



LOSCHELDER

**Newsletter Datenschutzrecht
November 2018**

Inhalt

**Praktische Hilfestellungen von der Datenschutzkonferenz:
Erste organisatorische und technische Modellmaßnahmen
veröffentlicht**

**Datenschutzkonforme Werbung: neue Orientierungshilfe
der Datenschutzaufsichtsbehörden**

**Neues zum Thema Abmahnungen durch Mitbewerber bei
DSGVO-Verstößen**

**Betroffene können keine bestimmte
Datensicherungsmaßnahme einklagen**

Das Fotografieren unter der DSGVO

Praktische Hilfestellungen von der Datenschutzkonferenz: Erste organisatorische und technische Modellmaßnahmen veröffentlicht

Mit der Datenschutzgrundverordnung geht die Pflicht einher, personenbezogene Daten technisch und organisatorisch risikoangemessen zu schützen und insbesondere auch mit Wegfall einer Verarbeitungserlaubnis zu löschen. Aber was heißt das konkret und wie lässt sich dies praktisch umsetzen? Genügt es, wenn einzelne Datensätze irreversibel unzugänglich gemacht werden oder muss der Datenträger physikalisch zerstört werden? Erste Hilfestellungen für konkrete Umsetzungsmaßnahmen enthalten die im September veröffentlichten sogenannten „Bausteine“, die von den Datenschutzaufsichtsbehörden veröffentlicht wurden.

Die Datenschutzkonferenz, der alle Landes-Datenschutzaufsichtsbehörden angehören, hat im April 2018 eine Erprobungsfassung des an die DSGVO angepassten Standard-Datenschutzmodells („SDM“) beschlossen. Perspektivisch soll das SDM den Verantwortlichen bei der Auswahl und Bewertung organisatorischer und technischer Maßnahmen zur Umsetzung der DSGVO als Vorbild und den Datenschutzaufsichtsbehörden als Blaupause für ihre Prüfungen dienen. Wirkliche Hilfestellungen bieten dabei indes erst die das SDM komplettierenden „Bausteine“, die inhaltliche Vorgaben zu bestimmten Themenfeldern enthalten. Am Ende des Entwicklungsprozess soll ein Maßnahmenpaket aus SDM inklusive aller Bausteine stehen, bei dessen Umsetzung die Verantwortlichen und Datenaufsichtsbehörden von einer Übereinstimmung mit der DSGVO ausgehen dürfen.

Die ersten Erprobungsfassungen solcher „Bausteine“ sind nunmehr im September veröffentlicht worden. der besonders relevanten Frage der Löschung und Vernichtung von Daten (Baustein 60) enthalten sie Modellmaßnahmen zur Aufbewahrung, Planung, Spezifikation, Dokumentation, Protokollierung, Trennung und zum Datenschutzmanagement. So wird dort z.B. konkret festgehalten, welche Maßnahmen für eine datenschutzrechtskonforme Löschung ausreichend sein können (u.a. Überschreiben der Informationen einzelner Datenfelder mithilfe von Löschmodulen, physikalische Zerstörung) und welche nicht (u.a. Austragen aus elektronischen Verzeichnissen, Formatieren von Datenträgern, Freigabe von Datenträgern zur Wiederverwendung durch Organisationsanweisung). Hinsichtlich der notwendigen Dokumentation der Datenschutzkonformität im Unternehmen erläutert ein eigener Baustein (Nr. 42), dass diese – strukturiert – schriftlich oder elektronisch erfolgen kann und in angemessenem Umfang vollständig und revisionsfest sowie aktuell sein muss.

Vorerst dienen die Bausteine als unverbindliche Orientierungshilfe. Erst mit dem Abschluss der Erprobung und Abstimmung mit der Konferenz der unabhängigen Datenschutzaufsichtsbehörden können sie zur „verbindlichen“ Empfehlung werden (die indes gerichtlich überprüfbar bleiben).

Die Erprobungsfassungen von SDM und den bereits vorliegenden Bausteinen sind abrufbar unter: <https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/>



Datenschutzkonforme Werbung: neue Orientierungshilfe der Datenschutzaufsichtsbehörden

Eine Verarbeitung personenbezogener Daten ist auch zu Werbezwecken nur zulässig, wenn eine Erlaubnisnorm greift. In Betracht kommen regelmäßig eine Einwilligung oder ein berechtigtes Interesse des werbenden Unternehmens. Wann genau ein solches vorliegt, wann eine Einwilligung wirksam ist, welche Informationen rund um die Datenverarbeitung gegeben werden müssen und welche technischen und organisatorischen Maßnahmen angemessen sind, ist Gegenstand umfassender Diskussionen – an einer stetigen Behördenpraxis oder gar klärender Rechtsprechung fehlt es bislang. Die insoweit bestehenden Rechtsunsicherheiten werden durch die am 7. November veröffentlichte Orientierungshilfe der Aufsichtsbehörden zur Verarbeitung von personenbezogenen Daten für Zwecke der Direktwerbung unter Geltung der Datenschutz-Grundverordnung (DSGVO) nunmehr reduziert.

Mangels spezieller Vorschriften zur Verarbeitung von personenbezogenen Daten zu Werbezwecken richten sich die Anforderungen nach den allgemeinen Grundsätzen der DSGVO, d.h. vereinfacht und abstrakt, entweder liegt eine Einwilligung des Betroffenen vor oder die Interessenabwägung fällt gemäß Art. 6 Abs. 1 lit. f DSGVO zugunsten der Verarbeitung zu Werbezwecken aus. Welche konkreten Anforderungen zu erfüllen sind und welche Besonderheiten es nach Ansicht der Datenschutzkonferenz zu beachten gilt, konkretisiert der Leitfaden. Interessierte können sich unter anderem informieren, welche Anforderungen an die Einwilligung und deren Gestaltung gestellt werden, welche Informationspflichten bestehen und wie mit einem Bewerberspruch

und einem Wunsch nach Datenlöschung umzugehen ist. Die Orientierungshilfe ist zwar kein verbindliches Dokument, verdeutlicht aber die Position der Aufsichtsbehörden und damit, wann mit einem Einschreiten dieser zu rechnen ist.

Hervorzuheben, da durchaus diskutabel, ist insbesondere die Position der Datenschutzaufsichtsbehörden zur Angabe von Löschfristen und dem Datenumgang im Fall eines Widerspruchs: Die Aufsichtsbehörden tendieren dahin, dass personenbezogene Daten nicht zeitlich unbegrenzt bis zu einem Widerspruch verarbeitet werden dürfen, sondern es eine „Höchstfrist“ geben müsse, jedenfalls im Fall längerer Werbepausen (beispielhaft angeführt wird eine Pause über 17 Monate). Zudem scheinen sie im Fall eines begründeten Widerspruchs – trotz anders lautendem Wortlaut der DSGVO – anstatt der sofortigen Löschung der Daten ihre Überführung in eine „Werbesperrdatei“ zu befürworten, die sicherstellen soll, dass derselbe Adressat nicht kurze Zeit später erneut Werbung unter Verweis auf Art. 6 Abs. 1 lit. f DSGVO erhält (da im Unternehmen nach Löschung nicht mehr bekannt ist, dass ein Widerspruch ausgesprochen wurde).

Erfreulich ist dagegen u.a. die Unterstützung für ein zweistufiges Informationsmodell (mit Basisinformationen z.B. auf einer Bestellpostkarte, die dann auf eine umfassende Information auf der Homepage verweist) und die Bestätigung, dass postalische Werbung oftmals ohne Einwilligung auf Grundlage des Art. 6 Abs. 1 lit. f DSGVO zulässig ist.

Die Orientierungshilfe ist abrufbar unter: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/11/OH_Werbung_Stand_07.11.2018.pdf



Neues zum Thema Abmahnungen durch Mitbewerber bei DSGVO-Verstößen

Wieder einmal beschäftigen die Gerichte die Abmahnfähigkeit von Verstößen gegen die Informationspflichten der Art. 13 und 14 DSGVO (Datenschutzerklärungen). Wir berichteten in der letzten Ausgabe von den divergierenden Urteilen der Landgerichte Bochum und Würzburg ([Newsletter Oktober 2018](#)). Diesmal hat sich ein Oberlandesgericht, das OLG Hamburg, in seinem Urteil für die grundsätzliche Abmahnfähigkeit ausgesprochen. Die Stimmen zugunsten einer Abmahnfähigkeit bestimmter DSGVO-Verstöße erhalten mit diesem Urteil eine gewichtige Unterstützung (zur Erinnerung: teils wird mit Blick auf das ausdifferenzierte Instrumentarium der DSGVO eine Abmahnfähigkeit von Verstößen insgesamt verneint).

Die Entscheidung bezog sich erneut auf eine unzureichende Datenschutzerklärung; Details sind bislang noch nicht öffentlich zugänglich. Abmahnfähig ist allerdings auch nach den Befürwortern dieser Position nicht jeder Verstoß gegen Vorschriften der DSGVO. Bei der in Rede stehenden datenschutzrechtlichen Bestimmung muss es sich um eine Marktverhaltensregel im Sinne von § 3a UWG handeln. Es bleibt damit bei den Grundsätzen, die auch unter der alten Rechtslage die Abmahnfähigkeit von datenschutzrechtlichen Verstößen bestimmt haben. Es bedarf für jede einzelne Vorschrift der DSGVO einer Beurteilung, ob sie eine solche Marktverhaltensregelung darstellt – für die Informationspflichten aus Art. 13, 14 DSGVO gegenüber Besuchern einer Homepage spricht einiges dafür. Bis eine gefestigte Rechtsprechung und somit Rechtssicherheit in dieser Frage vorliegt, wird allerdings noch einige Zeit vergehen.

Urteil des OLG Hamburg vom 25. Oktober 2018, Az.: 3 U66/17 – noch nicht veröffentlicht



Betroffene können keine bestimmte Datensicherungsmaßnahme einklagen

Im September 2018 haben die österreichischen Datenschutzbehörden eine interessante Entscheidung zu dem Umfang von Betroffenenrechten veröffentlicht. Nach ihrer Ansicht verleihen die Verpflichtungen zur Datenverarbeitungssicherheit aus Art. 32 DSGVO Betroffenen kein gegen den Verantwortlichen einklagbares (subjektives) Recht auf Einhaltung bestimmter Maßnahmen. Die Rechte der Betroffenen beschränkten sich auf die Art. 12 ff. DSGVO aufgeführten Rechte auf Information, Auskunft, Löschung usw. Die sonstigen objektiven Pflichten in den anderen Kapiteln der DSGVO trafen allein die Verantwortlichen und könnten allenfalls von den Behörden angeordnet werden.

Die Betroffene machte in ihrer Beschwerde ein Recht zur Pseudonymisierung geltend. Sie sah sich in ihrem Recht auf Geheimhaltung (potenziell) verletzt. Die Verantwortlichen speicherten Daten zu dem Sexualleben und der Gesundheit der Betroffenen in elektronischer Form ohne Pseudonymisierung. Die Betroffene befürchtete, dass ihre Daten unbeabsichtigt veröffentlicht werden könnten, zum Beispiel nach einem Hackerangriff, und eine Identifizierung ihrer Person in einem solchen Fall möglich wäre. Eigentlich begehrte die Betroffene eine Datenlöschung, die die Verantwortlichen aber verweigerten. Als Alternative verlangte sie zumindest eine Abtrennung ihrer Daten dergestalt, dass aus den verbleibenden Daten alleine nicht mehr auf ihre Identität geschlossen werden kann (Pseudonymisierung). Diese konkrete Datensicherungsmaßnahme – so die Behörde – könnte sie von Amts wegen anordnen, die Betroffene könne sie indes nicht verlangen.

Für die Praxis ist diese Entscheidung hilfreich: Sie beschränkt Betroffene auf die enumerativ aufgezählten – weitreichenden – Rechte der Art. 12 ff. DSGVO. Ein anderes Verständnis mit dem Recht Betroffener, spezifische Umsetzungsmaßnahmen aufgrund anderer Regelungen der DSGVO zu verlangen, hätte für die datenverarbeitenden Unternehmen verheerende Folgen – so könnte im obigen Beispiel z.B. eine einheitliche Handhabung der Datensätze unmöglich werden, wenn ein Betroffener die Pseudonymisierung durch Abtrennung verlangte, ein anderer eine besondere Form der Verschlüsselung und ein Dritter wiederum die Belegenheit nur auf Servern in einem Rechenzentrum vor Ort. Die Entscheidung ist auch inhaltlich überzeugend, da die DSGVO mit den Art. 12 ff. DSGVO und dem Beschwerderecht Betroffener ein hinreichendes Schutz-Instrumentarium bereithält.

Die Entscheidung ist abrufbar unter

http://www.ris.bka.gv.at/Dokumente/Dsk/DSBT_20180913_DSB_D123_070_0005_DSB_2018_00/DSBT_20180913_DSB_D123_070_0005_DSB_2018_00.pdf



Das Fotografieren unter der DSGVO

Fotografieren in Zeiten der DSGVO – bisher und sicherlich auch in Zukunft ein datenschutzrechtlicher Dauerbrenner. Erste Gerichts- und Behördenentscheidungen tragen jedoch zur Rechtssicherheit bei. So hat sich das OLG Köln im Juni mit dem Verhältnis zwischen DSGVO und Kunsturhebergesetz auseinandergesetzt (OLG Köln, Beschl. v. 18.06.2018 – Az.: 15 W 27/18). Jüngst hat sich auch der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg (LfDI) umfassend zu dieser Thematik geäußert (abrufbar unter: <https://www.baden-wuerttemberg.datenschutz.de/faq-fotografieren-und-datenschutz-wir-sind-im-bild/>).

Fotografien, die Menschen abbilden und nicht ausschließlich für den persönlichen oder familiären Gebrauch verwendet werden, fallen als personenbezogene Daten in den Anwendungsbereich der DSGVO. Die Erstellung, Verwendung und Veröffentlichung der Bilder muss daher datenschutzrechtlich erlaubt sein.

Für die **Anfertigung** der Bilder kommen zunächst die allgemeinen Erlaubnisnormen der DSGVO in Betracht. Ein mögliches – zurzeit wegen vermeintlich geringen Rechtsrisikos sehr gängiges - Vorgehen ist das Einholen von Einwilligungen der abgebildeten Personen. Für ihre Wirksamkeit bedarf es einer freiwilligen Abgabe; zudem entfalten sie nur solange rechtfertigende Wirkung wie sie nicht widerrufen worden sind. Eine Einwilligung muss nicht zwingend schriftlich eingeholt werden, sondern kann auch konkludent, z.B. durch Lächeln oder Posieren in die Kamera erfolgen. Rechtliche Schwierigkeiten können sich ergeben, weil nachzuweisen ist, dass eingewilligt wurde und die Rechtsbelehrung stattgefunden hat.

In vielen Fällen sind Einwilligungen allerdings wenig praktikabel, so dass andere Rechtsgrundlagen erwogen werden müssen. Handelt es sich bei dem Abgebildeten um den Vertragspartner, z.B. Auftragsfoto-

grafie, so kann auf die Erlaubnis zur Durchführung eines Vertrages zurückgegriffen werden. Von weitaus wichtigerer Bedeutung ist die Erlaubnis zur Datenverarbeitung aus berechtigtem Interesse (Art. 6 I 1 lit. f DSGVO). Nicht nur die grundrechtlich geschützte und garantierte Meinungs- und Informationsfreiheit, auch unternehmerische Interessen an der Dokumentation und Selbstdarstellung können als berechtigtes Interesse geltend gemacht werden – notwendig ist eine Interessenabwägung im Einzelfall, wobei die vernünftigen Erwartungen des Abgebildeten ausschlaggebend sind.

Für die **Veröffentlichung** von Bildmaterial kommt nach Rechtsauffassung des OLG Köln das Kunsturhebergesetz (KUG) in Betracht, wonach es ausnahmsweise – in den in § 23 KUG genannten Fällen – keiner Einwilligung bedarf. Demnach müssen insbesondere Personen, die als „Beiwerk“ der Umgebung oder als Teilnehmer einer Menschenmenge wie einer Versammlung auf einer Aufnahme gezeigt werden, nicht in die Veröffentlichung einwilligen. Der LfDI spricht sich im Gegensatz zum OLG Köln nicht unmittelbar für die Anwendbarkeit des KUG aus, hält den Streit jedoch für wenig relevant, da die Wertungen des KUG jedenfalls bei der Interessenabwägung des Art. 6 I 1 lit. f DSGVO zu berücksichtigen seien.

Ein Dauerthema bleibt die **Betroffeneninformation**, die den Verantwortlichen gerade bei einer unüberschaubaren Menschenmenge vor Herausforderungen stellen kann. Aus Sicht des LfDI ist es in solchen Situationen ausreichend, die Informationen beispielsweise über Ausgänge der Öffentlichkeit zugänglich zu machen, da wie bei einer heimlichen Datenerhebung die individuelle Information unmöglich oder mit unverhältnismäßigem Aufwand verbunden wäre.



**Für alle weiteren Fragen rund um das Datenschutzrecht
stehen Ihnen gerne zur Verfügung**



Dr. Kristina Schreiber
+49(0)221 65065-337
kristina.schreiber@loschelder.de



Dr. Simon Kohm
+49(0)221 65065-200
simon.kohm@loschelder.de

Impressum

LOSCHELDER RECHTSANWÄLTE

Partnerschaftsgesellschaft mbB

Konrad-Adenauer-Ufer 11

50668 Köln

Tel. +49 (0)221 65065-0, Fax +49 (0)221 65065-110

info@loschelder.de

www.loschelder.de