www.jusletter.ch

Lukas Bühlmann / Hatun Metin

Datenschutz im E-Commerce

Die Bearbeitung von personenbezogenen Daten ist nach der DSGVO nur zulässig, sofern sie sich auf einen Erlaubnistatbestand stützten kann. Bereits zu diesem grundlegenden Punkt bestehen gerade im Kontext des Online-Vertriebs zahlreiche offene Fragen. Die Autoren analysieren einige davon.

Beitragsart: Beiträge
Rechtsgebiete: Handelsrecht; Datenschutz

Zitiervorschlag: Lukas Bühlmann / Hatun Metin, Datenschutz im E-Commerce, in: Jusletter 15. Oktober 2018

ISSN 1424-7410, https://jusletter.weblaw.ch, Weblaw AG, info@weblaw.ch, T +41 31 380 57 77

Inhaltsübersicht

I. Einleitung und Übersicht

1. Einleitung

[Rz 1] Das Datenschutzrecht in Europa erfährt derzeit grundlegende Veränderungen. Seit dem 25. Mai 2018 ist die neue sog. Datenschutz-Grundverordnung (DSGVO)[1] in allen EU-Mitgliedstaaten direkt anwendbar.[2] Auch in der Schweiz ist eine Totalrevision des Datenschutzgesetzes im Gange. Welche konkreten Änderungen die Revision des schweizerischen Datenschutzrechts mit sich bringen wird und wann diese gelten werden, ist aktuell noch unklar. Feststeht immerhin, dass sich der Schweizer Gesetzgeber zu einem grossen Teil am EU-Vorbild orientieren wird.[3] Die Neuerungen werden branchenübergreifend alle Unternehmen und Organisationen sowie na-

1 Verordnung (EU) 2016/679 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; DSGVO).

2 Die DSGVO ist bereits am 24. Mai 2016 in Kraft getreten, wurde aber aufgrund ihrer zweijährigen Übergangsfrist erst per 25. Mai 2018 verbindlich, vgl. Art. 99 Abs. 2 DSGVO.

3 Medienmitteilung des Bundesrats vom 15. September 2017 (zit. Medienmitteilung-Bundesrat) betreffend die Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017 (BBl 2017 6941 ff.) (zit. Botschaft). Zu beachten ist, dass trotz Anlehnung an die DSGVO einige Unterschiede zu erwarten sind, so enthält der Entwurf zum Datenschutzgesetz bspw. Strafbestimmungen während die DSGVO verwaltungsrechtliche Sanktionen vorsieht, vgl. Mattig Cornelia/Zuber Simon, Datenschutz im Unternehmen, Expert Focus (EF) 9/18 S. 704 ff., hier S. 707 (zit. Mattig/Zuber).

hezu sämtliche Geschäftsprozesse betreffen. Gerade der Online-Handel ist aufgrund der grossen Bedeutung der Nutzung und Auswertung von (Kunden-)Daten besonders stark von den neuen Regelungen betroffen und steht somit vor einer grossen Herausforderung.

2. Übersicht

[Rz 2] Im Folgenden sollen einige der für den Online-Handel typischen Datenbearbeitungen dargestellt werden. Dabei bietet es sich an, den Kaufvorgang in einem Online-Shop Schritt für Schritt aus datenschutzrechtlicher Sicht zu beleuchten und zu beurteilen. Der Online-Vertrieb von Produkten setzt in aller Regel die Nutzung eines eigentlichen Online-Shops voraus (obschon andere digitale Verkaufskanäle durchaus denkbar sind[4]). Die vorliegende Darstellung bezieht sich folglich auf ausgewählte Aspekte in einem Online-Shop und kann im Übrigen nicht jede einzelne Datenbearbeitung abdecken.

[Rz 3] Während sich der erste Teil den Datenbearbeitungen annimmt, die bereits anlässlich des Besuchs des Nutzers auf einer Webseite und einem Webshop anfallen (Ziffer III), konzentrieren sich die darauffolgenden Ausführungen auf einige im Rahmen der Einkaufshandlungen anfallenden Datenschutzaspekte (Ziffer IV). Zuletzt widmet sich die vorliegende Publikation den Datenbearbeitungen, die typischerweise im Anschluss an den Einkauf anfallen und mit dem Vertrieb des Produktes im engeren Sinne nichts mehr zu tun haben – mit diesem aber in enger Verbindung stehen (Ziffer V). Vorab sollen jedoch die datenschutzrechtlichen Grundlagen dargestellt und insbesondere aufgezeigt werden, welches (Datenschutz-)Recht beim Betrieb eines Online-Shops überhaupt beachtet werden muss (Ziffer II).

II. Datenschutzrechtliche Grundprinzipien

[Rz 4] Je nach Ausgestaltung und Ausrichtung eines Online-Shops können unterschiedliche nationale und/oder europäische Gesetzesbestimmungen zur Anwendung kommen.

1. Anwendung schweizerischen Datenschutzrechts

[Rz 5] Weder die anstehende Totalrevision des schweizerischen Datenschutzgesetzes noch das aktuelle Datenschutzgesetz (DSG[5]) äussern sich ausdrücklich zum räumlichen Geltungsbereich.[6] In Lehre und Rechtsprechung ist aber anerkannt, dass im Allgemeinen das Auswirkungsprinzip gilt.[7] Gemäss dem Auswirkungsprinzip findet das Schweizer Datenschutzrecht nicht nur auf Sachverhalte Anwendung, die sich in der Schweiz abspielen, sondern auch auf internationale,

4 So z.B. den sog. Social Commerce, bei dem Produkte über die Sozialen Medien vertrieben werden.

5 Bundesgesetz über den Datenschutz vom 19. Juni 1992 (DSG; SR 235.1).

6 Vgl. statt vieler Belser Eva Maria/Epiney Astrid/Waldmann Bernhard, Datenschutzrecht, Grundlagen und öffentliches Recht, 2011, § 7 N 59 (zit. Belser/Epiney/Waldmann); Botschaft (Fn. 3), S. 7017.

7 Soweit es sich allerdings um Vorschriften mit öffentlich-rechtlichem Charakter handelt, kommt das Territorialitätsprinzip zum Tragen, vgl. Belser/Epiney/Waldmann (Fn. 6), § 7 N 59-60.

welche Auswirkungen in der Schweiz entfalten (sog. extraterritoriale Wirkung).[8] Wirkt sich ein Online-Shop folglich in der Schweiz aus oder richtet sich ein Online-Shop an Schweizer Abnehmer, sind die hiesigen Gesetze einschlägig. Im Zentrum des formellen[9] Datenschutzrechts der Schweiz steht hierbei neben dem eidgenössischen DSG auch dessen zugehörige Verordnung (VDSG[10]).[11]

[Rz 6] Von einer reinen Binnenausrichtung und somit der Anwendbarkeit schweizerischen Rechts kann allerdings nur dann die Rede sein, wenn sich ein Online-Shop durch seine entsprechende Ausgestaltung und Kommunikation nur an Schweizer Endkonsumenten richtet. Dies kann unter anderem dadurch zum Ausdruck kommen, dass beispielsweise die Preise ausschliesslich in Schweizer Franken angegeben werden, die Auslieferung der bestellten Produkte nur an Adressen in der Schweiz ermöglicht wird oder sich die Sprachauswahl auf der Webseite auf schweizerische Landessprachen beschränkt.[12]

[Rz 7] Obschon solche Anhaltspunkte eine schweizerische Binnenausrichtung unterstreichen, kann hingegen nicht im Sinne eines Umkehrschlusses gefolgert werden, es würde eine internationale Ausrichtung eines Online-Shops bereits vorliegen, wenn von diesen Anhaltspunkten punktuell abgewichen wurde. So vermag beispielsweise die Ausgestaltung der Webseite in englischer Sprache für sich alleine noch keine Ausrichtung ins Ausland begründen. Ferner ist zu beachten, dass trotz Vorliegens einer reinen Binnenausrichtung in die Schweiz die Anwendbarkeit europäischen Rechts nicht von vornherein ausgeschlossen werden darf. Ist ein Schweizer Online-Shop Teil einer europäischen Unternehmensgruppe und macht es als solches die Schweizer Daten auf europäischer Gruppenebene zugänglich, so finden die europäischen Bestimmungen dennoch Anwendung (zur Geltung europäischen Datenschutzrechts, vgl. sogleich Rz. 8 ff.). Die Frage der aktiven Ausrichtung eines Online-Shops ist daher immer anhand einer Gesamtbetrachtung verschiedener Kriterien zu beurteilen. In der Rechtsprechung europäischer Gerichte zeichnet sich jedoch die Tendenz ab, das Vorliegen einer aktiven Kundenansprache lokaler Konsumenten durch ein ausländisches Online-Angebot immer schneller zu bejahen.[13] Immerhin wird im Rahmen dieser Entwicklung auch deutlich, dass die Anwendbarkeit europäischen Rechts durch den Ausschluss der Belieferung von Kunden in bestimmten Ländern vermieden werden kann.[14]

---

8 Bühlmann Lukas/Reinle Michael, Extraterritoriale Wirkung der DSGVO, digma 2017, S. 8 ff., hier S. 10 (zit. Bühlmann/Reinle); Botschaft (Fn. 3), S. 7017.

9 Als formelles oder allgemeines Datenschutzrecht wird dasjenige Recht bezeichnet, welches die verfassungsrechtlichen Grundsätze des staatlichen Handels für das Bearbeiten von Daten konkretisiert. Hiervon zu unterscheiden ist das materielle oder auch bereichsspezifische Datenschutzrecht, vgl. zur Abgrenzung ausführlich Belser/Epiney/Waldmann (Fn. 6) § 7 N 12 i.V.m. N 15.

10 Verordnung zum Bundesgesetz über den Datenschutz vom 14. Juni 1993 (VDSG; SR. 235.11).

11 Weitere Bestimmungen finden sich in den Sachgesetzen, wie z.B. im Fernmeldegesetz vom 30. April 1997 (FMG; SR 784.10), vgl. insb. Art. 45 lit. c FMG oder im Asylgesetz vom 26. Juni 1998 (AsylG; SR 142.31), vgl. insb. Art. 86 ff. AsylG.

12 Vgl. insb. Urteil des europäischen Gerichtshofs (EuGH) C-585/08 vom 7. Dezember 2010, das die verschiedenen Kriterien zur Bestimmung der allfälligen Ausrichtung aufzählt.

13 So nahm der europäische Gerichtshof (EuGH) denn auch bereits vor der Einführung der DSGVO (und somit des Marktortprinzips im Datenschutzrecht) in seinem Urteil C-131/12 vom 13. Mai 2014 Bezug auf das Marktortprinzip; vgl. des Weiteren Urteil C-585/08 vom 7. Dezember 2010 sowie Lüttringhaus Jan, Das internationale Datenprivatrecht: Baustein des Wirtschaftskollisionsrecht des 21. Jahrhunderts, Zeitschrift für Vergleichende Rechtswissenschaft (ZVglRWiss 2018), S. 50 ff., hier S. 62–64 (zit. Lüttringhaus).

14 Vgl. Fn. 12.

2. Anwendung europäischen Datenschutzrechts

[Rz 8] Wie im Nachfolgenden aufgezeigt wird, ist die räumliche Ausrichtung eines Schweizer Online-Shops auch im europäischen Kontext und für die Anwendung europäischen Datenschutzrechts von zentraler Bedeutung.

a. Schweizer Online-Shops ohne Niederlassung in der EU (Marktortprinzip)

[Rz 9] Die europäische DSGVO beansprucht eine weit über das Hoheitsgebiet der EU-Mitgliedstaaten gehende Geltung und wird in Bezug auf die Definition ihres räumlichen Anwendungsbereiches gemäss Art. 3 DSGVO von zwei Grundprinzipen beherrscht: dem Marktort- und dem Niederlassungsprinzip (vgl. zum Niederlassungsprinzip sogleich Rz. 13).[15] Das Marktortprinzip ist vor allem relevant für Schweizer Online-Shops, die über keine Niederlassung in der EU verfügen.

[Rz 10] Kennzeichnend für das Marktortprinzip ist, dass danach das Recht desjenigen Ortes anwendbar ist, an dem aktiv in das Marktgeschehen eingegriffen und auf die Marktgegenseite eingewirkt wird.[16] Der schweizerische oder aussereuropäische Betreiber eines Online-Shops untersteht somit bereits der DSGVO, wenn er Waren oder Dienstleistungen an Unionspersonen anbietet, wobei es sich hierbei um natürliche Personen mit Wohnsitz in der EU handelt.[17] Ein Angebot im Sinne der DSGVO liegt allerdings erst vor, wenn ein *offensichtlich* beabsichtigtes Angebot an Kunden in der EU abgegeben wird.[18] Es ist unerheblich, ob es sich um ein entgeltliches oder unentgeltliches Angebot handelt.[19] Anhaltspunkte für ein offensichtlich beabsichtigtes Angebot sind – wie bereits erwähnt – die Verwendung einer Sprache oder Währung, die in einem oder mehreren Mitgliedstaaten gebräuchlich ist, in Verbindung mit der Möglichkeit, Waren in dieser Sprache zu bestellen.[20] Zu beachten ist, dass auch im Kontext der extraterritorialen Anwendbarkeit der DSGVO die blosse Zugänglichkeit einer Webseite oder Kontaktmöglichkeit durch Unionspersonen noch keine ausreichenden Anhaltspunkte darstellen.[21]

[Rz 11] Das Marktortprinzip hat allerdings zur Folge, dass bereits die blosse Beobachtung des Verhaltens von Unionspersonen zur Anwendung der DSGVO führt, soweit das Verhalten der betroffenen Personen in der Union erfolgt.[22] Diese erstaunlich weitgehend gefasste Bestimmung zielt auf Beobachtungen im Rahmen von Werbeaktivitäten ab und erfasst insbesondere jede Form von

---

15 Vgl. statt vieler Klar Manuel, in: Kühling/Buchner (Hrsg.), Datenschutz-Grundverordnung, Kommentar, 1. Aufl. 2017, Art. 3 N 2–3 (zit. DSGVO 2017-Autor).

16 DSGVO 2017-Klar (Fn.15), Art. 3 N 9.

17 Vgl. Art. 3 Abs. 2 lit. a DSGVO. Der verschiedentlich im Rahmen der Beratung angetroffenen Auffassung, für die Anwendbarkeit gemäss Art. 3 Abs. 2 lit. a DSGVO sei zudem erforderlich, dass sich die entsprechenden Personen im Moment der relevanten Datenbearbeitungen physisch in der EU befinden, kann (offensichtlich) nicht gefolgt werden. Datenbearbeitungen erfolgen selten über einen beschränkten, überblickbaren Zeitraum. Es wäre für einen Datenbearbeiter gar nicht möglich abzuschätzen, ob die DSGVO auf seine Datenbearbeitungen anwendbar wäre, a.M. Lüttringhaus (Fn. 13), S. 62.

18 Vgl. Erwägungsgrund 23 DSGVO.

19 Art. 3 Abs. 2 lit. a *in fine* DSGVO.

20 Vgl. Erwägungsgrund 23 DSGVO. Insofern kann auf die durch die Rechtsprechung im Rahmen der Anwendbarkeit verbraucherrechtlicher Bestimmungen entwickelten Kriterien zur Feststellung einer aktiven Ausrichtung abgestützt werden. Statt vieler vgl. Urteile des europäischen Gerichtshofs (EuGH) C-585/08 vom 7. Dezember 2010 sowie C-297/14 vom 23. Dezember 2015.

21 Vgl. Erwägungsgrund 23 DSGVO.

22 Art. 3 Abs. 2 lit. b DSGVO; Erwägungsgrund 24 DSGVO.

Webtracking-Technologien (z.B. durch Cookies oder Social Media Plug-Ins), die bei Online-Shops regelmässig eingesetzt werden (vgl. hierzu Rz. 28). Es ist zu hoffen, dass die Praxis von Behörden und Gerichten bald eine (einschränkende) Auslegung dieser Bestimmung bestätigen wird. Ansonsten wäre jedes weltweit zugängliche Online-Angebot unter Einsatz von Webtracking-Technologien vom Anwendungsbereich der DSGVO erfasst.

[Rz 12] Ein weiterer Umstand, der dazu führen *kann*, dass Schweizer Unternehmen ohne Niederlassung in der EU der DSGVO unterstehen, sind die sog. Auftragsdatenverarbeitungsverhältnisse (vgl. Art. 28 DSGVO). Ein solches Verhältnis liegt vor, wenn ein schweizerisches Unternehmen die eigenen Daten durch ein europäisches Unternehmen verarbeiten lässt oder umgekehrt, ein schweizerisches Unternehmen für einen europäischen Datenverantwortlichen dessen Daten in der Schweiz verarbeitet. Auftragsdatenbearbeitungsverhältnisse kommen in nahezu jedem Unternehmen vor (sei es im Zusammenhang mit der Nutzung eines externen Rechenzentrums, der Nutzung eines Cloud-Speichers, der Wartung von IT-Systemen durch technische Dienstleister etc.), wobei jeweils im Einzelfall zu beurteilen ist, ob die DSGVO anwendbar ist.[23]

b. Schweizer Online-Shops mit Niederlassung in der EU (Niederlassungsprinzip)

[Rz 13] Vollständigkeitshalber ist darauf hinzuweisen, dass neben dem Marktortprinzip auch das Niederlassungsprinzip im Zusammenhang mit der räumlichen Anwendung der DSGVO zu beachten ist.[24] Aus dem Niederlassungsprinzip folgt, dass die DSGVO auf Unternehmen mit Sitz in der Schweiz Anwendung finden kann, wenn das besagte Unternehmen über eine Niederlassung in der EU verfügt und im Rahmen der Tätigkeiten dieser Niederlassung personenbezogene Daten bearbeitet werden.[25] Der Begriff der Niederlassung wird weit verstanden und kann neben einfachen Zweigniederlassungen auch Abteilungen oder andere Einrichtungen eines Unternehmens erfassen.[26] Im Online-Vertrieb ist beispielsweise denkbar, dass ein europäisches Produktlager als Niederlassung qualifiziert wird.[27]

---

23 Zur Anwendung der DSGVO in Auftragsdatenbearbeitungsverhältnissen vgl. z.B. Vasella David, Zum Anwendungsbereich der DSGVO, digma 2017, S. 220 ff.

24 Zur Geltung der DSGVO im Allgemeinen, vgl. z.B. Bühlmann/Reinle (Fn. 8), S. 8 ff.; Voigt Paul/von dem Bussche Axel, The EU General Data Protection Regulation (GDPR): A Practical Guide, Springer International Publishing, Cham 2017, S. 9 ff. (zit. Voigt/von dem Bussche); zum räumlichen Geltungsbereich im Besonderen siehe auch Widmer Barbara, Welches Recht soll es sein?, digma 2018, S. 78 ff., hier S.78.

25 Ausführlich zum Niederlassungsprinzip nach Art. 3 Abs. 1 DSGVO, vgl. z.B. Däubler Wolfgang, Das Kollisionsrecht des neuen Datenschutzes, Recht der internationalen Wirtschaft (RIW) 2018, S. 405 ff., hier S. 406–407 (zit. Däubler).

26 In diesem Zusammenhang wird oftmals auch von einem flexiblen Niederlassungsbegriff gesprochen, vgl. Däubler (Fn. 25), S. 407.

27 Verschiedentlich wird auch vertreten, bereits ein Serverstandort könne für das Vorliegen einer Niederlassung genügend sein (vgl. z.B. Alich Stefan / Nolte Georg, Zur datenschutzrechtlichen Verantwortlichkeit (aussereuropäischer) Hostprovider für Drittinhalte, Computer und Recht (CR), Band 27/11, S. 741 ff., hier S. 742 ff. m.w.H.). Eine solch ausufernde Definition des Begriffs ist schon aus systematischen Gründen abzulehnen, zumindest soweit auf einem solchen Server keine Daten von Unionsbürgern verarbeitet werden.

c. Gesetzliche Grundlagen der vorliegenden Erörterung

[Rz 14] Da davon auszugehen ist, dass aufgrund des Marktortprinzips einerseits die Mehrheit der Schweizer Online-Shop-Betreiber der DSGVO unterstellt sind[28] und sich andererseits das schweizerische Datenschutzgesetz zwecks Angleichung an den europäischen Datenschutzstandard in Revision befindet[29], wird nachfolgend ausschliesslich auf die Bestimmungen der DSGVO eingegangen.

3. Datenschutzrechtliche Grundsätze

[Rz 15] Die europäische Datenschutzgesetzgebung ist ein technikneutral ausgestaltetes Gesetz.[30] Als solches ist es auf eine Vielzahl unterschiedlich gelagerter Fälle anwendbar und statuiert keine punktuellen Sonderregelungen für einen Online-Shop oder andere Vertriebsplattformen. Die DSGVO hat den Anspruch, den Umgang mit personenbezogenen Daten insgesamt zu regeln und ist entsprechend umfassend anwendbar.

a. Verbot mit Erlaubnisvorbehalt, Art. 6 Abs. 1 DSGVO

[Rz 16] Der DSGVO inhärent ist das Rechtsprinzip des sog. Verbots mit Erlaubnisvorbehalt.[31] Nach diesem Prinzip ist jede Bearbeitung personenbezogener Daten[32] grundsätzlich verboten und nur bei Vorliegen eines sog. Erlaubnistatbestandes zulässig. Die DSGVO benennt die Erlaubnistatbestände in Art. 6 Abs. 1 lit. a–f abschliessend. Zulässig ist demnach die Datenbearbeitung gestützt auf:

- eine *Einwilligung*: Eine Datenbearbeitung kann zulässig sein, wenn sie auf einer Einwilligung der betroffenen Person beruht. Eine Einwilligung ist erst gültig, wenn sie nach angemessener Information der betroffenen Person freiwillig erfolgt und unmissverständlich ist.[33] Die Einwilligung muss in Form einer Erklärung oder sonstigen bestätigenden Hand-

---

28 Die Kombination des sehr weitgehenden Ausrichtungsbegriffs einerseits und des Marktpotentials schon alleine im deutschsprachigen Raum (sog. DACH-Region) andererseits führen dazu, dass die meisten Schweizer Online-Angebote vom Anwendungsbereich erfasst sind. Hinzu kommt, dass die DSGVO seit dem 20. Juli 2018 auch in Liechtenstein direkt anwendbar ist, vgl. Blonski Dominika, Aus den Datenschutzbehörden, digma 2018, S. 154 ff., hier S. 156. Aufgrund der Zollunion zwischen dem Fürstentum Liechtenstein und der Schweiz ist die überwiegende Mehrheit der Schweizer Online-Shops folglich direkt vom Anwendungsbereich betroffen, soweit Konsumenten aus Liechtenstein nicht ausgeschlossen werden.

29 Medienmitteilung-Bundesrat (Fn.3).

30 Erwägungsgrund 15 DSGVO.

31 DSGVO 2017-Buchner/Petri (Fn.15), Art. 6 N 11–15.

32 Als personenbezogene Daten sind gemäss Art. 4 Abs. 1 DSGVO alle Informationen zu verstehen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Eine natürliche Person wird als identifizierbar angesehen, wenn sie direkt oder indirekt zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann. Siehe auch Voigt/von dem Bussche (Fn. 24), S. 11 ff.

33 Leeb Christina Maria/Liebhaber Johannes, Grundlagen des Datenschutzrechts, Juristische Schulung (JuS) 6/2018, S. 534 ff., hier S. 536–537 (zit. Leeb/Liebhaber).

lung abgegeben werden, wobei die Handlung eindeutig erfolgen muss und eine konkludente Einwilligung nicht leichthin angenommen werden sollte.[34]

- einen *Vertrag*: Eine Datenbearbeitung kann rechtmässig sein, wenn sie zur Erfüllung eines Vertrages oder vorvertraglicher Massnahmen mit der betroffenen Person erforderlich ist.[35]

- eine *gesetzliche Erlaubnis*: Erlaubt sind Datenbearbeitungen, die zur Erfüllung einer gesetzlichen Verpflichtung erforderlich sind (z.B. Aufbewahrungspflichten im Rechnungslegungsrecht). Zu beachten ist, dass schweizerische Gesetze nicht unter diesen Erlaubnistatbestand fallen.[36] Bei zwingenden gesetzlichen Vorgaben des Schweizer Rechts dürfte jedoch regelmässig ein überwiegendes berechtigtes Interesse gegeben sein.

- ein *überwiegendes berechtigtes Interesse*: Eine konkrete Datenbearbeitung kann schliesslich erlaubt sein, wenn sie zur Wahrung eines berechtigten Interesses eines Unternehmens erforderlich ist und dieses Interesse dasjenige der betroffenen Person überwiegt.[37] Als berechtigtes Interesse kann jedes wirtschaftliche oder ideelle Interesse in Frage kommen.[38] In diesem Zusammenhang sind Art, Inhalt und Aussagekraft der betroffenen Daten an dem mit der Datenverarbeitung verfolgten Zweck zu messen.[39] Es handelt sich um eine Wertungsfrage.[40]

[Rz 17] Eine Verarbeitung muss sich auf mindestens einen dieser Erlaubnistatbestände stützen. Stützt sie sich auf mehrere Tatbestände, stehen diese alle gleichrangig nebeneinander.[41] Deshalb sollte bei Vorliegen mehrerer Tatbestände jeweils auf alle verwiesen werden.[42] Die Nennung aller Erlaubnistatbestände ist wichtig, da eine bestimmte Datenbearbeitung sehr wohl aufgrund eines anderen Erlaubnistatbestandes zulässig sein kann, wenn eine betroffene Person entweder durch

---

34 Eine Einwilligung durch Stillschweigen oder Untätigkeit ist folglich von vornherein ausgeschlossen, vgl. Leeb/Liebhaber (Fn. 33), S. 536; Peitz Martin/Schweitzer Heike, Ein neuer europäischer Ordnungsrahmen für Datenmärkte? Neue Juristische Wochenschrift (NJW) 5/2018, S. 275 ff., hier S. 276 (zit. Peitz/Schweitzer).

35 Gierschmann Sibylle, Gestaltungsmöglichkeiten bei Verwendung von personenbezogenen Daten in der Werbung, MultiMedia und Recht (MMR) 2018, S. 7 ff., hier S. 8 (zit. Gierschmann); Griesinger Marcel, Zulässigkeit der Verwendung von Google-Analytics nach der Datenschutz-Grundverordnung, Compliance Berater (CB) 2018, S. 327 ff., hier S. 328 (zit. Griesinger); DSGVO 2017-Buchner/Petri (Fn. 15), Art. 6 N 26–27.

36 DSGVO 2017-Buchner/Petri (Fn. 15), Art. 6 N 86.

37 Peitz/Schweitzer (Fn. 34), S. 276; Griesinger (Fn. 35), S. 328; DSGVO 2017-Buchner/Petri (Fn. 15), Art. 6 N 148.

38 Gierschmann (Fn. 35), S. 9 f.

39 DSGVO 2017-Buchner/Petri (Fn. 154), Art. 6 N 148; je sensibler die Information, umso grösser wird das Interesse des Betroffenen am Ausschluss einer Verarbeitung sein, vgl. Gierschmann (Fn. 35), S. 11.

40 Winkler Markus, Datenschutz bei M&A Transaktionen, GesKR 2018, S. 124 ff., hier S. 137. Das Interesse an einer bestimmten Datenbearbeitung muss entsprechend nicht nur objektiv betrachtet berechtigt sein, es muss zudem das Interesse der betroffenen Personen am Unterbleiben der Datenbearbeitung überwiegen. Diese Interessenabwägung muss für jede fragliche Datenbearbeitung im konkreten Fall beurteilt werden. Folglich kann dieser Erlaubnistatbestand keine stabile Grundlage für regelmässige Datenbearbeitungen bilden.

41 Remmertz Frank, DSGVO ante portas: Aktuelle Brennpunkte im Online-Marketing, GRUR-Prax 2018, S. 254 ff., hier S. 254 (zit. Remmertz, Online-Marketing); Gierschmann (Fn. 35), S. 8.

42 In der Regel geschieht dies im Rahmen des Online-Handels über die sog. Datenschutzerklärungen.

Verweigern der Einwilligung oder im Rahmen ihrer Betroffenenrechte[43] einer Bearbeitung ihrer Daten widerspricht.[44]

b. Grundprinzipien der rechtmässigen Datenbearbeitung, Art. 5 DSGVO[45]

[Rz 18] Das Vorliegen eines Erlaubnistatbestandes führt für sich alleine noch nicht zu einer DSGVO-konformen Datenbearbeitung. Vielmehr sind bei einer rechtmässigen Datenbearbeitung auch die sog. Datenbearbeitungsgrundsätze einzuhalten. Die Grundsätze sind die Verarbeitung nach Treu und Glauben und Transparenz (Art. 5 Abs. 1 lit. a DSGVO), Zweckbindung (Art. 5 Abs. 1 lit. b DSGVO), Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO), Richtigkeit (Art. 5 Abs. 1 lit. d DSGVO), Speicherbegrenzung (Art. 5 Abs. 1 lit. e DSGVO), Integrität und Vertraulichkeit (Art. 5 Abs. 1 lit. f DSGVO) sowie die Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO).

[Rz 19] Auf die Bedeutung dieser Datenbearbeitungsgrundsätze wird sogleich anlässlich der Beleuchtung der einzelnen Datenbearbeitungen näher eingegangen.

III. Besuch der Webseite und des Online-Shops

1. Datenschutzrechtliche Aspekte beim Aufruf der Webseite

[Rz 20] Da beim Aufruf einer Webseite stets eine technische Kommunikation zwischen dem Server eines Internetnutzers und dem Server eines Webseiten-Betreibers erfolgt, hinterlässt ein Nutzer bereits beim blossen Aufruf einer Webseite eine Vielzahl von technischen Daten. Der Server eines Webseiten-Betreibers ist in der Regel mit einer Protokollierungsfunktion ausgestattet, die es ihm ermöglicht, diese Daten in einer technischen Datei (sog. Logfile) zu erfassen und zu speichern.[46] Die Bearbeitung erfolgt automatisch und ohne Zutun des Nutzers. Die im Logfile erfassten Daten sind mit der IP-Adresse des anfragenden Rechners verknüpft. IP-Adressen sind mittlerweilen grundsätzlich als personenbezogene Daten zu behandeln.[47] Deren Speicherung hat somit den datenschutzrechtlichen Bestimmungen standzuhalten und es besteht unter anderem die Pflicht, die betroffene Person «*in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache*» über die Verarbeitung ihrer Daten sowie über ihre Rechte zu informieren (Transparenzgrundsatz, Art. 5 Abs. 1 lit. a DSGVO). Der Transparenzgrundsatz gilt ungeachtet des jeweiligen Erlaubnistatbestandes (und insbesondere auch bei Vorliegen eines überwiegenden berechtigten Interesses). Die Informationsvermittlung erfolgt in der Regel mittels sog. Datenschutzerklärungen. Da die Bearbeitung nicht anlasslos erfolgen darf, müssen

43 Betroffenenrechte sind insb. das Recht auf Information (Art. 13–14 DSGVO), Auskunftsrecht (Art. 15 DSGVO), Recht auf Berichtigung (Art. 16 DSGVO), Recht auf Löschung (Art. 17 DSGVO), Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO), Recht auf Mitteilung (Art. 19 DSGVO), Widerspruchsrecht (Art. 20 DSGVO).

44 DSGVO 2017-Buchner/Petri (Fn. 15), N 23.

45 Für einen guten Überblick über die datenschutzrechtlichen Grundsätze, vgl. statt vieler Frenzel Eike Michael, in: Paal / Pauly (Hrsg.), Datenschutz-Grundverordnung Bundesdatenschutzgesetz: DSGVO BDSG, Kommentar, 2. Aufl. 2018, Art. 5.

46 Weber Rolf H., E-Commerce und Recht, Rechtliche Rahmenbedingungen elektronischer Geschäftsformen, 2. Aufl. 2010, S. 471.

47 Urteil des europäischen Gerichtshofs (EuGH) vom 19. Oktober 2016 (C-582/14) sowie Urteil des deutschen Bundesgerichtshof (BGH) vom 16. Mai 2017 (VI ZR 135/13); BGE 136 II 508 (Logistep-Urteil); Moos Flemming / Heidrich Jörg, in: Forgo/Helfrich/Schneider (Hrsg.), Betrieblicher Datenschutz, 2. Aufl. 2017, § 1 N 7 m.w.H.

in der Datenschutzerklärung auch Angaben zum Zweck der Datenbearbeitung und zur Rechtsgrundlage der Bearbeitung gemacht werden.[48] Die Datenschutzerklärungen sind im Rahmen der Webseiten-Nutzung jederzeit auffindbar zu halten.[49]

[Rz 21] Der Zweck der Speicherung der IP-Adressen und anderer Daten im Logfile liegt dabei regelmässig in der Sicherheit und Stabilität der Webseite. Die Daten aus dem Logfile werden bei allfälligen Angriffen auf die Netzinfrastruktur oder anderen unerlaubten oder missbräuchlichen Webseiten-Nutzungen zur Aufklärung und Abwehr ausgewertet und können gegebenenfalls auch im Rahmen eines Strafverfahrens gegen die betroffene Person verwendet werden. Daran hat ein Webseiten-Betreiber anerkanntermassen ein berechtigtes Interesse, das die Interessen des Nutzers auf Unterlassen dieser Datenbearbeitungen überwiegt. Da die entsprechenden Daten ausserdem nach einer gewissen Dauer gelöscht werden müssen, ist die Datenbearbeitung auch vor dem Hintergrund der datenschutzrechtlichen Grundsätze, insbesondere des Datenminimierungsgebots, rechtmässig. Das Datenminimierungsgebot besagt, dass die Daten nur solange bearbeitet werden dürfen, wie es deren Zweck erfordert.[50] Zu beachten ist, dass die Speicherung der Logfile-Daten nur während einer gewissen Zeit vom Sicherheitsbedürfnis eines Webseiten-Betreibers gedeckt sein kann. Je länger die Daten gespeichert werden, desto ausführlicher sollte in der Datenschutzerklärung über die Zwecke und die Dauer der Speicherung informiert werden.

2. Verwendung von Tracking- und Webanalysetools

[Rz 22] Die Auswertung der Kundendaten sowie der Daten potentieller Kunden und damit die Beschaffung von Informationen zu deren Interessen und Vorlieben ist für den geschäftlichen Erfolg im E-Commerce von zentraler Bedeutung. Entsprechend ist moderner E-Commerce ohne den Einsatz technischer Tools in einem Online-Shop kaum mehr kompetitiv möglich. Diese Webanalyse-Tools werden insbesondere für Marketingzwecke und die technische Optimierung der Abläufe und Funktionen des Online-Shops verwendet und basieren bekanntlich auf dem Einsatz von Cookies oder vergleichbaren Technologien. Das bekannteste Webanalysetool ist Google Analytics.[51]

[Rz 23] Die Rechtmässigkeit des Einsatzes solcher Technologien bedingt wiederum die vollständige und transparente Information betreffend die mit dem Einsatz verbundenen Datenbearbeitungen. Schliesslich stellt sich auch hier die Frage der Rechtsgrundlage. Dabei stehen beim Einsatz von Tracking- und Webanalysetools die Erlaubnistatbestände des berechtigten Interesses (Art. 6 Abs. 1 lit. f DSGVO) und der Einwilligung (Art. 6 Abs. 1 lit. a DSGVO) im Vordergrund. Beide Erlaubnistatbestände sind in diesem Kontext jedoch umstritten bzw. problematisch.

---

48 Weitere Angaben sind bspw. der Name und Kontaktdaten des Verantwortlichen sowie ggf. seines Vertreters sowie die Dauer der Datenspeicherung, vgl. Art. 13 DSGVO.

49 Auch die Auffindbarkeit ist Ausfluss der Informationspflicht gemäss Art. 13 DSGVO.

50 Leeb/Liebhaber (Fn. 35), S. 537; Thouvenin Florent, Forschung im Spannungsfeld von Big Data und Datenschutzrecht: eine Problemskizze, in: Boehme-Nessler/Rehbinder (Hrsg.): Big Data: Ende des Datenschutzes? Gedächtnisschrift für Martin Usteri, Schriften zur Rechtspsychologie Band 15, 2017, S. 27 ff., hier S. 34 f. (zit. Thouvenin).

51 Google Analytics ist ein Tool des Unternehmens Google Inc. und untersucht als Datenverkehrsanalyse u.a. die Herkunft der Besucher und ihre Verweildauer und erlaubt damit eine bessere Erfolgskontrolle von Werbekampagnen. Es wird von geschätzt 50–80% aller Webseiten verwendet (Web Technology Survey von W3Techs, abrufbar unter: https://w3techs.com/technologies/overview/traffic_analysis/all, zuletzt abgerufen am 20. September 2018).

[Rz 24] Mit Bezug auf das berechtigte Interesse eines Webseiten-Betreibers ist umstritten, ob dieses Interesse dasjenige des Besuchers überwiegen und als alleinige Rechtsgrundlage herangezogen werden kann.

[Rz 25] Teilweise wird argumentiert, vom Schutzbedürfnis des Besuchers könne nicht ausgegangen werden, da dieser über kein überwiegendes berechtigtes Interesse verfüge.[52] So würden beispielsweise die IP-Adressen beim Einsatz solcher Tools üblicherweise verkürzt und pseudonymisiert verwendet, das heisst, eine *persönliche* Identifizierung des Nutzers sei nicht direkt möglich.[53] Die Tools bzw. das Setzen der Cookies würden lediglich die *Wiedererkennung* des Besuchers ermöglichen.[54] Des Weiteren wird auch argumentiert, der Besucher müsse als durchschnittlich verständiger Internetnutzer davon ausgehen, dass seine IP-Adresse vom Betreiber einer Internetseite zu Marketing- und Optimierungszwecken ausgewertet wird, sei es doch ein offenkundiges Interesse eines Webseiten-Betreibers, Informationen für Marketingzwecke über seine Besucher zu erlangen.[55] Ausserdem müsse ein Webseiten-Betreiber, der das Analyse-Tool einsetzt, den Anbieter des Tools ohnehin vertraglich zur Einhaltung der datenschutzrechtlichen Vorgaben verpflichten (insbesondere im Rahmen eines Auftragsdatenbearbeitungsvertrages nach Art. 28 DSGVO).[56] Dadurch vermindere sich das Schutzbedürfnis der betroffenen Person. Zusammenfassend könne daher gefolgert werden, dass (zumindest die «standardmässigen») Webanalysen mittels Tracking-Technologien durch ein überwiegendes und berechtigtes Interesse des Webseiten-Betreibers nach Art. 6 Abs. 1 lit. f DSGVO gerechtfertigt werden können und keiner anderen Rechtsgrundlage, insbesondere keiner Einwilligung bedürfen.[57]

[Rz 26] Dieser Ansicht kann nach hier vertretener Auffassung nicht gefolgt werden, da die Person, obschon nicht identifiziert, trotzdem identifizierbar bleibt und die DSGVO ausdrücklich festhält, eine Identifikation durch «Online-Kennungen» wie Cookies oder IP-Adressen seien personenbezogene Daten.[58] Die Diskussion über ein allfälliges berechtigtes und überwiegendes Interesse des Webseiten-Betreibers ist aber ohnehin von vergänglicher Relevanz, denn es ist zu erwarten, dass die geplante sog. europäische E-Privacy-Verordnung[59] den Einsatz von Cookies und ähnlicher Technologien nur noch mit vorgängiger aktiver und informierter Einwilligung zulassen wird.[60]

[Rz 27] Gerade im Zusammenhang mit neueren oder komplexen Technologien ist es indes – selbst rein theoretisch – fraglich, ob die Voraussetzung der Informiertheit einer gültigen Einwilligung bei einem durchschnittlichen Internetnutzer im Rahmen des alltäglichen Surfverhaltens

---

52 Vgl. z.B. Griesinger (Fn. 35), S. 328.

53 Ibid.

54 Mit dem Thema der Identifizierbarkeit setzt sich differenziert auseinander Rosenthal David, Personendaten ohne Identifizierbarkeit?, digma 2017, S. 198 ff., hier S. 198 (zit. Rosenthal).

55 Hanloser Stefan, Geräte-Identifier im Spannungsfeld von DSGVO, TMG und e-Privacy-VO, Zeitschrift für Datenschutz (ZD) 2018, S. 213 ff., hier S. 215-217 (zit. Hanloser); Griesinger (Fn. 35), S. 328.

56 Griesinger (Fn. 35), S. 328.

57 Griesinger (Fn.35), S. 328; Hanloser (Fn.55), S. 215–217, anderes würde gelten, wenn besonders schützenswerte Daten Bestandteil der Analyse sind. Dann ist stets eine Einwilligung durch die betroffene Person erforderlich, vgl. Art. 9 Abs. 2 lit. a DSGVO.

58 Art. 4 Ziff. 1 i.V.m Art. 30 DSGVO; Rosenthal (Fn. 54), S. 198.

59 Vorschlag für eine Verordnung des europäischen Parlaments des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation) vom 10. Januar 2017, COM (2017).

60 Die E-Privacy-Verordnung wird ebenfalls einen sehr weiten geografischen Anwendungsbereich enthalten und auch für Schweizer Unternehmen relevant sein, vgl. Mattig/Zuber (Fn. 3), S. 704.

überhaupt erreicht und sichergestellt werden kann. Nach der hier vertretenen Auffassung vermag denn auch das pauschale Abstellen auf ein angeblich überwiegendes berechtigtes Interesse nach Art. 6 Abs. 1 lit. f DSGVO diese Schwierigkeit nicht aufzulösen. Die Zwecke des Trackings können sehr vielfältig sein und ein allfällig überwiegendes Interesse muss einer konkreten Prüfung im Einzelfall standhalten. In der Regel werden – um die Informiertheit und Erkennbarkeit der eingesetzten Technologie zu gewährleisten – sog. Cookie-Banner eingesetzt, die auf den Einsatz der Cookies und Technologien hinweisen. Davon entbindet das Vorliegen eines überwiegenden berechtigten Interesses nicht. Gegenwärtig ist absehbar, dass die E-Privacy Verordnung bei den Cookie-Bannern, für die bisher eher Opt-Out-Lösungen vorgehsehen waren, ein aktives Opt-In verlangen wird.[61] Gegen dieses Opt-In-Erfordernis, wonach der Besucher ausdrücklich seine Einwilligung zu den Cookies zu geben hat, formiert sich erheblicher Widerstand in der Online-Wirtschaft, da werbebasierte Geschäftsmodelle als gefährdet angesehen werden.[62] Gegenwärtig finden noch Konsultationen auf politischer Ebene statt, sodass noch nicht abschliessend gesagt werden kann, wann die E-Privacy-Verordnung in Kraft treten wird und wie in Zukunft mit Cookies und ähnlichen Technologien umgegangen werden muss. Die Deutsche Konferenz der unabhängigen Datenschutzaufsichtsbehörden (DSK) hat in ihrem Positionspapier jedenfalls festgehalten, Tracking-Mechanismen würden bereits mit Inkrafttreten der DSGVO klar einer vorherigen Einwilligung bedürfen.[63]

3. Verwendung von Social Media zur Verkaufsförderung

[Rz 28] Viele Online-Shops stellen ihren Kunden die Möglichkeit zur Verfügung, Produkte oder Kauferfahrungen in den Social Media Kanälen zu kommentieren und zu teilen. Aus datenschutzrechtlicher Sicht sind insbesondere die sog. Social-Plugins (z.B. der Facebook «Like»-Button) heikel. Sofern nicht spezifische Massnahmen getroffen werden, kommunizieren diese Plugins mit der darin verlinkten Social Media Plattform im Hintergrund. Dabei werden, ohne Wissen und aktives Tun des Nutzers, Daten an die Social Media Plattform gesendet und zwar selbst dann, wenn der Nutzer über kein entsprechendes Profil auf der Plattform verfügt. Es besteht deshalb die Gefahr, dass «Schattenprofile» von Nicht-Mitgliedern erstellt werden.[64] Mit anderen Worten werden die Daten an die Social Media Plattform übermittelt, ohne dass die betroffene Person entsprechend informiert wurde und ohne dass sie ihre Einwilligung hierfür erteilt hat.

[Rz 29] Der Einsatz solcher Social Plugins beruht somit auf keinem der von der DSGVO vorgesehenen Erlaubnistatbestände. Weiter widerspricht der Einsatz dieser Plugins – zumindest in der durch die entsprechenden Sozialen Medien zur Verfügung gestellten Form – verschiedenen

---

61 Remmertz Frank, Aktuelle Entwicklungen im Social Media-Recht, MultiMedia und Recht (MMR) 2018, S. 507 ff., hier S. 508 (zit. Remmertz, Social Media).

62 Remmertz, Social Media (Fn. 61), S. 508 m.w.H.

63 Positionspapier der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 26. April 2018, S. 3, abrufbar unter: https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Technik/Inhalt/TechnikundOrganisation/Inhalt/Zur-Anwendbarkeit-des-TMG-fuer-nicht-oeffentliche-Stellen-ab-dem-25_-Mai-2018/Positionsbestimmung-TMG.pdf, zuletzt abgerufen am 11. Oktober 2018.

64 Bühlmann Lukas/Schüepp Michael, Marketing und Internet – datenschutzrechtliche Aspekte, in: Passadelis et al. (Hrsg.), Datenschutzrecht, 2015, N 19.95 m.w.H. (zit. Bühlmann/Schüepp).

datenschutzrechtlichen Grundprinzipien, insb. dem Transparenz- und Zweckbindungsprinzip (Art. 5 Ziff. 1 lit. a und b DSGVO).

[Rz 30] Eine Möglichkeit zur Reduzierung der rechtlichen Risiken besteht im Einsatz der sog. 2-Klick-Lösung oder dem sog. «Shariff»-Plugin, verbunden mit einer transparenten Information über den Einsatz dieser Plugins sowie den damit verbundenen Datenbearbeitungen.

[Rz 31] Bei den 2-Klick-Lösungen werden die Social Plugins erst dann aktiviert und die Daten an die Social Media Plattform übermittelt, wenn auf die entsprechende Schaltfläche geklickt wird. Ist der Button aktiviert, wird der eigentliche Like-Button geladen, den der Nutzer noch ein zweites Mal anklicken muss, um dessen eigentliche Funktion auslösen zu können. Bei «Shariff» ist demgegenüber nur ein Klick erforderlich und Informationen der Webseiten-Besucher werden erst nach dem Anklicken auf den Button an die Plattform übertragen.[65] Durch entsprechende Ausgestaltung der Webseite (*privacy by design*) und namentlich klarer Information in der Datenschutzerklärung kann folglich eine Einwilligung des Nutzers vor der Übermittlung der Daten eingeholt werden. Dabei ist sicherzustellen, dass die Informationen vollständig und transparent erfolgen, d.h. es ist insbesondere auf die Weitergabe der Daten an das entsprechende Soziale Netzwerk hinzuweisen. Trotzdem bleibt die Verwendung dieser Plugins nicht unproblematisch, da die Einwilligung nicht beweissicher protokolliert und dokumentiert werden kann.

IV. Einkaufen im Online-Shop

1. Preisgabe von Daten zur Durchführung einer Bestellung

[Rz 32] Für die Bestellung in einem Online-Shop muss eine Vielzahl personenbezogener Daten bekanntgegeben werden (z.B. Name, E-Mail-Adresse, Wohnadresse etc.). Da der Kunde die Daten selber eingibt und der Zweck der darauffolgenden Datenbearbeitung (Vertragsschluss und Bestellabwicklung) erkennbar ist, kann hier jeweils nur fraglich sein, ob die Erhebung bestimmter Daten im Hinblick auf den Abschluss oder die Abwicklung des Vertrages verhältnismässig ist. Da im Online-Kontext der Vertragspartner identifiziert werden muss, dürfte es dem Verhältnismässigkeits- und auch Datenminimierungsgebot entsprechen, wenn Kunden ihren Namen sowie ihre Adresse angeben müssen. Auch die Option, Bestellungen nur als Gast und somit ohne Eröffnung eines Kundenkontos zu tätigen, kann als Ausfluss des Grundsatzes der Datenminimierung gesehen werden. Denn zur einfachen Abwicklung einer Bestellung sind die Eröffnung eines Kundenkontos und die damit verbundene dauerhafte Speicherung zusätzlicher Angaben durch den Shop-Betreiber nicht erforderlich. Unproblematisch ist im Übrigen auch die Erhebung einer E-Mail-Adresse. Denn Online-Anbieter sind ohnehin gesetzlich verpflichtet, den Eingang einer Bestellung auf elektronischem Wege zu bestätigen.[66] Im Übrigen ist jeweils im Einzelfall zu prüfen, ob die erhobenen Daten für den Zweck der Abwicklung der Bestellung notwendig und damit verhältnismässig erscheinen. Werden mehr Daten erhoben, als zu diesem offensichtlichen Zweck erforderlich, ist dies nur gestützt auf eine zusätzliche Rechtsgrundlage möglich. In der Regel ist dann eine informierte Einwilligung einzuholen, und in der Datenschutzerklärung sind wieder-

65 Vgl. zu beiden Lösungen ausführlich Föhlisch Carsten/Pilous Madeleine, Der Facebook Like-Button – datenschutzkonform nutzbar? Analyse und Risikoeinschätzung des «Gefällt mir»-Buttons auf Webseiten, MultiMedia und Recht (MMR) 2015, S. 631 ff., hier S. 635–636.

66 Bühlmann/Schüepp (Fn. 64), N 19.51.

um Zweck und Ausmass der zusätzlichen Bearbeitung darzulegen. Selbstverständlich sind diese zusätzlichen Datenbearbeitungen im Kontext des Online-Handels üblich, weshalb Kunden – wie bereits erwähnt – im Rahmen des Vertragsschlusses dazu ermutigt werden, ein Kundenkonto zu eröffnen.

2. Eröffnung eines Kundenkontos

[Rz 33] Bei der Eröffnung eines Kundenkontos werden regelmässig umfangreichere Informationen über die Kunden erhoben und dauerhaft im Kundenverwaltungssystem (sog. Customer Relationship Management, CRM) des Webshop-Betreibers gespeichert. Diese Datenbearbeitung kann nicht auf den Erlaubnistatbestand des Vertragsschlusses und der Bestellabwicklung gestützt werden.[67] Zur Rechtmässigkeit braucht es in aller Regel eine informierte Einwilligung der betreffenden Personen. In einer Datenschutzerklärung ist über die mit dieser dauerhaften Speicherung der Kundendaten verbundenen Zwecke transparent zu informieren (Transparenzgebot, Art. 5 Ziff. 1 lit. a DSGVO). Sodann sind die erhobenen Daten auf diejenigen zu beschränken, die für das Bereitstellen und das Führen des Kundenkontos benötigt werden (Datenminimierungsgebot, Art. 5 Ziff. 1 lit. c DSGVO). In den meisten Fällen beschränkt sich dies auf die Login-Informationen. Je nach Funktionalitäten der Kundenkonti und den damit verbundenen Kundennutzen ist aber durchaus denkbar, dass auch weitere Informationen zur Eröffnung eines Kontos zwingend erhoben werden dürfen. Selbstredend ist, dass Kundenkonti gelöscht, resp. die mit der Eröffnung verbundenen Einwilligungen widerrufen werden können. Entsprechend ist die Information über die Betroffenenrechte und deren Ausübung in diesem Zusammenhang besonders wichtig.

3. Bonitätsprüfungen / Scoring

[Rz 34] Für den Onlinehandel ist die Bonitätsprüfung eines der wichtigsten Mittel zur Vermeidung von Zahlungsausfällen (insbesondere im Rahmen des sog. Rechnungskaufs, wenn also der Online-Shop mit seiner Warenlieferung in Vorleistung geht). Die Bonitätsprüfung wird in aller Regel durch ein Drittunternehmen im Hintergrund anlässlich des Bestellprozesses im Interesse des Online-Händlers durchgeführt. Folglich sind die Anforderungen bezüglich der Auftragsdatenbearbeitung einzuhalten.[68]

[Rz 35] Hinzu kommt, dass die Prüfung regelmässig automatisiert, also ohne «menschliches Zutun» erfolgt. Mit anderen Worten wird automatisiert unter Umständen darüber entschieden, zu welchen Bedingungen mit dem Besteller ein Vertrag geschlossen wird oder nicht (beim Entscheid über die Gewährung des Rechnungskaufes handelt es sich letztlich um einen Kreditentscheid). Die DSGVO gewährt den Betroffenen grundsätzlich das Recht, solche «automatisierten Einzelentscheidungen» durch einen Menschen überprüfen zu lassen.[69] Dies soll jedoch auch nach Ansicht von Datenschützern nicht gelten, wenn der Vorgang zur Reduktion des Risikos von Zahlungsaus-

67 So ist es für den Vertragsschluss oder den Bestellvorgang nicht zwingend nötig, dass die Kundendaten in einem CRM gespeichert werden.

68 Vgl. Art. 28 Abs. 3 DSGVO.

69 Art. 22 Abs. 3 DSGVO, wobei es sich hierbei nicht nur um ein Individualrecht des Betroffenen handelt. Vielmehr handle es sich bei der Bestimmung um ein allgemeines Verbot bzw. eine Rechtmässigkeitsvoraussetzung, vgl. Abel Ralf, Automatisierte Entscheidungen im Einzelfall gem. Art. 22 DSGVO, Zeitschrift für Datenschutz (ZD) 2018,

fällen führt.[70] Eine verhältnismässige Bonitätsprüfung ist somit beim Kauf auf Rechnung auch künftig zulässig, ohne dass eine nachträgliche Überprüfung vorgenommen werden muss. Gleichwohl sind die weiteren Vorgaben der DSGVO auch hier zu beachten. So muss vor allem auf die automatisierte Bonitätsprüfung deutlich in der Datenschutzerklärung hingewiesen und in verständlicher Weise über die Grundprinzipien der involvierten Logik informiert werden.

[Rz 36] Da die Datenübermittlung bzw. -einholung mit dem Vertragsschluss und der Vertragsabwicklung in unmittelbarem Zusammenhang steht, ist sie auch ohne Einwilligung durch den Kunden rechtmässig. Vorausgesetzt ist aber stets, dass die Bonitätsprüfung im Sinne einer Gesamtbeurteilung, insbesondere in Anbetracht des Werts der angebotenen Leistung als angemessen erscheint.[71]

4. Anmeldung zum Newsletter

[Rz 37] Nach Abschluss der Bestellung an der virtuellen Kasse hat der Kunde regelmässig die Möglichkeit, sich für den Newsletter des Verkäufers anzumelden. Der Kunde hat hierfür meist ein Kästchen anzukreuzen, wobei das Setzen des Kreuzes eine Einwilligung darstellt (Single Opt-In). Eingewilligt wird dabei in die Verwendung seiner Daten (insbesondere der E-Mail-Adresse) zwecks Versands bzw. Erhalts des Newsletters und die Auswertung der anschliessenden Nutzung des Newsletters.

[Rz 38] Die entsprechend eingeholte Einwilligung führt für sich alleine aber noch nicht zur Rechtmässigkeit des Newsletter-Versandes und der Nutzung der darüber erfassten Daten.[72] Die datenschutzrechtliche Wirksamkeit der Einwilligung ist wiederum von der vorgängigen Information über die mit der Nutzung des Newsletters verbundenen Datenbearbeitungen abhängig. Diese Informationen sind leicht zugänglich, d.h. in unmittelbarer Nähe des anzukreuzenden Kästchens mit einem verlinkten Hinweis anzubringen.

[Rz 39] Wichtig ist sodann die Freiwilligkeit der Anmeldung zum Newsletter.[73] Diese stellt eine zentrale Anforderung an die Wirksamkeit der Einwilligung dar.[74] An der Freiwilligkeit fehlt es nicht nur, wenn ohne Anmeldung nicht bestellt werden kann. Sie kann auch in Frage gestellt werden, wenn andere vertragliche Nebenleistungen im Bereich des After-Sales von der Anmeldung eines Newsletters, meist verbunden mit der Eröffnung eines Kundenkontos, abhängig gemacht werden und dafür keine objektive Notwendigkeit besteht.[75] Der Online-Shop-Betreiber muss sodann nachweisen können, dass eine rechtswirksame Einwilligung eingeholt wurde.[76] Erfolgt die Anmeldung zum Newsletter im Rahmen eines Bestellabschlusses in einem Online-Shop, ist die-

S. 304 ff., hier S. 305; Martini Mario / Nink David, Wenn Maschinen entscheiden..., Neue Zeitschrift für Verwaltungsrecht (NVwZ) 2017, S. 681 ff., hier S. 681.

70 Vgl. statt vieler Schuld Sebastian, in: Gola (Hrsg.), Datenschutz-Grundverordnung, Kommentar, 2. Aufl. 2018, Art. 22 N 29–30 m.w.H.

71 Bühlmann/Schüepp (Fn. 64), N 19.55.

72 Leeb/Liebhaber (Fn. 33), S. 536.

73 Art. 7 Abs. 4 DSGVO.

74 Vgl. zum Ganzen DSGVO 2017-Buchner/Kühling (Fn. 15), Art. 7 N 41.

75 DSGVO 2017-Buchner/Kühling (Fn. 15), Art. 7 N 42.

76 Sog. Nachweispflicht, vgl. DSGVO 2017-Buchner/Kühling (Fn. 15), Art. 7 N 22. Die Nachweispflicht ergibt sich sodann auch aus den Spam-Vorschriften, im Schweizer Recht insb. aus Art. 3 lit. o Bundesgesetz gegen den unlauteren Wettbewerb vom vom 19. Dezember 1986 (UWG; SR 241).

ser Nachweis durch die Identifikation des Bestellers über den Vertragsschluss in der Regel ohne weiteres möglich. Dies zumindest bei dem Besteller eindeutig zuzuordnender E-Mail-Adresse. Erfolgt die Anmeldung zum Newsletter unabhängig von einer konkreten Bestellung, besteht das Risiko, dass die Anmeldung nicht durch den Empfänger der angegebenen E-Mail-Adresse erfolgt. Die meisten Online-Shop- und Webseiten-Betreiber bedienen sich deshalb des sog. «Double-Opt-In»-Verfahrens. Beim Double-Opt-In-Verfahren wird im Rahmen des Anmeldeprozesses zunächst eine erstes «Opt-In» durch das Ankreuzen des Kästchens und die Angabe der E-Mail-Adresse des Empfängers verlangt. Unmittelbar danach wird ein weiteres «Opt-In» verlangt, indem dem Kunden eine erste E-Mail geschickt wird, mit der Bitte, er möge die Anmeldung mittels Anklicken eines Links bestätigen (zweites «Opt-In»).

[Rz 40] Im Übrigen ist an dieser Stelle auch auf das sog. Kopplungsverbot hinzuweisen. Eine verbotene Kopplung würde beispielsweise vorliegen, wenn die Erfüllung eines Vertrages von der Einwilligung in weitere Datenbearbeitungen (z.B. Bearbeitung der Daten für Werbezwecke) abhängig gemacht wird und diese «weiteren Datenbearbeitungen» mit dem Vertrag nicht zusammenhängen.[77] Jüngst hat sich auch das oberste Gericht Italiens mit dem Kopplungsverbot befasst.[78] Das Gericht gelangte dabei – für viele erstaunlicherweise etwas unerwartet – zum Ergebnis, dass es durchaus zulässig sein kann, die unentgeltliche Erbringung von Dienstleistungen von einer Einwilligung in die Verwendung personenbezogener Daten zu Werbezwecken abhängig zu machen. An der Freiwilligkeit der Einwilligung könne es nach Ansicht des Gerichts nur dann fehlen, wenn die betroffene Dienstleistung unersetzbar oder unverzichtbar sei. Im besagten Fall wurde dies in Bezug auf einen Newsletter für Finanz- und Steuerinformationen jedoch verneint, weil die Nutzer «ohne ernsthafte Nachteile» auf den Dienst verzichten könnten und es sich eindeutig um Informationen handle, die leicht auf andere Weise erwerbbar seien.[79] Diese erste Entscheidung zum neuen Kopplungsverbot gemäss DSGVO ist nach hier vertretener Ansicht zu begrüssen.

V. Datenbearbeitungen im Anschluss an den Einkauf im Online-Shop

1. Weitergabe der Daten zwecks Versendung der Ware

[Rz 41] Viele Online-Händler überlassen die Versandlogistik einem externen Dienstleister. Entsprechend ist es üblich, dass einem sog. Fullfillment-Dienstleister, der die Ware lagert und für den Versand vorbereitet, über eine technische Schnittstelle Zugriff auf die Bestelldaten gegeben wird. Im Verhältnis zum Kunden als betroffene Person ist diese Datenbearbeitung durch den Vertragsschluss gedeckt und rechtmässig, solange darüber in der Datenschutzerklärung informiert wird. Im Verhältnis zum externen Logistik-Dienstleister ist diese Datenweitergabe selbstverständlich ebenfalls datenschutzrechtlich relevant und führt zu einem typischen Auftragsdatenbearbeitungsverhältnis (der Dienstleister bearbeitet die Daten im Auftrag und Interesse des Online-Händlers als verantwortlicher Dateninhaber). Solche Formen der Zusammenarbeit müs-

77 In diesem Zusammenhang ist zwischen dem absoluten und relativen Kopplungsverbot zu unterscheiden, beide sind problematisch, vgl. Remmertz, Online-Marketing (Fn. 41), S. 255 m.w.H.

78 Urteil des Obersten Gerichtshof Italiens vom 11. Mai 2018, Urteil Nr. 17278/2018.

79 Vgl. hierzu die Urteils-Erörterung im MLL-Newsletter vom 1. September 2018, abrufbar unter: https://www.mll-news.com/italiens-kassationsgericht-zum-kopplungsverbot-bei-gratisdiensten-freiwilligkeit-der-einwilligung-fehlt-nur-bei-unverzichtbaren-diensten/, zuletzt abgerufen am 20. September 2018.

sen gemäss DSGVO datenschutzrechtlich im Rahmen eines spezifischen schriftlichen Vertrages geregelt werden (eines Auftragsdatenbearbeitungsvertrages).[80] Die DSGVO macht konkrete Vorgaben an den Regelungsinhalt eines solchen Vertrages.[81] So muss sich der Auftraggeber, also der Online-Händler, insbesondere Weisungs- und Kontrollrechte zusichern lassen.[82] Der Auftraggeber trägt die Verantwortung der Datensicherheit und bleibt in jedem Fall – trotz Einsatz eines Dritten – gegenüber den von der Datenverarbeitung betroffenen Personen verantwortlich für die Einhaltung der datenschutzrechtlichen Vorgaben. Entsprechend verpflichtet sich der Auftragnehmer unter diesem Vertrag zur instruktionsgemässen Bearbeitung der Daten und Beachtung aller relevanten Datenschutzvorschriften.[83] Der Datenverantwortliche ist folglich gut beraten, Datenbearbeitungen nur durch Unternehmen vornehmen zu lassen, die durch die Implementierung von technischen und organisatorischen Massnahmen die Bearbeitung im Einklang mit der DSGVO sicherstellen können.[84]

[Rz 42] Besondere Beachtung ist stets auch der Frage zu schenken, in welchen Ländern die Auftragsverarbeiter ihren Sitz haben. So gelten beispielsweise die USA, China oder Russland als Länder ohne angemessenes Datenschutzniveau.[85] Verfügt ein Land über kein angemessenes Datenschutzniveau, ist eine Datenübermittlung in dieses Land ohne zusätzliche besondere Vorkehrungen nicht erlaubt. Dabei ist zu beachten, dass die Zugriffsmöglichkeit auf die Daten aus einem solchen Land einer eigentlichen Datenübermittlung gleichzustellen ist. Dies führt dazu, dass sich die Problematik der Datenweitergabe in ein unsicheres Drittland je nach beigezogenem Dienstleister nicht nur bei internationalen Logistikpartnern, sondern durchaus auch schon bei der lokalen Logistik in der EU stellen kann. Im Zusammenhang mit den USA stellt die Zertifizierung im Rahmen des sog. «Privacy-Shield»-Abkommens eine solche besondere (und ausreichende) Vorkehrung dar. Unter dem «Privacy Shield» zertifizieren sich US-Unternehmen selbst und verpflichten sich damit zur Beachtung eines minimalen datenschutzrechtlichen Standards, der demjenigen der Schweiz resp. der EU entspricht.[86] Alternativ zur «Privacy-Shield»-Zertifizierung gibt es die Möglichkeit, einen Datentransfer in ein Drittland mit unzureichendem Datenschutzniveau trotzdem zu ermöglichen. Gemäss der DSGVO können Datenübermittlungen auch erfolgen, wenn der Verantwortliche (vorliegend also der Online-Händler) geeignete, zusätzliche vertragliche Garantien vorsieht.[87] Solche Vertragsklauseln können entweder *ad hoc* vereinbart werden oder es können die sog. EU-Standarddatenschutzklauseln (sog. EU Model Contract Clauses), die von der europäischen Kommission spezifisch für diesen Kontext genehmigt wurden, verwendet werden.[88] In der Regel werden die Klauseln im Rahmen der Auftragsdatenbearbeitungsverträge

80 Vgl. Art. 28 DSGVO.

81 Unter anderem muss sich der Verarbeiter darin zur Vertraulichkeit und zum Ergreifen organisatorischer und technischer Massnahmen für den Schutz der Daten verpflichten, vgl. Art. 28 Abs. 3 DSGVO.

82 DSGVO 2017-Hartung (Fn. 15), Art. 28 N 68–69.

83 Vgl. Art. 28 Abs. 3 lit. a DSGVO.

84 DSGVO 2017-Hartung (Fn. 15), Art. 28 N 56.

85 Länder-Liste des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) vom 12. Januar 2017, abrufbar unter: https://www.nb.admin.ch/dam/snl/de/dokumente/projekte_und_programme/Stand%20des%20Datenschutzes%20weltweit.pdf.download.pdf/12012017_Laenderliste_d.pdf, zuletzt abgerufen am 11. Oktober 2018.

86 Hierbei handelt es sich um ein Übereinkommen zwischen den USA und der Schweiz respektive der EU, vgl. Geppert Nadine, Überprüfung der Modelle zur Datenübermittlung in Drittländer, Zeitschrift für Datenschutz (ZD) 2018, S. 62 ff., hier S. 62 (zit. Geppert).

87 Art. 46 Abs. 2 lit. c und d DSGVO.

88 Geppert (Fn. 86), S. 65.

vereinbart, weshalb die meisten Muster-Auftragsdatenverarbeitungsverträge auch bereits Bestimmungen enthalten, die für datenschutzkonforme Datentransfers in Länder ohne angemessenes Datenschutzniveau notwendig sind.[89]

2. Verwendung der Einkaufsdaten für weitere Zwecke

[Rz 43] In der Regel wollen Online-Händler die erhobenen Kundendaten nicht nur für die Abwicklung einer Bestellung, sondern auch für weitere Zwecke nutzen, die sich zudem über die Zeit verändern können. Dies ist vor dem Hintergrund des datenschutzrechtlichen Grundprinzips der Zweckbindung problematisch, sofern diese weiteren Zwecke nicht von der informierten Einwilligung im Zeitpunkt der Datenerhebung erfasst sind. Wie bereits mehrfach erläutert, muss die betroffene Person zum Zeitpunkt der erstmaligen Datenerhebung über den vollständigen Verwendungszweck informiert sein, wobei dieser Zweck anschliessend grundsätzlich nicht geändert oder beliebig ausgeweitet werden darf.[90] Ob überhaupt eine Zweckänderung vorliegt, hängt massgeblich davon ab, wie weit oder eng der ursprüngliche Zweck auszulegen ist, resp. definiert wurde.[91] Für eine jeweils enge Auslegung spricht das Prinzip der Transparenz, welches verlangt, dass die Zweckbeschreibung eindeutig zu sein hat.[92] Die DSGVO statuiert, dass der Zweck, zu welchem die Daten weiterverarbeitet werden, mit dem ursprünglichen Erhebungszweck grundsätzlich nicht unvereinbar sein darf.[93] Durch diese Rückkopplung an den Erhebungskontext soll gewährleistet werden, dass die personenbezogenen Daten eines Betroffenen nicht für Zwecke verarbeitet werden, mit denen er bei der Erhebung gar nicht rechnen musste (sog. Kompatibilitätstest).[94]

[Rz 44] Möchte ein Online-Shop-Betreiber die Bestelldaten nun beispielsweise in sein CRM überführen und die Daten dort mit anderen, bereits vorhandenen Daten (etwa aus früheren Bestellungen o.ä.) verknüpfen, so müssen die Kunden in einer Datenschutzerklärung darauf hingewiesen werden. Meist wird zudem eine Einwilligung des Kunden für die Überführung notwendig sein, da nur die Speicherung der *Bestell*daten durch den Erlaubnistatbestand des Vertrages nach Art. 6 Abs. 1 lit. b DSGVO abgedeckt wird, nicht aber die *Verknüpfung* und Weiterverwendung der Daten in einem CRM-System.[95]

[Rz 45] Für den datenschutzkonformen Einsatz eines solchen CRM-Systems ist dem dazugehörigen Zugriffsreglement besondere Bedeutung zu schenken. Es muss anhand datenschutzfreundlicher Voreinstellungen sichergestellt werden, dass Mitarbeiter nur auf diejenigen Daten zugreifen können, die für die Erfüllung ihrer jeweiligen Aufgabe erforderlich sind (sog. *need-to-know-*

89 Diese Bestimmungen sind dabei grundsätzlich unverändert zu übernehmen, wobei das Hinzufügen weiterer Klauseln zwar möglich ist, den genehmigten Standarddatenschutzklauseln der Kommission aber nicht widersprechen dürfen, vgl. statt vieler Zerdick Thomas, in: Ehmann/Selmayer (Hrsg.), Datenschutz-Grundverordnung, Kommentar, 2. Aufl. 2018, Art. 46 N 10 (zit. DSGVO 2018-Autor).

90 Thouvenin (Fn. 50), S. 35 ff.

91 Schantz Peter, Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht, Neue Juristische Wochenschrift (NJW) 2016, S. 1841 ff., hier S. 1843–1844 (zit. Schantz); siehe allerdings Thouvenin (Fn. 50), S. 38, wonach eine weite Zweckumschreibung gemäss EU Recht ausgeschlossen sei.

92 Schantz (Fn. 91), S. 1843–1844.

93 Art. 5 Ziff. 1 Iit. b DSGVO, vgl. zum Ganzen Schantz (Fn. 91), S. 1844; DSGVO 2018-Heberlein, Art. 6 N 48.

94 Schantz (Fn. 91), S. 1844; DSGVO 2018-Heberlein, Art. 6 N 48–49.

95 Denkbar wäre selbstverständlich das Vorliegen eines überwiegenden berechtigten Interesses des Online-Händlers, welches das Vorliegen der Einwilligung obsolet machen könnte.

Prinzip).[96] Das Prinzip ist durch ein Berechtigungskonzept umzusetzen, in welchem Zugriffsregeln für einzelne Benutzer oder Benutzergruppen festgelegt werden.[97] Neben diesem unternehmensinternen Aspekt ergeben sich auch bereits aus der Wahl des jeweiligen CRM-Systems grundlegende Anforderungen. Basiert das CRM-System auf einer Cloud-Lösung und befinden sich die Anbieter oder Hoster im Ausland, sind wiederum die Vorgaben für die Übermittlung ins Ausland sowie die Auftragsdatenverarbeitung zu beachten (vgl. Rz. 41 f.).

VI. Fazit

[Rz 46] Aufgrund der technikneutralen Ausgestaltung der datenschutzrechtlichen Gesetze sind die allgemeinen Datenschutzbestimmungen bei der gesamten Customer-Journey im Onlinevertrieb zu beachten. Die datenschutzrechtlichen Pflichten und Aufgaben können in der Regel nicht durch einmaliges Handeln (z.B. Einholen einer Einwilligung, Veröffentlichung einer Datenschutzerklärung etc.) erfüllt und erledigt werden. So muss zum Beispiel bei der Weiterverwendung von Daten und einer allfälligen Zweckänderung sorgfältig geprüft werden, ob die fragliche Datenbearbeitung mit den transparent gemachten Zwecken und Datenbearbeitungshandlungen (noch) kompatibel ist. Allfällige Einwilligungen können an Gültigkeit verlieren bzw. das Einholen einer Einwilligung für gewisse Datenbearbeitungen kann sich plötzlich aufdrängen (z.B. wenn eine bis anhin vorliegende Vertragsbeziehung nicht mehr gelebt wird und somit der Erlaubnistatbestand des Vertrages wegfällt). Datenschutzerklärungen müssen fortlaufend aktualisiert werden (insbesondere wenn neue Auftragsdatenbearbeiter hinzukommen oder neue Technologien in einem Online-Shop eingesetzt werden). Datenschutzrechtliche Aufgaben sind folglich als Daueraufgabe zu betrachten und es ist jeweils fortlaufend zu beurteilen, ob die Datenbearbeitungen im Sinne einer Gesamtbeurteilung immer wieder aufs Neue den gesetzlichen Bestimmungen und Grundsätzen standhalten.

Lukas Bühlmann (LL.M) ist Rechtsanwalt und leitet als Partner die Praxisgruppe Digital, Data Privacy & E-Commerce bei Meyerlustenberger Lachenal AG.

Hatun Metin (MLaw) ist Rechtsanwältin in der Praxisgruppe Digital, Data Privacy & E-Commerce bei Meyerlustenberger Lachenal AG.

96 Statt vieler, vgl. Grützner Thomas / Jakob Alexander, Compliance von A-Z, 2. Aufl. 2015, Buchstabe N.

97 Ob ein korrektes Berechtigungskonzept vorliegt, ist anhand verschiedener Kriterien zu überprüfen, vgl. hierzu z.B. den Fragekatalog von Koreng Ansgar / Lachenmann Matthias, Formularhandbuch Datenschutzrecht, 2. Aufl. 2018, S. 218 ff.