteller sorgen muss.

Man könnte beispielsweise an eine Erweiterung des Produkthaftungsgesetzes denken. Nach diesem Gesetz können nicht nur Hersteller, sondern sogar Händler haftbar gemacht werden, sofern letztere den Vorlieferanten nicht innerhalb einer bestimmten Frist nennen können. Sofern Persönlichkeitsrechtsverletzungen durch fortschreitende Technik und Datenverknüpfungen zunehmen, könnte sich in entsprechender Ausgestaltung einer Schmerzensgeldtabelle für eingetretene Körperschäden ebenfalls eine Richtschnur für angemessene Beträge entwickeln.[190]

Ein Verbandsklagerecht für Verbraucherverbände ist nun in Artikel 80 Datenschutz-Grundverordnung sowie im deutschen Recht im Unterlassungsklagegesetz berücksichtigt.[191]

185 Siehe hierzu auch Ausführungen des Forum Privatheit im White Paper Datenschutz-Folgeabschätzung https://www.forum-privatheit.de/forum-privatheit-de/texte/veroeffentlichungen-des-forums/themenpapiere-white-paper/Forum_Privatheit_White_Paper_Datenschutz-Folgenabschaetzung_2016.pdf, S. 35.

186 Siehe hierzu die Beschreibung von CoMaFeDS in dieser Stellungnahme, S. 3 ff. und in der Studie der Stiftung Datenschutz, Kapitel II. 2. sowie den Dienst „DigiMe“ Kapitel II. 2. der Stiftungsstudie.

187 Siehe zum „Gefährdungsdiskurs“ in Bezug auf Privat und der Frage, warum Privatheit nicht allein als individueller, sondern auch als gesellschaftlicher Wert betrachtet werden sollte, insgesamt Seubert, Der gesellschaftliche Wert des Privaten, DuD 2012, S. 100 ff.

188 Ungeklärt ist, inwieweit ein Hersteller als „Verantwortlicher“ im Sinne von Artikel 4 Nr. 7 Datenschutz-Grundverordnung eingeordnet werden kann, wenn er Mittel der Verarbeitung bereitstellt.

189 Siehe https://www.vda.de/dam/vda/Medien/DE/Themen/Innovation-und-Technik/Vernetzung/Gemeinsame-Erkl-rung-VDA-und-Datenschutzbeh-rden-2016/Gemeinsame-Erklaerung-VDA-und-Datenschutzbehoerden-2016.pdf

190 Gemäß § 8 Produkthaftungsgesetz kann wegen des Schadens, der nicht Vermögensschaden ist, eine billige Entschädigung in Geld gefordert werden.

191 Siehe Verbraucherschutz in Zeiten von Big Data vom 12.3.2015, S. 28 https://www.bundestag.de/blob/371456/30e60f5f09a696b737bf65fece23afa4/vzbv-data.pdf sowie https://www.bundestag.de/blob/373540/dfa875e79c70deaa7c188933c2b5048b/caspar-data.pdf, S. 8.

Die Regelungen im Unterlassungsklagegesetz ermöglichen Verbraucherverbänden, Wirtschaftsverbänden, Industrie- und Handelskammern und Handwerkskammern Klagemöglichkeiten, die jedoch beschränkt sind auf die unzulässige Erhebung, Verarbeitung oder Nutzung von Verbraucherdaten zu Zwecken der Werbung, der Markt- und Meinungsforschung, des Betreibens von Auskunfteien, des Erstellens von Persönlichkeits- und Nutzungsprofilen, des Adresshandels, des sonstigen Datenhandels oder zu vergleichbaren kommerziellen Zwecken. Die Regelung des Artikel 80 Datenschutz-Grundverordnung geht darüber hinaus, da hiernach „die betroffene Person das Recht hat, eine Einrichtung, Organisationen oder Vereinigung ohne Gewinnerzielungsabsicht, die ordnungsgemäß nach dem Recht eines Mitgliedstaats gegründet ist, deren satzungsmäßige Ziele im öffentlichem Interesse liegen und die im Bereich des Schutzes der Rechte und Freiheiten von betroffenen Personen in Bezug auf den Schutz ihrer personenbezogenen Daten tätig ist, zu beauftragen, in ihrem Namen eine Beschwerde einzureichen, in ihrem Namen die in den Artikeln 77, 78 und 79 genannten Rechte wahrzunehmen und das Recht auf Schadensersatz gemäß Artikel 82 in Anspruch zu nehmen, sofern dieses im Recht der Mitgliedstaaten vorgesehen ist.“ Danach ist jede Datenverarbeitung betroffen, die nicht im Einklang mit der Verordnung besteht.

Im Sinne des umfassenden Persönlichkeitsschutzes wäre zu befürworten, wenn von diesen „Organisationen“ und „Vereinigungen“ des Artikel 80 Datenschutz-Grundverordnung ebenso Gewerkschaften und Betriebsräte umfasst wären und ein entsprechendes Verbandsklagerecht bestehen würde.

! Fazit Nr. 10

Die Entwickler des Einwilligungsassistenten sollen frühzeitig den konkreten Verwendungs- und Einsatzweck definieren, um die Verantwortlichkeiten in der praktischen Umsetzung ausreichend berücksichtigen zu können. Unklar ist, ob der Einwilligungsassistent selbst einen eigenständigen Dienst (z. B. Dienst der Informationsgesellschaft oder Dienst mit Zusatznutzen) darstellen kann.

Wirtschaft und Wissenschaft sollten generische Datenschutz-Folgenabschätzungen bei neuen Technologien gemeinsam entwickeln. Diese können gleichermaßen eine Grundlage für die konkreten Datenschutz-Folgenabschätzungen der Datenschutz-Grundverordnung darstellen.

Liegt das System in der Verantwortung des Nutzers und gibt es im Sinne der Datenschutz-Grundverordnung keinen Verantwortlichen der Datenverarbeitung – ausgenommen dem Nutzer selbst -, ist zumindest ein Datenschutzsiegel (vgl. Erwägungsgrund 100) zu fordern. Unter Umständen könnte auch eine wissenschaftliche Datenschutz-Folgenabschätzung ein adäquates Mittel zur ordnungsgemäßen Prüfung und Wahrung der Betroffenenrechte darstellen.

Hersteller sind zwar angehalten, datenschutzgerechte Technik zu entwickeln, aber ohne konkrete rechtliche Verantwortlichkeit. Ungeklärt ist, inwieweit ein Hersteller als „Verantwortlicher“ im Sinne der Verordnung eingeordnet werden kann, wenn er Mittel der Verarbeitung bereitstellt. Hier könnte über die Erweiterung des Produkthaftungsgesetzes nachgedacht werden. Die Datenschutzaufsichtsbehörden haben mit dem Verband der Automobilindustrie eine gemeinsame Erklärung unterzeichnet, so dass Hersteller als Ansprechpartner zur Verfügung stehen sollen. Solche Erklärungen sollten zukünftig auch bei anderen technischen Entwicklungen in Betracht kommen.

Im Hinblick auf Artikel 80 Datenschutz-Grundverordnung könnte klargestellt werden, ob damit auch Arbeitnehmervertretungen/Gewerkschaften erfasst sind.

F. Zukünftige Fragestellungen

Die oben dargestellte Prüfung geht davon aus, dass der Einwilligungsassistent im Sinne der granularen Vorgaben einer betroffenen Person die erteilte Einwilligung umsetzt. Das System wird nicht selbstlernend verwendet und trifft darauf basierend keine eigenen Entscheidungen. Wenn das System jedoch über diese genannten Voraussetzungen hinaus eingesetzt wird, sollen kurz die beiden folgenden Fragen skizziert werden, ohne diese jedoch abschließend prüfen zu können.

I. Automatisierte Entscheidungsfindung

Relevant wäre datenschutzrechtlich, wie eine automatisierte Entscheidung zu werden ist. Hier ist Artikel 22 Datenschutz-Grundverordnung einschlägig.

Sofern der Einwilligungsassistent von einem Dienstleister oder einem Vertragspartner eingesetzt wird, stellt sich die Frage, ob der Einwilligungsassistent nicht bereits als solches die Voraussetzungen des Artikels 22 Datenschutz-Grundverordnung erfüllen muss.

Gemäß Artikel 22 Absatz 1 Datenschutz-Grundverordnung hat die betroffene Person 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.

Dies gilt jedoch nicht gemäß Absatz 2, wenn die Entscheidung

- für den Abschluss oder die Erfüllung eines Vertrages zwischen der betroffenen Person und dem Verantwortlichen erforderlich ist,

- 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 enthalten, oder

- mit ausdrücklicher Einwilligung der betroffenen Person erfolgt.

Für einen Einwilligungsassistenten, der automatisiert Entscheidungen trifft (unter der Voraussetzung, dass nicht der Nutzer als alleiniger Entscheider angesehen wird und sofern keine entsprechenden gesetzlichen Regelungen in den Mitgliedstaaten vorhanden sind), bedeutet dies:

⇢ Es muss zuvor ein Vertrag für die „Anwendung des Einwilligungsassistenten an sich“ zwischen Nutzer und Verantwortlichen abgeschlossen werden, der klar regelt, welche Funktionen der Einwilligungsassistent erfüllen soll (so dass die automatisierte Entscheidungsfindung zur Vertragserfüllung erforderlich ist)

oder

⇢ Für die Nutzung des Einwilligungsassistenten ist eine ausdrückliche Einwilligung des Nutzers einzuholen.

Hier ist wiederum entscheidend, ob dies auf informierter Basis und in Kenntnis der Sachlage für eine genau umrissene Situation umsetzbar ist. Die Artikel-29-Datenschutzgruppe hat wie oben ausgeführt dargelegt, dass eine Einwilligung nicht alle rechtmäßigen Zwecke abdecken kann, sondern sich auf die Verarbeitung beziehen muss, die in Bezug auf den Zweck angemessen und erforderlich ist. Daher ist dies aus datenschutzrechtlicher Sicht besonders kritisch zu sehen.

Zu berücksichtigen ist zudem, wer Verantwortlicher der Einwilligungsassistenten ist und ob ein eigenständiger Dienst in Betracht kommt oder dies dezentral in der alleinigen Verantwortung des Nutzers verbleibt.[192]

Besondere Kategorien personenbezogener Daten gemäß Artikel 9 dürfen im Rahmen einer automatisierten Entscheidungsfindung im Übrigen nur bei ausdrücklicher Einwilligung des Betroffenen verarbeitet werden oder wenn es entsprechende Rechtvorschriften auf der Grundlage des Unionsrechts oder des Rechts der Mitgliedstaaten gibt.

Zu beachten ist allerdings, dass die Bildung von Profilen als solche keinem besonderen Schutz unterliegt, sondern allein an den Voraussetzungen des Artikel 6 Datenschutz-Grundverordnung zu messen ist.

Insgesamt bleibt aber bei Anwendbarkeit des Artikel 22 Datenschutz-Grundverordnung vorab die Frage offen, wie die Regelung auszulegen ist, dass eine betroffene Person das Recht hat, nicht einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden. Sofern der Nutzer weiterhin selbst die Möglichkeit hat, bei der Nutzung des Einwilligungsassistenten konkrete Vorgaben zu machen, könnte das Merkmal der „Ausschließlichkeit“ hier entfallen.

Die Informationspflichten sowie das Auskunftsrecht der betroffenen Person würden sich zudem im Falle einer automatisierten Entscheidung, einschließlich Profiling, gemäß Artikel 13, 15 ebenso auf die Logik und Tragweite einer derartigen Verarbeitung beziehen. Es besteht außerdem ein Recht auf einer Kopie der Daten, die Gegenstand der Verarbeitung sind (Artikel 15 Absatz 4).

Nach der Datenschutz-Grundverordnung entfällt zwar der Grundsatz der Direkterhebung. Dennoch obliegen dem Verantwortlichen Informationspflichten gemäß Artikel 14 Datenschutz-Grundverordnung, wenn Daten nicht bei der betroffenen Person erhoben werden. Daher bleibt es notwendig, die betroffenen Personen zu informieren, wenn auch nicht unbedingt bei Erhebung.

II. Datenschutzrecht und Zivilrecht

Ohne vertiefend hierauf eingehen zu können, sollen folgende Überlegungen zum Zivilrecht kurz aufgegriffen werden:

Eine Einwilligung muss aus datenschutzrechtlicher Sicht nicht für die Übermittlung von Daten für vertragsrelevante Zwecke eingeholt werden. Sie spielt aber insoweit eine Rolle, wenn der Einwilligungsassistent selbstständig Tätigkeiten übernimmt, etwa durch Sprachsteuerung ein Hotel oder Taxi bucht. Dieses erweiterte Konzept ist nicht von den in dieser Stellungnahme untersuchten technischen Lösungen erfasst, soll aber hier bereits kurz erwähnt werden, da große Anbieter (wie etwa Deutsche Telekom AG) solche Lösungen planen.

192 Siehe oben S. 21 und S. 55.

Wenn ein solcher Einwilligungsassistent den „Auftrag“ hat, ein Taxi zum Flughafen zu bestellen, muss sichergestellt sein, dass zivilrechtlich Handlungswille und Erklärungsbewusstsein bestehen.[193] Ohne einen entsprechenden Handlungswillen liegt keine Willenserklärung vor[194] und insgesamt ist entscheidend, auf wessen Willen die Entscheidung basiert.[195] Datenschutzrechtlich muss sichergestellt sein, dass die entsprechenden Daten verarbeitet bzw. übermittelt werden dürfen. Dies ist nur der Fall, wenn der Vertrag auch geschlossen wurde. In diesem Fall wird datenschutzrechtlich keine Einwilligung benötigt. Dementsprechend muss die betroffene Person vorher nochmals eine Rückmeldung erhalten, die sie für jeden Einzelfall bestätigen muss, und zwar bevor die Daten an mögliche Empfänger weitergegeben werden.

Es müsste darüber hinaus geklärt werden, wer das Angebot abgibt und wer den Antrag annimmt. Ein Hotel muss wissen, mit wem es einen Vertrag abschließen möchte, so dass es für einen Hotelbetreiber wichtig sein kann, die persönlichen Angaben im Vorhinein zu erhalten. Der Bundesgerichtshof hat hierzu entschieden, dass nicht nur Privatleute, sondern auch Unternehmen ihr Hausrecht grundsätzlich frei ausüben können. Eingeschränkt wird dieses Recht jedoch bei Vorliegen von sachlichen Gründen, etwa wenn aufgrund einer vertraglichen Abrede ein Erfüllungsanspruch erworben wurde.[196] Bei einem Massengeschäft Taxi sind die Angaben zur Person dagegen weniger wichtig bzw. werden im Alltag regelmäßig nicht erfragt.

Aus zivilrechtlicher Sicht werden bei einer automatisierten Entscheidungsfindung nicht nur Handlungswille und Erklärungsbewusstsein und der Zeitpunkt des Vertragsschlusses relevant sein, sondern ebenso die Frage, unter welchen Gesichtspunkten ein Mangel oder eine Pflichtverletzung erheblich ist. Dies erhält bei einer automatisierten Entscheidungsfindung insoweit Relevanz, wenn nur wenige Angaben etwa zur Kategorie gemacht werden oder beispielsweise eine blaue Corvette gekauft werden soll, wenn sie endlich gefunden wurde, aber „automatisiert“ eine schwarze gekauft wird.[197] Hier wird es auch zivilrechtlich auf die Granularität ankommen.[198]

Zivilrecht und Datenschutzrecht sind daher strikt zu trennen. Aus datenschutzrechtlicher Sicht ist keine Willenserklärung in Form einer Einwilligung zusätzlich notwendig, um vertragsrelevante Daten verarbeiten zu dürfen.

Bei der Gestaltung des Einwilligungsassistenten ist somit darauf zu achten, dass für den Nutzer nicht der Eindruck entsteht, er würde nun ebenso seine Einwilligung für vertragsrelevante Zwecke erteilen, gleichwohl muss der Nutzer transparent über diese Zwecke informiert werden.

193 *Siehe hierzu bereits oben S. 22 ff.*

194 *Siehe etwa Köhler, BGB, Allgemeiner Teil, 40. Auflage, München 2016, der auf den Handlungswillen als notwendiges Tatbestandsmerkmal einer Willenserklärung verweist und das Beispiel der Hypnose anführt; der Handlungswille fehle, wenn die äußerlich als Willenserklärung gewertete Handlung nicht gewollt war (§ 7 Rn. 4). Ebenso Rüthers/Stadler, Allgemeiner Teil des BGB, 17. Auflage, München 2011, § 17 Rn. 7: Handlungswille ist notwendige Voraussetzung für das Vorliegen einer Willenserklärung.*

195 *Köhler, BGB, Allgemeiner Teil, 40. Auflage, München 2016, § 6 Rn. 8 stellt klar, dass automatisierte Willenserklärungen echte Willenserklärungen sind, wenn die Datenverarbeitungsanlage keine autonomen Entscheidungen trifft, sondern nur logische Operationen aufgrund eines vorgegebenen Programms verwirklicht. Dahinter stehe der Wille des Anlagenbetreibers.*

196 *BGH Urteil vom 9. März 2012 -V ZR 115/11 ; http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&nr=59967&pos=0&anz=1*

197 *BGH NJW-RR 2010, 1289 ff., 1292 mit Abkehr von der Vorinstanz, die noch eine unerhebliche Pflichtverletzung gemäß § 323 Absatz 5 BGB bei dieser Farbabweichung angenommen hatte.*

198 *Aus datenschutzrechtlicher Sicht würde es auf diese Frage nur ankommen, wenn die Verwendung des Einwilligungsassistenten selbst der Einwilligung bedarf.*

Der Einwilligungsassistent müsste also insgesamt so konzipiert sein (inhaltlich und grafisch), dass dem Betroffenen im Einzelfall bewusst ist, eine Erklärungshandlung vorzunehmen.
Es müsste mindestens im Nachhinein nochmals die automatische Information über die Einwilligung im Einzelfall erfolgen. Allerdings ist damit ein im Vorfeld fehlender Handlungswille nicht ohne weiteres zu kompensieren. Um diesen Handlungswillen sicherzustellen, muss der betroffenen Person deutlich sein, dass eine Willenserklärung erfolgt. Aus zivilrechtlicher Hinsicht kann dies mit Schwierigkeiten behaftet sein, da gegebenenfalls immer unterstellt werden kann, dass bei einer automatisierten Entscheidung kein Handlungswille und damit keine Willenserklärung vorliegt. In diesem Fall müsste also zusätzlich diskutiert werden, wer (nach deutschem Recht) das Angebot gemäß § 145 BGB abgibt und wer dieses annimmt. Sofern man unterstellt, dass aus zivilrechtlicher Sicht kein verbindliches Angebot vorliegt, etwa da beim Buchen eines Taxis oder Hotels noch als essentialia negotii der Preis und/oder Empfänger noch nicht feststehen, müsste der Annehmende der Nutzer des Dienstes sein und der Dienstleister gibt das verbindliche Angebot ab (siehe Deutsche Telekom AG, die über Sprachsteuerung, die Möglichkeit per Assistent eröffnen möchten, etwa Hotels und Taxen selbstständig zu buchen).

G. Zusammenfassung der Anforderungen an den Einwilligungsassistenten

Die Entwickler der eingangs beschriebenen Systeme sollten berücksichtigen, dass die weitere technische Ausgestaltung des Systems und vor allem der geplante konkrete Einsatzzweck einen erheblichen Einfluss auf die Frage der rechtlichen Einstufung des Einwilligungsassistenten und ebenso der Verantwortlichkeit und Haftung nach sich zieht.

Es muss daher zukünftig geklärt werden, ob der Einwilligungsassistent als Teil der Datenverarbeitung einen eigenständigen (Online)Dienst darstellt. Vorstellbar wäre ebenso, dass er von einem weiteren Anbieter als eigenständige Dienstleistung eingesetzt wird. Der Einwilligungsassistent (als Software) könnte aber ebenso an Nutzer zum Selbstmanagement veräußert werden.

Aufgrund der noch nicht näher beschriebenen und veröffentlichten technischen Details und Funktionsweise können daher lediglich die im Folgenden dargestellten grundsätzlichen Anforderungen benannt, aber keine abschließende rechtliche Beurteilung vorgenommen werden:

- Eine eindeutig bestätigende Handlung gemäß Artikel 4 Nr. 11 Datenschutz-Grundverordnung wird durch den Einwilligungsassistenten erfüllt, wenn bereits im Voraus präzise, leicht zugänglich und verständlich sowie in klarer und einfacher Sprache ermöglicht wird, dass eine betroffene Person in unterschiedliche

- Verarbeitungszwecke

- Empfänger oder Kategorien von Empfängern

- personenbezogene Daten

einwilligen kann.

Es ist dabei auf die notwendige Granularität zu achten. Bei Standortdaten muss gesondert geprüft werden, wie genau die Standortbestimmung erfolgen muss.

Wenn dabei die betroffene Person entsprechend der Vorgaben der Artikel-29-Datenschutzgruppe leere Kästchen mit dem jeweilig gewünschten Verarbeitungszweck ankreuzen kann, würde sogar eine ausdrückliche Einwilligung vorliegen. Dies würde wiederum der Intention der ursprünglichen geplanten Datenschutz-Grundverordnung (Entwurf vom 25.01.2012) sowie der Vorgabe „Datenschutz durch Technikgestaltung“ gemäß Artikel 25 Datenschutz-Grundverordnung entsprechen. Die Erkenntnisse zu P3P (Platform for Privacy Preferences) können bei der Umsetzung berücksichtigt werden.

- Der Zweck muss eindeutig formuliert sein. Im Sinne einer datenschutzgerechten Auslegung sollte der Zweck ausdrücklich benannt werden, was mittels eines Einwilligungsassistenten gut realisiert werden kann. Der Kontext ist eingeschränkt und eng auszulegen. So wird die zweckgebundene Verarbeitung im Sinne von Artikel 5 Absatz 1b) Datenschutz-Grundverordnung realisiert.

  Pauschale Einwilligungen sind unwirksam. Daher muss bei „Interessensbekundungen“ eine dynamische Einwilligungsmöglichkeit gegeben sein, wie sie aktuell bei CoMaFeDS geplant ist.[199]

  Konzepte wie CoMaFeDS könnten gleichwohl bei Forschungszwecken unterstützend eingesetzt werden. Gemäß Erwägungsgrund 33 Datenschutz-Grundverordnung kann die betroffene Person ihre Einwilligung für bestimmte Bereiche wissenschaftlicher Forschung geben, d.h. ohne vollständige Angabe des Zwecks. Dies könnte ebenso entsprechend für die Empfänger (im Sinne von Datennehmern) gelten.

- Die automatisierte Übersetzung von Datenschutzhinweisen in eine Einwilligungserklärung (z. B. in der Form einer Liste, deren leere Felder der Nutzer aktivieren muss) muss im Einzelfall aus rechtlicher Sicht überprüfbar sein. Schwierigkeiten können sich etwa dann ergeben, wenn in den Datenschutzhinweisen etwa die Information über vertragsrelevante Zwecke enthalten ist und daraus automatisiert eine Einwilligungserklärung generiert wird. Für vertragliche Zwecke ist keine Einwilligung erforderlich, wohl aber eine transparente Information.

- Soll der Einwilligungsassistent zukünftig daher zur Unterstützung bei Vertragsabschlüssen eingesetzt werden, müssen Zivilrecht und Datenschutzrecht getrennt werden. Zivilrechtlich sind übereinstimmende Willenserklärungen für das Zustandekommen eines Vertrages erforderlich, als essentialia negotii eines Kaufvertrages umfasst dies außerdem die Festlegung von Gegenstand und Vertragspartner. Aus datenschutzrechtlicher Sicht dürfen Daten ohne Einwilligung verarbeitet werden, wenn dies für vertragliche Zwecke erforderlich ist. Dennoch muss transparent über die Datenverarbeitung (etwa Verarbeitung für vertragsrelevante Zwecke) informiert werden. Bei der Gestaltung des Einwilligungsassistenten ist daher insgesamt zu achten, dass diese Trennung für den Nutzer deutlich wird. Die Einwilligung beinhaltet aus datenschutzrechtlicher Sicht stets ein Widerrufsrecht.

- Insgesamt ist daher zu berücksichtigen, dass die Zulässigkeit der Datenverarbeitung aus datenschutzrechtlicher Sicht auf unterschiedlichen Rechtsgrundlagen beruhen kann. Wird eine Einwilligung eingeholt, muss dem Betroffenen auch das Widerspruchsrecht zustehen. Der Verantwortliche kann sich im Nachhinein nicht auf andere Legitimationsgrundlagen (etwa berechtigte Interessen) berufen.

199 Die rechtlichen Voraussetzungen einer solchen „dynamischen Einwilligung“ müssen gesondert geprüft werden.

- Systeme wie LETsmart bieten dem Nutzer ein Selbstmanagement an, so dass er jederzeit seine Einwilligung ändern, berichtigen und löschen kann. Damit können die Anforderungen an einen jederzeitigen Widerruf gemäß Artikel 7 Absatz 3 Datenschutz-Grundverordnung erfüllt werden. Probleme, die sich im Zusammenhang mit dem Recht auf Datenübertragbarkeit (Artikel 20 Datenschutz-Grundverordnung) ergeben könnten, wären in diesem Zusammenhang ebenso umgangen.[200]

- Die Richtigkeit der Daten (Artikel 5 Absatz 1d) Datenschutz-Grundverordnung) kann systemseitig erfüllt werden, wenn der Einwilligungsassistent in der Lage ist, alle Datenzugriffe zu verhindern, bei welchen Empfänger, Zweck und die konkreten personenbezogenen Daten nicht übereinstimmen. Die möglichen Empfänger erhalten den Zugriff auf die Datensätze der Nutzer ausschließlich unter der Bedingung, dass die richtige Kombination von legitimierten Empfängern und Verarbeitungszwecken vorliegt. Bei Abweichungen muss der Einwilligungsassistent zudem in der Lage sein, in dynamischer Form die Einwilligungserklärung des Nutzers einzuholen, was bei dem System CoMaFeDS geplant ist.[201]

- Im Rahmen der Gestaltung des Einwilligungsassistenten muss im besonderen Maße auf das Kopplungsverbot und die freie Bestimmung durch den Betroffenen geachtet werden. Der Düsseldorfer Kreis hat die Problematik vor allem bei kostenlosen Angeboten betont. Daher müssen die Gesamtumstände berücksichtigt werden, ob die betroffene Person tatsächlich vollständig überblicken kann, für welche Marketing- und/oder Scoringzwecke die persönlichen Daten verwendet werden. Diese Selbstbestimmtheit kann im Einzelfall schwierig zu ermitteln sein. Aber je mehr Zwecke miteinander verknüpft sind oder je mehr Datenempfänger involviert sind, desto wahrscheinlicher ist die Unübersichtlichkeit für die betroffene Person.

- Der Einwilligungsassistent sollte automatisiert sicherstellen, dass eine Einwilligung nicht zeitlich unbegrenzt erteilt wird, sondern entweder bei Wegfall des Verwendungszwecks Datenzugriffe automatisiert verhindert werden oder aber nach einer entsprechenden Dauer der Nutzer gefragt wird, ob er die Einwilligung aufrecht erhalten möchte.[202] In diesem Falle werden die Gebote der Speicherbegrenzung (Artikel 5 Absatz 1e Datenschutz-Grundverordnung) sowie der Datenminimierung (Artikel 5 Absatz 1c Datenschutz-Grundverordnung) erfüllt, da die betroffene Person selbst entscheidet, welche Daten über sie verarbeitet werden, indem die erteilte Einwilligungserklärung mit der Kategorie von Empfängern (im Sinne von Datennehmern) ihrem Zugriff unterliegt.

- Der für die Datenverarbeitung Verantwortliche muss die Einwilligung auf informierter Basis bereitstellen. Er muss also vor Erhebung der Daten die Information bereitstellen und er muss die Einwilligung nachweisen können. Zukünftig ist jedoch zu klären, ob bei einer elektronischen Einwilligung die Voraussetzungen des Telekommunikationsgesetzes und Telemediengesetzes in Bezug auf die Protokollierung und jederzeitige Abrufbarkeit weiterhin Geltung beanspruchen. Zu berücksichtigen ist, dass die Protokollierung eine Form des Nachweises darstellen kann, aber im Sinne einer europaweiten Vereinheitlichung gegebenenfalls auch andere Methoden in Frage kommen, was zu prüfen wäre. Für die Nachweispflicht werden zukünftig Verhaltensregeln maßgeblich sein.

200 Davon unberührt bleibt, dass der Empfänger der Daten bei Kopie und Speicherung der Nutzerdaten in seinem eigenen System weiterhin den datenschutzrechtlichen Anforderungen unterliegt.

201 Die rechtlichen Voraussetzungen einer solchen „dynamischen Einwilligung" müssen gesondert geprüft werden.

202 LETsmart plant, die Daten nach Wegfall des Verwendungszwecks automatisiert zu löschen.

- Zur Unterstützung einer transparenten Gestaltung der Auswahlmöglichkeiten (Zweck, Empfänger, Daten) und im Sinne einer informierten und unmissverständlichen Willensbekundung könnten bei einem Einwilligungsassistenten zusätzlich visuelle Elemente (Erwägungsgrund 58 Datenschutz-Grundverordnung) verwendet werden.

- Bei komplexer Datenverarbeitung mit unterschiedlichen Zwecken oder Empfängern könnte jedoch auch bei Verwendung eines Einwilligungsassistenten eine intransparente Darstellung vorliegen, die gemäß Artikel 5 Absatz 1 a Datenschutz-Grundverordnung gerade vermieden werden muss. Hier könnte geprüft werden, inwieweit der so genannte „One-Pager“ als transparente Zusammenfassung der erteilten Einwilligung unterstützend in Betracht kommen könnte.[203]

H. Fazit und Zusammenfassung der Handlungsempfehlungen

Entsprechend der in der Einführung dargestellten Zielsetzung wurde der Einwilligungsassistent auf grundsätzliche Vereinbarkeit mit rechtlichen Vorgaben überprüft, um entsprechende Anforderungen an seine Umsetzung zu formulieren. Hierfür mussten die Voraussetzungen an eine Einwilligung nach der Datenschutz-Grundverordnung unter Berücksichtigung der aktuellen Rechtspraxis ausgelegt werden. Daher musste gleichermaßen - auch im Hinblick auf entsprechende Empfehlungen - eine grundsätzliche Begutachtung erfolgen. Entscheidend ist stets, wie die Intention der Datenschutz-Grundverordnung, ein gleichmäßiges und hohes Datenschutzniveau für natürliche Personen durch ein gleichwertiges Schutzniveau für die Rechte und Freiheiten von natürlichen Personen bei der Verarbeitung ihrer personenbezogenen Daten in allen Mitgliedstaaten zu gewährleisten, zukünftig umgesetzt werden kann.

Gemäß den Ausführungen in dieser Stellungnahme ist daher insgesamt folgendes festzuhalten:

Im Sinne einer Vollharmonisierung und der Sicherstellung eines gleichwertigen Datenschutzniveaus in der Europäischen Union sollte insgesamt frühzeitig kontrolliert werden, ob eine unterschiedliche Auslegung des Wortlauts der Datenschutz-Grundverordnung durch die Mitgliedstaaten diesem Ziel entgegenstehen könnte und welche Vorgehensweise in der Praxis vertretbar ist. Ein Indikator für diese Prüfung kann die Umsetzung der Richtlinie 96/46/EG in den einzelnen Mitgliedstaaten darstellen.

Für eine einheitliche Anwendung des Datenschutzrechts in Europa sollten die Möglichkeiten in der Datenschutz-Grundverordnung wahrgenommen und entsprechende Verhaltensregeln und/oder Leitlinien erarbeitet werden. Festgestellt wurde dies anhand der Prüfung der Einwilligungsvoraussetzungen nach der Datenschutz-Grundverordnung. Dabei sollte die Sicherstellung eines einheitlichen Wettbewerbs mit berücksichtigt werden. Der Prozess nach Artikel 40 Datenschutz-Grundverordnung bezüglich der Erstellung europaweit geltender Verhaltensregel könnte in zeitlicher Hinsicht langwierig sein. So muss sich die Verhaltensregel auf Verarbeitungstätigkeiten in mehreren Mitgliedstaaten beziehen und die zuständige Aufsichtsbehörde muss diese dem Europäischen Datenschutzausschuss vorlegen, bevor die Kommission erklären kann, dass diese in der Union allgemeine Gültigkeit besitzen.

203 Siehe zum „One-Pager“ die Hinweise des Bundesministeriums der Justiz und für Verbraucherschutz unter http://www.bmjv.de/DE/Themen/FokusThemen/OnePager/OnePager_node.html.

Daher empfiehlt sich bereits zum jetzigen Zeitpunkt die Benennung und Prüfung von Fragestellungen, die für eine auch in praktischer Hinsicht notwendige Harmonisierung des Datenschutzrechts erforderlich sind.

⇢ Die deutschen Aufsichtsbehörden könnten bereits zum jetzigen Zeitpunkt
mit der Förderung der Ausarbeitung von Verhaltensregeln beginnen und außerdem klare Anforderungen im Hinblick auf die Gestaltung einer Einwilligungserklärung formulieren.[204] Hier kann sich darüber hinaus die Formulierung eines Negativkatalogs empfehlen.

⇢ Der Europäische Datenschutzausschuss könnte zukünftig
eine Leitlinie hinsichtlich der Einwilligungskriterien formulieren. Die Formulierung von Artikel 4 Nr. 11 Datenschutz-Grundverordnung in Verbindung mit Erwägungsgrund 32 Datenschutz-Grundverordnung schließt nicht eindeutig aus, dass sich weiterhin europaweit eine unterschiedliche Praxis entwickeln könnte. Unterschiedliche Auslegungsmöglichkeiten der Einwilligung zeigen sich bislang bei Anwendung der Richtlinie 2002/58/EG (in der Fassung von 2009/136/EG) durch die Mitgliedsländer. Hier ist insgesamt unklar, ob tatsächlich eine konkludente (aber nicht im Sinne einer stillschweigenden/schweigenden) Einwilligung durch transparente Information möglich ist oder nur die Einleitung von Vertragsverletzungsverfahren versäumt wurde. Daher ist die Bildung einer einheitlichen Rechtsauffassung wichtig. Denn nur dadurch können gleichwertige Sanktionen bei einer nicht ordnungsgemäßen Datenverarbeitung umgesetzt werden.

⇢ außerdem Leitlinien hinsichtlich der Bedingungen für Direktwerbung unter Beachtung der Überschneidungen zum Wettbewerbsrecht formulieren. Datenschutzrechtlich muss die betroffene Person die Tatsache der Verarbeitungstätigkeit und deren Zweck vernünftigerweise erwarten dürfen, wobei sich die Datenschutz-Grundverordnung ebenso auf die Einwilligung „in einem Kontext“ bezieht. Fraglich ist, ob dies in einem europaweiten Vergleich stets gleichbedeutend mit „ähnliche Dienstleistung“ zu verstehen ist, was in dieser Stellungnahme nicht näher geprüft werden konnte. Hier kann sich daher ein europaweit, einheitliches Verständnis unter Berücksichtigung der Frage empfehlen, inwieweit als Auslegungshilfen das Kartellrecht oder Markenrecht heranzuziehen sind. Die Einwilligung „in einem Kontext“, aber auch die Zweckänderung gemäß Artikel 6 Absatz 4 Datenschutz-Grundverordnung bedürfen insgesamt klarer Regelungen. Die bisherigen Ausführungen der Artikel-29-Datenschutzgruppe könnten für deren Ausgestaltung herangezogen werden.

⇢ die Ausarbeitung von einheitlichen, europaweiten Verhaltensregeln in den genannten Bereichen fördern, soweit diese aufgrund einer Verarbeitungstätigkeit in mehreren Mitgliedstaaten ausgearbeitet werden können.

⇢ Durch Initiative der Europäischen Kommission
könnte sich ein aktueller Vergleich der Übersetzungen der Datenschutz-Grundverordnung durch die einzelnen Mitgliedstaaten noch vor deren Inkrafttreten dahingehend empfehlen, inwieweit ein einheitliches, europaweites Verständnis über die Auslegung der Begriffe „explicit“, „specified“ und „provide with“ besteht.[205] Dabei sollte berücksichtigt werden, ob unterschiedliche Auslegungen Auswirkung auf die Betroffenenrechte im Sinne eines einheitlichen Schutzniveaus haben könnten.

204 *Siehe hierzu auch Düsseldorfer Kreis, „Orientierungshilfe zur datenschutzrechtlichen Einwilligungserklärung in Formularen“, März 2016.*

205 *Vgl. hierzu auch die Studie zur Umsetzung der Richtlinie 95/46/EG unter http://ec.europa.eu/justice/policies/privacy/docs/lawreport/consultation/technical-annex_en.pdf(„Analysis and impact study on the implementation of Directive EC 95/46 in Member States“) sowie Artikel-29-Datenschutzgruppe, „Opinion 03/2013 on purpose limitation“, WP 203 adopted on 2 April 2013.*

Bereits in der Vergangenheit wurde der Begriff „explicit“ von den Mitgliedstaaten im Hinblick auf die Zweckbestimmung unterschiedlich übersetzt.

⇢ Die deutsche Politik und Gesetzgebung
sollten in Bezug auf die Einwilligung die Verpflichtung zur Protokollierung und jederzeitige Abrufbarkeit prüfen. Die Protokollierung kann eine Form des Nachweises sein, aber zu prüfen wäre, ob es weitere Möglichkeiten gibt und welche Anforderungen dazu vorliegen sollten. In diesem Zusammenhang sollte gemäß Artikel 95 Datenschutz-Grundverordnung in Verbindung mit der Richtlinie 2002/58/EG auch klargestellt werden, was unter zusätzlichen Pflichten zu verstehen ist (z. B. „jederzeitige Abrufbarkeit“ und „Protokollierung“ oder in Bezug auf Standortdaten „ausdrücklich, gesondert und schriftlich). Darüber hinaus sollte darauf hingewirkt werden, auf europäischer Ebene einheitliche Verhaltensregeln auszuarbeiten, soweit dies aufgrund einer Verarbeitungstätigkeit in mehreren Mitgliedstaaten möglich ist.

⇢ könnten prüfen, inwieweit eine Erweiterung des Produkthaftungsgesetzes in Bezug auf die Sicherstellung des Persönlichkeitsschutzes in Betracht kommen kann. Kann sich auch hier im Laufe der Zeit eine Schmerzensgeldtabelle entsprechend der Verletzung bei Körperschäden herausbilden?

⇢ Wirtschaft und Wissenschaft
sollten bei neuen Technologien generische Datenschutz-Folgenabschätzungen gemeinsam entwickeln. Diese können gleichermaßen eine Grundlage für die konkreten Datenschutz-Folgenabschätzungen der Datenschutz-Grundverordnung darstellen.

⇢ Die Entwickler
müssen bei der Gestaltung des Einwilligungsassistenten, der im Rahmen eines zivilrechtlichen Vertragsabschlusses eingesetzt wird, darauf achten, dass für den Nutzer nicht der Eindruck entsteht, er würde nun ebenso seine datenschutzrechtliche Einwilligung für vertragsrelevante Zwecke erteilen. Aus datenschutzrechtlicher Sicht bedarf es keiner Einwilligung für Zwecke, die für die Vertragserfüllung erforderlich sind. Gleichwohl muss der Nutzer transparent über diese Zwecke informiert werden. Zivilrecht und Datenschutzrecht müssen getrennt werden und diese Trennung muss transparent sein.

⇢ sollten außerdem die Anregungen der Artikel-29-Dateschutzgruppe zur Ausgestaltung technischer Systeme zur „Einwilligung in Cookies“ in Ihre Überlegungen einbeziehen und prüfen, ob ihr Konzept entsprechend erweitert werden könnte – immer unter der Maßgabe, dass bei Third-Party-Cookies die vorherige Einwilligung erforderlich ist.

⇢ ihre Konzepte zudem dahingehend analysieren, ob eine Kombination mit bereits bestehenden Diensten und Funktionen, wie sie beispielsweise „MyData“ oder „DigiMe“ bieten, möglich und sinnvoll sein könnte.[206]

⇢ sich frühzeitig überlegen, ob ein dezentrales oder zentrales System in Betracht kommt:
Bei zentraler Datenspeicherung mit Zugriffsmöglichkeiten von unterschiedlichen Empfängern ist vor allem an die Sicherheit des „Wissensgraphen“ (CoMaFeDS) zu denken und die Frage entscheidend, wer Verantwortlicher dieses „Wissensgraphen“ ist und ob sowie in welcher Form diesbezüglich eine zusätzliche Einwilligung des Nutzers vorliegen muss. Für eine solche zentrale Plattform empfiehlt sich eine Zertifizierung, da ein Nutzer die technischen Voraussetzungen, technische Sicherheit und die Vorgehensweise einer Datenverarbeitung nicht überblicken kann.

206 Siehe Studie der Stiftung Datenschutz, Kapitel II. 2.

Gemäß dem aktuellen Entwicklungsstand enthält die Plattform selbst keine Datensätze, sondern nur das (verschlüsselte) Wissen, wo diese zu finden sind. Ein Nutzer muss jedoch die Gewissheit haben, dass die Verschlüsselung ausreichend, seine Anonymität gegenüber potenziellen Empfängern gewahrt ist und keine Verknüpfungsmöglichkeiten bestehen, insbesondere da diese Plattform großes Potenzial für Big Data-Anwendungen bietet.

Bei dezentraler Speicherung und der Verantwortung des Nutzers für das System bzw. Software stellt in gleichem Maße die Frage nach Sicherheit sowie Zertifizierung und der Verantwortung der Hersteller/Entwickler. Die Datenschutzaufsichtsbehörden könnten auch hier auf Erklärungen der Industrie hinwirken, dass diese als Hersteller ebenso als datenschutzrechtliche Ansprechpartner agieren (siehe gemeinsame Erklärung mit dem Verband der Automobilindustrie). Dies gilt unter der Maßgabe, dass Hersteller zwar angehalten sind, datenschutzgerechte Technik zu entwickeln, aber ohne konkrete rechtliche Verantwortlichkeit, da ungeklärt ist, inwieweit ein Hersteller als „Verantwortlicher“ im Sinne der Verordnung eingeordnet werden kann, wenn er Mittel der Verarbeitung bereitstellt.

sollten die Sicherheit der Datenverarbeitung aus technischer Sicht gesondert und besonders prüfen, vor allem unter Maßgabe, wer als Verantwortlicher des Systems einzustufen ist. Dies hängt auch von dem oben ausgeführten Verwendungszweck ab und von der Frage, ob es sich um einen eigenständigen Dienst handelt oder um Software, die der Verantwortung des Nutzers oder eines Dienstanbieters obliegt.

I. Zusatz zur rechtlichen Stellungnahme vom Dezember 2016

Prof. Dr. Anne Riechert, Stiftung Datenschutz / Frankfurt University of Applied Sciences
Stand: Januar 2017, begründet auf:

Proposal „Regulation on Privacy and Electronic Communications", (10.01.2017) – 2017/0003 (COD)

Allgemein

Der Vorschlag der EU-Kommission („Regulation on Privacy and Electronic Communications" – im Folgenden: „Vorschlag") beinhaltet Regelungen zum Schutz der Privatsphäre und der personenbezogenen Daten in der elektronischen Kommunikation und soll die Richtlinie 2002/58/EG ersetzen. Klarstellend wird darauf verwiesen, dass diese Richtlinie „lex specialis" zur Datenschutz-Grundverordnung darstellt (siehe 1.2). Dies entspricht insoweit der aktuellen Rechtslage im Hinblick auf das Verhältnis der Richtlinie 2002/58/EG zur Datenschutz-Richtlinie (95/46/EG). Unberührt bleiben gemäß dem Vorschlag die Regelungen der Richtlinie 2000/31/EG (siehe Artikel 2 Nr. 4). Darüber hinaus steht es den Mitgliedstaaten ebenfalls frei, Regelungen zur Vorratsdatenspeicherung zu erlassen (siehe 1.3 des Vorschlags)

In dem Vorschlag sind unter anderem die Ergebnisse einer öffentlichen Befragung (durch Beteiligung von Verbraucherorganisationen, Industrie und Behörden) umgesetzt. Außerdem wurden Workshops sowie eine Meinungsumfrage unter EU-Bürgern durchgeführt (siehe 3.2 des Vorschlags). Aufgrund letzterer wurde beispielsweise festgestellt, dass 78% der Befragten es sehr wichtig finden, dass ein Zugang zu den auf einem Computer, Smartphone oder Tablet gespeicherten persönlichen Informationen nur aufgrund ihrer Erlaubnis möglich ist, und dass 89% mit der vorgeschlagenen Möglichkeit einverstanden sind, aufgrund von Voreinstellungen im Browser das Teilen ihrer persönlichen Informationen zu verhindern.

Des Weiteren basiert der Vorschlag auf einer Folgenabschätzung unter Berücksichtigung von Effektivität und Wirtschaftlichkeit, wobei nach der Untersuchung von unterschiedlichen möglichen Maßnahmen die Option befürwortet wurde, die eine maßvolle bzw. gemäßigte Stärkung von Privatsphäre und Vereinfachung beinhaltet. Damit ist gemäß den Ausführungen in dem Vorschlag vor allem gemeint, die Vertraulichkeit der elektronischen Kommunikation durch geeignete technische Einstellungen zu verbessern sowie das Regelungsumfeld zu vereinfachen, indem der Handlungsspielraum für die Mitgliedstaaten verringert wird (siehe 3.4 des Vorschlags).

Cookies

In Bezug auf Cookies verweist der Vorschlag gemäß Erwägungsgrund 21 darauf, dass für erforderliche Cookies keine Einwilligung eingeholt werden muss (z. B. das Ausfüllen von Online-Formularen über mehrere Seiten, das Messen des Traffic der Webseite). In Erwägungsgrund 22 wird detailliert aufgeführt, dass technische Voreinstellungen in Bezug auf Tracking-Cookies für den Nutzer übersichtlicher sind als Anfragen hinsichtlich seiner Zustimmung, wobei in Erwägungsgrund 23 im Besonderen auf die damit verbundene Anforderung des Artikel 25 Datenschutz-Grundverordnung hingewiesen wird („Privacy by Design").

Die Umsetzung dieses Anspruch sollte danach durch unterschiedliche und für den Nutzer leicht erkennbare Privatsphäreeinstellungen erfolgen, die beispielsweise Funktionen wie „Cookies niemals akzeptieren" bis „Cookies immer akzeptieren" bieten, aber ebenso die Option „nur Erstanbieter Cookies akzeptieren" umfassen.

In Erwägungsgrund 24 und Artikel 9 Absatz 1 des Vorschlags wird sodann auf die Geltung der Einwilligungsvoraussetzungen gemäß Artikel 4 Nr. 11 sowie Artikel 7 Datenschutz-Grundverordnung verwiesen. Davon unberührt ist gemäß Artikel 9 Absatz 2 Datenschutz-Grundverordnung jedoch die Verpflichtung, dort wo es „technisch möglich und machbar ist", für die Zwecke von Artikel 8 Absatz 1b des Vorschlags (für Informationen, die im Endgerät des Nutzers gespeichert sind), die Einwilligung des Nutzers durch geeignete technische Einstellungen mittels einer Softwareapplikation einzuholen. Erwägungsgrund 24 regelt hierzu näher, dass im Falle von „Third-Party-Cookies" die Nutzer aktiv auswählen sollen, dass sie mit „Third-Party-Cookies" einverstanden sind und diese Einwilligung bestätigen sollen. Dies gilt unter der Maßgabe, dass sie die notwendigen Informationen erhalten haben, diese Auswahl treffen zu können.

Im Sinne der oben bereits genannten Option (=maßvolle bzw. gemäßigte Stärkung von Privatsphäre und Vereinfachung) bezieht sich der Vorschlag darauf, eine Dialogbox zwischen Nutzer und besuchten Webseiten einzurichten, die dem Nutzer die Ablehnung von „Third-Party-Cookies" ermöglicht (siehe 3.4 des Vorschlags). Gemäß den Ausführungen in dem Vorschlag könnten damit Cookie-Banner und Benachrichtigungen umgangen werden, was zur Vereinfachung, aber auch Kosteneinsparung führen würde. Klarstellend wird darauf verwiesen, dass Webseitenbetreiber jedoch nach wie vor das Recht haben, eine Einwilligung aufgrund einer individuellen Anfrage beim Endnutzer einzuholen (siehe 3.4 des Vorschlags).

Aus wirtschaftlicher Sicht wird auf eine geschätzte, aber nicht näher begründete Kosteneinsparung von 948.8 Million Euro verwiesen (siehe 3.4 des Vorschlags).

Als Verantwortliche für diese technische Umsetzung könnten Internet Browser, Drittanbieter (die das Tracking durchführen) und die Webseiten in Betracht kommen (siehe 3.4 des Vorschlags). Gemäß Artikel 10 in Verbindung mit Artikel 23 des Vorschlags müssen Anbieter von elektronischer Kommunikationssoftware die Möglichkeit bieten, „Third-Party-Cookies" zu verhindern und die Einwilligung der Nutzer einzuholen. Anderenfalls können Bußgelder bis zu 10.000.000 EURO, alternativ 2% des weltweiten Jahresumsatzes drohen.

Relevanz im Hinblick auf die rechtliche Stellungnahme zum Einwilligungsassistenten und Handlungsempfehlung

Insgesamt besteht die Intention des Vorschlags darin, eine Einwilligung durch Unterstützung von Software, im Besonderen durch Internet Browser, einzuholen. Internet Browser stellen aber nur eine Möglichkeit dar. In den Handlungsempfehlungen der rechtlichen Stellungnahme vom Dezember 2016 (siehe Studie) wurden die Entwickler bereits zur Prüfung aufgefordert, ob ihr Konzept ebenso auf Cookies erweitert werden könnte.

In Bezug auf Cookies stellen die Erwägungsgründe klar, dass eine Einwilligung durch eine bestätigende Handlung erteilt werden soll, beispielsweise dadurch, dass von den Nutzern verlangt wird, eine Einstellung „accept third party cookies“ aktiv auszuwählen (Erwägungsgrund 26). Daraus lässt sich die Absicht entnehmen, dass ausdrücklich (nicht konkludent) durch Auswahl und aktiver Bestätigung unterschiedlicher Optionen ein Dialog stattfinden soll. Aufgrund dessen, dass dies aber (nur) ein Ausführungsbeispiel darstellt und gemäß Artikel 9 Absatz 2 zudem der Vorbehalt der „technischen Möglichkeit und Machbarkeit“ enthalten ist sowie außerdem unter 3.4 darauf verwiesen wird, dass Webseitenbetreiber das Recht haben, eine Einwilligung aufgrund einer individuellen Anfrage beim Endnutzer einzuholen, kann sich eine weitere Klarstellung empfehlen. So könnten im Hinblick auf die „technische Machbarkeit“ klare Regelfälle definiert werden. Außerdem wäre eine Betonung dahingehend möglich, dass ausschließlich (und nicht nur beispielsweise) durch die aktive Auswahl des Nutzers (Checkbox) von unterschiedlichen Optionen eine Einwilligung zustande kommt, damit eine transparente Information unter Weiternutzung des Dienstes deutlich ausgeschlossen ist (siehe etwa Rechtspraxis auf der Webseite der unabhängigen Datenschutzaufsichtsbehörde (ICO) von Großbritannien – aufgeführt in der rechtlichen Stellungnahme zum Einwilligungsassistenten).

Hinsichtlich der Einwilligungsvoraussetzungen insgesamt verweist Artikel 9 Absatz 1 auf die Voraussetzungen der Datenschutz-Grundverordnung (Artikel 4 Nr. 11 und Artikel 7 Datenschutz-Grundverordnung), so dass auch hier auf die Ausführungen in der rechtlichen Stellungnahme verwiesen wird (siehe etwa die Problematik im Hinblick auf die konkludente Einwilligung oder der Auslegung der Begriffe „explicit“ und „specified“).

Die rechtliche Verantwortung wird aufgrund der Regelungen in Artikel 10 und 23 des Vorschlags ebenso auf den Softwareentwickler verlagert, was in der Datenschutz-Grundverordnung in einer solch namentlich benannten Formulierung nicht vorgesehen ist. In der Datenschutz-Grundverordnung ist zwar der Grundsatz „Datenschutz durch Technik“ gemäß Artikel 25 enthalten, aber im Vorschlag „Regulation on Privacy and Electronic Communications” wird ausdrücklich benannt, dass auch der Anbieter von Software zur Umsetzung verpflichtet ist und ihm Geldbußen auferlegt werden können. Im Hinblick auf die Datenschutz-Grundverordnung könnte daher der Begriff des Verantwortlichen gemäß Artikel 4 Nr. 7 präzisiert werden, inwieweit ein Softwareanbieter als „Verantwortlicher“ im Sinne der Verordnung eingeordnet werden kann, da er Mittel der Verarbeitung bereit stellt und daher mit entscheiden könnte. Insgesamt muss vermieden werden, dass ein Dienstanbieter sich auf die mangelnde Umsetzung oder Entwicklung der erforderlichen softwareseitig sicherzustellenden Einwilligungsvoraussetzungen eines Softwareanbieters beruft (siehe Artikel 9 Absatz 2 „technically possible and feasible“), da Browserlösungen unter Umständen Entwicklungszeit benötigen.

Klarstellend könnte daher geregelt werden, dass jeder Anbieter verpflichtet ist, eine ausdrückliche Einwilligung durch Bereitstellung von interaktiven Auswahlmöglichkeiten einzuholen. Damit wäre eine aktive Entscheidung der Nutzer sichergestellt, die nicht in der Weiternutzung des Dienstes (auch nicht durch transparente Information) bestehen kann. In diesem Zusammenhang sei ebenso darauf verwiesen, dass Konzepte wie P3P in der Vergangenheit vom Windows-Browser seit der Version Windows 10 nicht mehr unterstützt wurden. Externe Softwareentwickler und Browseranbieter müssen daher in Bezug auf „technische Machbarkeit“ eng zusammenarbeiten.

Darüber hinaus wäre als vertrauensbildende Maßnahme für die Nutzer an dieser Stelle zertifizierte Software hilfreich.
Empfehlenswert wäre bei einer Verlagerung des Datenschutzes auf die technische Seite außerdem, eine Bildungsoffensive zu starten. Es ist ganz entscheidend, dass Nutzer keine Vorbehalte oder Ressentiments gegenüber einem technischen Datenschutz haben, sich die Bedienung von vorneherein zutrauen und nachvollziehen können, aus welchem Grunde technische Maßnahmen wichtig sind. Hier geht es im Besonderen um die Nachvollziehbarkeit des Selbstdatenschutzes, da dadurch gleichermaßen ein verantwortungsvoller Umgang der Daten seitens des Nutzers erwartet wird. Im Hinblick auf „Big Data“ muss einem Nutzer bekannt sein, wo die Gefahren von Third-Party-Cookies liegen. Um überhaupt eine Entscheidung treffen zu können, darf ihm die Entscheidung, welche Arten von Cookies er akzeptiert, nicht aus Unwissenheit „egal sein“.

Daher ist sowohl die Schul- als auch Erwachsenenbildung über (technischen) Datenschutz sehr bedeutsam.

STIFTUNG DATENSCHUTZ

Stiftung Datenschutz
rechtsfähige Stiftung bürgerlichen Rechts
Karl-Rothe-Straße 10–14
04105 Leipzig
Deutschland

Telefon 0341 / 5861 555-0
mail@stiftungdatenschutz.org
www.stiftungdatenschutz.org