

DATENSCHUTZ- BERATER

» Ihr zuverlässiger Partner für Datenschutz und Datensicherheit

Chefredakteur: Dr. Carlo Piltz

Schriftleitung: Prof. Dr. Alexander Golland, Tilman Herbrich, Philipp Quiel, Laurenz Strassemeyer

Editorial

Tilman Herbrich

EuGH kippt Safe Harbor

Seite 185

Stichwort des Monats

Laurenz Strassemeyer

**Vorhang auf für das Trans-Atlantic Data Privacy Framework –
der nächste Akt ist eröffnet**

Seite 186

Datenschutz im Fokus

Alexander Jung und Peng Tao

Meldung nach Art. 33 DSGVO – Zulässigkeit der Rücknahme

Seite 192

Sebastian Laoutoumai

**Anforderungen an die Erhebung und Nutzung von Informationen
aus dem Liegenschaftskataster**

Seite 196

Anna Cardillo, Guido Hansch, Wolfgang Lehna und Heiko Markus Roth

Koordinierte Prüfung zu Stellung und Aufgaben von Datenschutzbeauftragten

Seite 200

Erdem Durmus und Nadya Kaplan

**Das Recht auf Datenübertragbarkeit – Anwendungsbeispiele jenseits
von Social Networks**

Seite 203

Dr. Marcus Sonnenberg

**Das neue Hinweisgeberschutzgesetz – Datenschutzbeauftragte als
fachkundige Meldestelle?**

Seite 207

Aktuelles aus den Aufsichtsbehörden

Dr. Carlo Piltz

Bußgeld-Zuständigkeit bei Verstößen gegen Cookie-Vorgaben des TTDSG

Seite 210

Rechtsprechung

Hendrik Seidel

**Der Personenbezug von Daten ist (weiterhin) relativ zu bestimmen –
das EuG erinnert an „Breyer“**

Seite 212

Celin Fischer

**EuG zum Begriff der personenbezogenen Daten: Schon anonymisierte
oder noch pseudonymisierte Daten?**

Seite 215

Dr. Dominik Sorber

**Kein Schadensersatz nach Art. 82 Abs. 1 DSGVO bei Verletzung der
Auskunftspflicht gem. Art. 15 DSGVO**

Seite 218

▪ Nachrichten Seite 188

Erdem Durmus und Nadya Kaplan

Das Recht auf Datenübertragbarkeit – Anwendungsbeispiele jenseits von Social Networks

Das mit der DSGVO eingeführte Recht auf Datenübertragbarkeit – auch Recht auf Datenportabilität genannt – stand bisher im Schatten der Betroffenenrechte. Angesichts von Diskussionen über Datenteilung und Datenstrategien ist es perspektivisch jedoch von hoher Bedeutung. Bisher nicht abschließend geklärt ist die Frage, wie sich dieses Recht in der Praxis umsetzen lässt. Zudem lässt der bisherige, auf Social Networks fokussierte Anwendungsbereich auf eine geringe Praktikabilität schließen. Dieser Beitrag befasst sich mit der Rechtslage und erörtert alternative Anwendungsbeispiele.

Sinn und Zweck

Sinn und Zweck des in Art. 20 DSGVO geregelten Betroffenenrechts ist es, Betroffenen mehr Kontrolle über ihre personenbezogenen Daten zu geben. Mithilfe dieses Rechts können Betroffene ihre, einem Verantwortlichen bereitgestellten Daten, entweder selbst erhalten und einem anderen Verantwortlichen übermitteln oder gem. Art. 20 Abs. 2 DSGVO vom ersten Verantwortlichen einem zweiten Verantwortlichen direkt übermitteln lassen. Die Hürde der erneuten Dateneingabe bei neuen Anbietern soll den Betroffenen genommen und die Möglichkeit, Anbieter zu wechseln, attraktiv gemacht werden. Es handelt sich insoweit auch um ein Verbraucherschutzrecht.

Voraussetzungen für die Anwendbarkeit

Der Anwendungsbereich des Rechts auf Datenübertragbarkeit ist eröffnet, sofern die personenbezogenen Daten auf Grundlage einer Einwilligung gem. Art. 6 Abs. 1 lit. a DSGVO oder eines Vertrags gem. Art. 6 Abs. 1 lit. b DSGVO bereitgestellt werden und die Verarbeitung mithilfe automatisierter Verfahren erfolgt, wobei diese Voraussetzungen kumulativ vorliegen müssen.

Bereitgestellte Daten

Art. 20 Abs. 1 DSGVO sieht vor, dass die betroffenen personenbezogenen Daten dem Verantwortlichen bereitgestellt werden. Bereitstellung ist hier im weitestmöglichen Sinne zu verstehen. Demnach schließt sie aktiv und wissentlich bereitgestellte Daten, aber auch durch Nutzung eines Dienstes oder Geräts bereitgestellte Daten ein. Insoweit ist der Begriff der Bereitstellung nach Art. 20 DSGVO mit dem des § 327 Abs. 3 BGB („Bezahlen mit Daten“-Paragraph) gleichzusetzen, welcher weder auf den Zeitpunkt der Bereitstellung, noch auf eine aktive Datenübermittlung des Betroffenen abstellt. Denkbar als Ausschlusskriterium ist einzig ein fehlender Personenbezug der bereitgestellten Daten (Analysedaten und algorithmische Ergebnisse ungeachtet – bei diesen handelt es sich um Ableitungen und Rückschlüsse aus den von der betroffenen Person bereitgestellten personenbezogenen Daten, die im Rahmen der Verarbeitung durch den Verantwortlichen erzeugt werden).

Einwilligung oder Vertrag

Die Verarbeitung der bereitgestellten personenbezogenen Daten muss auf einer Einwilligung oder einem Vertrag beruhen. Hier kommt das Ziel des Kontrollgewinns zum Tragen. So sind alternative Rechtsgrundlagen für die Anwendung von Art. 20 DSGVO explizit ausgeschlossen (ErwGr. 68 S. 4 zur DSGVO). Folgerichtig ist auch das vorvertragliche Verhältnis der Vertragsparteien von diesem Erlaubnistatbestand nicht umfasst.

Automatisiertes Verfahren

Zudem setzt die Vorschrift das Vorliegen automatisierter Verfahren bei der Verarbeitung voraus. Mangels Definition in der DSGVO bleibt unklar, wie der Begriff zu bestimmen ist. Ein Blick in die Vorgängerin der DSGVO, die RL 95/46/EG, schafft hier Abhilfe. Sie stellt auf den Einsatz von Datenverarbeitungsanlagen ab. Angesichts der geringen praktischen Relevanz nicht-automatisierter Verfahren kann die Bestimmung des Begriffs jedoch dahinstehen. Ausschlaggebend ist eine Maschinenlesbarkeit.

Format

Weiter spezifiziert die Vorschrift das Format, in welchem die Möglichkeit zum Erhalt der personenbezogenen Daten gegeben werden soll. So soll dieses nach Art. 20 Abs. 1 DSGVO strukturiert, gängig und maschinenlesbar sein.

Strukturiertheit als Anforderung ist insoweit nirgends sonst in der DSGVO vorhanden. Eine Definition sucht man vergeblich. Die Definition des „Dateisystems“ in Art. 4 Nr. 6 DSGVO, unter der jede strukturierte Dateisammlung zu verstehen sein kann, hilft an der Stelle nicht weiter. Einzig nahe liegt eine dem Begriff immanente Anordnung der personenbezogenen Daten in einer für den Betroffenen nachvollziehbaren Weise. Eine solche Auslegung entspräche auch dem Transparenzgrundsatz der DSGVO.

In Anbetracht des Ziels des Rechts auf Datenübertragbarkeit ist das Kriterium der Gängigkeit nur sinnvoll. Es wird insoweit auf marktübliche Formate, die wohl von der Mehrheit der Marktteilnehmer verwendet werden, abge-

stellt. Fraglich ist, ob sich hieraus möglicherweise das Erfordernis der Entwicklung von Standards ergibt. ErwGr. 68 S. 2 zur DSGVO spricht jedenfalls von einer Aufforderung an den Verantwortlichen, „interoperable Formate zu entwickeln, die die Datenübertragbarkeit ermöglichen“. Dass diese Anforderung einzig an marktbeherrschende Unternehmen gerichtet sein soll, ist nicht nachvollziehbar und die Erarbeitung von Standards bspw. durch Fachverbände mehr als empfehlenswert.

Letztlich sieht Art. 20 Abs. 1 DSGVO die Maschinenlesbarkeit vor. Was für automatisierte Verfahren in der Auslegung als Anhaltspunkt gilt, findet hier explizite Erwähnung. Folglich stellen automatisierte Formate grundsätzlich maschinenlesbare Formate dar. Gesetzliche Definitionen von Maschinenlesbarkeit finden sich zuhauf. Etabliert hat sich doch eine Orientierung an ErwGr. 21 der RL 2013/37/EU, welcher Maschinenlesbarkeit annimmt, wenn betreffende Dokumente „in einem Dateiformat vorliegen, das so strukturiert ist, dass Softwareanwendungen die konkreten Daten einfach identifizieren, erkennen und extrahieren können.“ Im Bereich der Textdateien ist hier bspw. „.txt/.odt“, aber auch das .rtf- Format nennenswert.

Nicht in Art. 20 DSGVO erwähnt ist die aus ErwGr. 68 zur DSGVO stammende, bereits angesprochene Anforderung der Interoperabilität. Sie bezeichnet die Fähigkeit von verschiedenen Systemen auf unterschiedlichen Ebenen miteinander zu kommunizieren, mithin Daten auszutauschen. Hinsichtlich der Verhinderung von Monopolstellungen ist Interoperabilität von nicht zu vernachlässigender Bedeutung. Auch die Annahme, Interoperabilität vereine alle übrigen Anforderungen an das Recht auf Datenübertragbarkeit als Überbegriff scheint durchaus sinnvoll. Ein interoperables Format schließt die Strukturiertheit, Gängigkeit und Maschinenlesbarkeit demnach ein und stellt im Ergebnis das gewünschte Format dar.

Recht auf Erhalt

Betroffene haben nach Art. 20 DSGVO das Recht, ihre personenbezogenen Daten selbst zu erhalten. Getreu dem Gedanken der informationellen Selbstbestimmung immaniert dem Recht auf Erhalt mithin die volle Kontrolle, auch was die eventuelle Portabilität an einen anderen Verantwortlichen betrifft. Das Recht auf Erhalt beinhaltet insofern einen Anspruch auf den Erhalt einer Kopie der Daten, wenngleich ein Löschanpruch hieraus jedenfalls nicht resultiert. Demnach sind Szenarien denkbar, in denen die betroffenen Daten bei Ausübung des Rechts auf Datenübertragbarkeit zeitgleich von mehreren Anbietern (weiter-)verarbeitet werden, bspw. wenn ihre Speicherung der handelsrechtlichen Verpflichtung zur Aufbewahrung dient.

Recht auf Übermittlung an einen anderen Verantwortlichen

Ferner haben Betroffene das Recht, diese Daten einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, dem die personenbezogenen Daten bereitgestellt wurden, zu übermitteln. Das Statut der Nichtbehinderung an dieser Stelle ist angesichts wettbewerbsrechtlicher Ziele, die Art. 20 DSGVO verfolgt, wenig überraschend. Insofern wurden die Aufsichtsbehörden in ErwGr. 137 zur DSGVO sogar mit dem Recht auf Erlass einer Maßnahme ausgestattet, „wenn eine erhebliche Behinderung der Durchsetzung des Rechts einer betroffenen Person droht“. Mangels Definition ist man gut beraten, von einer weiten Auslegung des Begriffs auszugehen, wenngleich es naheliegt, dass die Regelung in erster Linie auf technische Einschränkungen abzielt, welche die Datenübertragbarkeit umgehen und somit den Wettbewerb gefährden. So sind bspw. rechtliche Behinderungen nicht ausgeschlossen. Es wird wohl auf die vom Verantwortlichen eingesetzten Mittel und ihre Eignung zur Behinderung ankommen, wobei hierzwischen zu differenzieren ist. Auch Vorsätzlichkeit oder Fahrlässigkeit sollte hier in Betracht gezogen werden.

Anwendungsbeispiele aus der Praxis

Aus praktischer Sicht sind viele Fälle denkbar, in denen das Recht auf Datenübertragbarkeit Anwendung finden kann, während aus rechtshistorischer Sicht in erster Linie auf die Anwendbarkeit im Bereich Social Networks abgestellt wurde. Grundlegende Voraussetzung für die Anwendbarkeit ist, dass die normativen Tatbestandsmerkmale erfüllt werden. Darüber hinaus können vom Verantwortlichen allerdings auch weitere Kriterien, insbesondere auch die vorhandene technische und organisatorische Infrastruktur oder Praktikabilität herangezogen werden. Im Folgenden sollen zusätzliche Anwendungsbeispiele jenseits von Social Networks erörtert werden.

Filehosting-Dienste

In der heutigen Zeit kommt den Filehosting-Diensten, also Massenspeichern in Form von Cloud-Anwendungen, eine erhebliche Bedeutung zu. Viele namhafte Tech-Unternehmen bieten bereits ein Produkt zur „digitalen“ Speicherung und Verwaltung von Daten an. Filehosting-Dienste werden sowohl im privaten als auch im beruflichen Kontext genutzt. Das Unternehmen Statista schätzt die im Jahr 2025 voraussichtlich anfallende, digitale Datenmenge auf 181 Zettabytes ein (Statista, Volumen der jährlich generierten/replizierten digitalen Datenmenge weltweit in den Jahren 2012 und 2020 und Prognose für 2025). Ein beträchtlicher Teil dieser Daten wird seinen Weg in Cloud-Speicher finden.

Ebenso wie Social Networks standen auch Filehosting-Dienste im Fokus der EU-Kommission als mögliche

Adressaten des Rechts auf Datenübertragbarkeit. Die EU-Kommission stellte fest, dass auch Filehosting-Anbieter wenig Interesse an Interoperabilität und einheitlicher Normung, dafür aber größeres Interesse an einer marktbeherrschenden Stellung und starrer Kundenbindung hätten.

Damit Filehosting-Dienste eine direkte Übermittlung von Kundendaten an einen anderen Wettbewerber ermöglichen können, müssen sie insbesondere Interoperabilität gewährleisten. Das Europäische Institut für Telekommunikationsunternehmen (ETSI) hat hierfür an der Entwicklung einer neuen Industrienorm mitgewirkt, nämlich der ISO/IEC 19941. Diese spezifiziert die Arten von Interoperabilität und Portabilität im Cloud Computing, die Beziehung und die Wechselwirkungen zwischen diesen beiden Querschnittsaspekten des Cloud Computing sowie die gemeinsame Terminologie und die Konzepte, die zur Diskussion von Interoperabilität und Portabilität verwendet werden, insbesondere in Bezug auf Cloud-Dienste.

Filehosting-Diensten dürfte es in der Praxis schwerfallen, den Anwendungsbereich des Art. 20 DSGVO exakt zu bestimmen und einzuhalten. So könnte es für solche Anbieter problematisch werden, aus einem Benutzeraccount lediglich die Daten herauszufiltern, die als eindeutig personenbezogen gelten. Ein typisches Szenario ist das Backup eines Smartphone-Speichers mit Hunderten oder gar Tausenden von Bildern und Videos, ungeachtet der übrigen Daten, wie etwa Dokumente, Musik, Kontakte und App-Daten. Nicht all diese Daten sind per se personenbezogen oder erfüllen die normativen Voraussetzungen des Art. 20 DSGVO. Aus Praktikabilitätsgründen sollte ein Filehosting-Dienst allerdings alle Daten entweder dem Betroffenen zur Verfügung stellen oder an einen anderen Filehosting-Dienstleister direkt übermitteln. Zwar wären auf diese Weise auch nicht personenbezogene Daten betroffen, allerdings stünde eine aufwändige vorherige Filterung in keinem angemessenen Kosten-Nutzen-Verhältnis, zumal der Betroffene in den meisten Fällen an einem ganzheitlichen Umzug seiner Daten interessiert sein wird.

Personalwesen

Auch im Personalwesen sind Fälle denkbar, in denen das Recht auf Datenübertragbarkeit zur Anwendung kommt. Um die relevanten Sachverhalte abschließend zu erfassen, ist ein genauerer Blick in das Verzeichnis von Verarbeitungstätigkeiten empfohlen. Denn dort muss für jede Verarbeitungstätigkeit auch eine Rechtsgrundlage hinterlegt sein. Sofern eine Verarbeitung auf Grundlage einer Einwilligung oder eines Vertrags erfolgt und der Arbeitnehmer ihn betreffende personenbezogene Daten selbst bereitgestellt hat, ist der Anwendungsbereich des Art. 20 DSGVO eröffnet. Auch wenn die Einwilligung im Beschäftigungsverhältnis in Fachkreisen nunmehr seit Jahren als kritisch eingeordnet wird, dient sie für manche Verarbeitungstätig-

keiten dennoch als Rechtsgrundlage (z. B. Veröffentlichung von Mitarbeiterfotos, Erstellung von Geburtstagslisten, Eingabe von zusätzlichen Daten in die Personalverwaltungssoftware etc.).

Von praktischer Relevanz ist das Recht auf Datenübertragbarkeit bei Einsatz von Personalverwaltungssoftware. Personenbezogene Daten eines Arbeitnehmers, die in einer Personalverwaltungssoftware gespeichert sind, müssen auf Anfrage in einem strukturierten, gängigen, maschinenlesbaren und interoperablen Format diesem verfügbar gemacht werden, sofern die Voraussetzungen erfüllt sind. Diese Datensammlung würde zunächst Angaben zur Begründung des Beschäftigungsverhältnisses enthalten. Im Einzelnen wären dies der Lebenslauf (Ausbildung und berufliche Stationen), Qualifikationen (Bescheinigungen, Zeugnisse und Zertifikate) sowie das Anschreiben. Auch Angaben, die der Arbeitnehmer freiwillig macht, etwa ein hochgeladenes Portrait-Foto, müssten in einem entsprechenden Format herausgegeben werden. Demnach müssten sich Verantwortliche überlegen, wie sie die Daten im besten Fall verfügbar machen, sodass der Arbeitnehmer sie insbesondere auch im Falle eines Arbeitgeberwechsels nutzen kann. Idealerweise bietet sich hierfür eine Export-Möglichkeit an. Auf diese Weise könnten die Daten bspw. in einer Excel-Tabelle oder einem Word-Dokument zur Verfügung gestellt werden. Nicht geeignet ist etwa ein kopiergeschütztes PDF-Dokument, zumal dies den Betroffenen daran hindern würde, die Daten unkompliziert weiterzuverwenden.

Musik-Streaming-Dienste

Ein weiteres Anwendungsbeispiel sind Musik-Streaming-Dienste. Auch wenn diese Dienste in Nuancen Unterschiede aufweisen, sind sie im Wesentlichen gleich: Der Nutzer hat die Möglichkeit, Musiktitel, Alben und Playlists anderer Nutzer zu favorisieren bzw. diese lokal innerhalb der Anwendung offline verfügbar zu machen oder zu speichern, eigene Playlists zu erstellen und auf seine Suchhistorie zurückzugreifen. Die Gesamtheit der vom Nutzer zusammengestellten Titel wird häufig unter Oberbegriffen wie „Bibliothek“ oder „Sammlung“ zusammengefasst. Da diese Zusammenstellung individuell ist und Rückschlüsse auf die musikalischen Vorlieben des Nutzers ermöglicht, ist sie als personenbezogenes Datum einzuordnen.

Aus Nutzersicht wäre es sehr praktisch, die über Stunden, möglicherweise auch Tage hinweg mühselig zusammengestellte Bibliothek bei einem Anbieterwechsel „mitnehmen“ zu können. Insofern könnte hier der Wunsch bestehen, die mit dem Profil verbundenen Inhalte möglichst lückenlos vom initialen Musik-Streaming-Dienst an einen anderen Musik-Streaming-Dienst direkt übermitteln zu lassen. Dies setzt natürlich voraus, dass der Übermittlungsvorgang i. S. d. Art. 20 Abs. 2 DSGVO „technisch machbar ist“. Die

technische Machbarkeit wiederum beruht auf Gegenseitigkeit der beteiligten Verantwortlichen, zumal der Erfolg der Übermittlung nicht lediglich von der sendenden Partei, sondern auch der empfangenden Partei abhängt. Die Parteien müssen beide Interoperabilität aufweisen, was durch entsprechende Schnittstellen gewährleistet werden kann. Weiterhin spielt es eine Rolle, inwieweit das Angebot des neuen Dienstes mit dem des alten Dienstes kompatibel ist. Sollten (einzelne) Musik-Titel beim neuen Dienst nicht verfügbar sein (z. B. aufgrund von fehlenden Lizenzen), sind diese vom Portabilitätsanspruch ausgenommen.

Ebenfalls nicht umfasst sind Inhalte, die auf Basis des Konsumverhaltens und somit der bereitgestellten Daten des Betroffenen erzeugt werden. Einige Musik-Streaming-Dienste analysieren den Musikgeschmack des Nutzers und schlagen auf Basis dessen ähnliche Musik-Titel, Alben oder Playlists vor. Hierbei handelt es sich um „abgeleitete Daten“. Die Art. 29-Datenschutzgruppe ist der Ansicht, dass sich das Recht auf Datenübertragbarkeit nicht auf solche Daten beziehen sollte (Art. 29-Datenschutzgruppe, Leitlinien zum Recht auf Datenübertragbarkeit, WP 242 rev.01, S. 11 f.).

In manchen Fällen besteht auch die Möglichkeit, zusammen mit anderen Nutzern gemeinsame Playlists zu erstellen. Deren Profilinformatoren sind in diesem Fall unmittelbar mit den zu portierenden Daten verknüpft. An dieser Stelle erscheint es nur realistisch, dass solche Playlists ohne Referenzen zu etwaigen anderen Nutzern verfügbar gemacht oder an einen anderen Anbieter direkt übermittelt werden, sodass ihre Rechte und Freiheiten gem. Art. 20 Abs. 4 DSGVO nicht beeinträchtigt werden.

Online-Marktplätze

Bei der Nutzung von Online-Marktplätzen stellen Nutzer ebenfalls umfangreich personenbezogene Daten bereit. Neben Profilinformatoren, Stamm- und Kontaktdaten sind hier zusätzlich Kaufinteressen, Suchaufträge oder die Transaktionshistorie betroffen. Des Weiteren werden Versand- und Rechnungsadressen sowie Bezahldienste spezifiziert. Eine mögliche direkte Übermittlung dieser Informationen an einen anderen Anbieter würde auf Seiten des Betroffenen einen großen Aufwand sparen.

Der Anspruch auf Datenübertragbarkeit darf allerdings nicht so weit gehen, dass Prozesse und (Sicherheits-)Vorkehrungen bei einem Verantwortlichen unterlaufen werden. Sollte der neue Verantwortliche, an den die personenbezogenen Daten des Betroffenen vom ursprünglichen Verantwortlichen direkt übermittelt werden, etwa Maßnahmen zur Verifikation der Identität oder des Bezahlvorgangs vorsehen, so sind diese einzuhalten. Insoweit geht der Portierungsanspruch nicht automatisch mit einem Recht auf Begründung eines Vertrags einher. Diesem An-

spruch können berechtigte Interessen eines Verantwortlichen entgegenstehen. Vielmehr soll für den Betroffenen eine Möglichkeit geschaffen werden, seine personenbezogenen Daten auf einfache Weise zu kontrollieren und von einem Punkt an einen anderen zu transferieren.

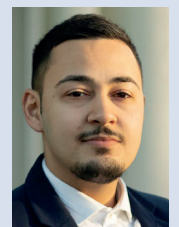
Fazit

Das Recht auf Datenübertragbarkeit ist ein erstmalig mit Anwendbarkeit der DSGVO eingeführtes Betroffenenrecht, das die informationelle Selbstbestimmung des Betroffenen stärkt. Aufgrund der Intention des europäischen Gesetzgebers, marktbeherrschende Strukturen von Unternehmen mithilfe dieses Rechts zu lockern und kleineren Unternehmen eine bessere Stellung im Wettbewerb zu ermöglichen, lässt es sich nicht eindeutig als datenschutzrechtliches Betroffenenrecht klassifizieren.

Nach fünf Jahren Anwendbarkeit der DSGVO ist festzustellen, dass das Recht auf Datenübertragbarkeit keine übergeordnete praktische Relevanz hat, wenngleich darin ein hohes Potenzial zu erkennen ist. Gerade im Kontext von Online-Anwendungen, in denen individuelle Benutzeraccounts erstellt und verschiedene Daten bereitgestellt werden können, kann das Recht auf Datenübertragbarkeit in Anspruch genommen werden.

Damit das Recht reibungslos zur Anwendung kommen kann, müssen Unternehmen und Branchenverbände an interoperablen Standards und Schnittstellen arbeiten. Es ist allerdings nachvollziehbar, dass marktbeherrschende Unternehmen wenig daran interessiert sind, eine einfache Möglichkeit zu schaffen, ihren Kunden, Nutzern oder Mitgliedern einen „Ausweg“ aus ihrem Dienst zu bieten. Insofern wird der Lock-In-Effekt in den meisten Fällen bestehen bleiben. Um über dieses Mittel mehr Einfluss auf den Wettbewerb zu nehmen, muss das Betroffenenrecht viel häufiger in Anspruch genommen werden. Gerade kleinere Unternehmen sollten sich deshalb für eine intensivere Aufklärungsarbeit bei ihren Zielgruppen stark machen.

Autoren: Erdem Durmus (LL.M.), CIPP/E ist Praktiker und externer Datenschutzbeauftragter bei der NOTOS Xperts GmbH in Darmstadt.



Nadya Kaplan ist Data Protection Expert bei Oriflame Cosmetics Sweden am Standort Schaffhausen.

