



**LOSCHELDER**

**Newsletter Datenschutzrecht  
April 2019**

## **Inhalt**

**Tracking-Cookies: Anforderung an die Einwilligung**

**BVerwG zur Videoüberwachung – es bleibt beim Alten**

**Abmahnungen wegen fehlender SSL/TLS-Verschlüsselungen**

**Reichweite und Beschränkungen des Auskunftsanspruchs  
nach Art. 15 DSGVO**

**DSK: Facebook Fanpages rechtswidrig**

## Tracking-Cookies: Anforderung an die Einwilligung

Ende März veröffentlichte der Generalanwalt am EuGH seine Schlussanträge in der [Rechtssache](#) Planet 49 (C-673/17) zu den datenschutzrechtlichen Anforderungen an die Verwendung von sog. Tracking-Cookies, wie sie beispielsweise Google Analytics verwendet. Auch die deutschen Datenschutzbehörden haben sich zu diesem Thema jüngst erneut positioniert, sodass es empfehlenswert ist, den Einsatz von Tracking-Cookies auf der eigenen Homepage zu überprüfen.

Die Besonderheit von Tracking-Cookies liegt in zwei Aspekten: Zum einen werden diese Cookies längerfristig auf den Endgeräten der Website-Besucher gespeichert, ggf. über Wochen, Monate oder sogar Jahre. Zum anderen ermöglichen diese Cookies die Nachverfolgbarkeit des individuellen Nutzerverhaltens, in der Regel website-übergreifend. So helfen sie bei der gezielten Werbeansprache oder auch bei der Optimierung der eigenen Website, wenn Besuchintervalle u.ä. besser analysiert werden können. Der Generalanwalt bestätigte in den Schlussanträgen zu Planet 49 in zident, dass es sich bei den Cookies und daraus generierten Informationen um personenbezogene Daten handelt. Bereits im April 2018 positionierten sich die deutschen Aufsichtsbehörden kritisch gegen die Verwendung solcher Tracking-Cookies ohne Einwilligung. Nach den Schlussanträgen und den letzten Veröffentlichungen der deutschen Aufsichtsbehörden zeichnet sich eine differenziertere Positionierung ab:

- a. Tracking-Cookies für passgenaue Werbung oder für detaillierte Profile des Surfverhaltens einzelner Nutzer dürfen nur nach aktiver, individueller Einwilligung eingesetzt werden – unwirksam sind Einwilligung über voreingestellte Kästchen oder Cookie-Banner, bei denen vorgesehen ist, dass „durch Nutzung der Website“ das Einverständnis mit der Verwendung von Tracking-Cookies erklärt wird;
- b. Tracking-Cookies, die für Webanalysen eingesetzt werden, um die eigene Seite zu optimieren, die Website-Sicherheit zu erhöhen oder die Reichweite zu messen, können aus berechtigten Interessen ohne Einwilligung zulässig sein;
- c. über den Einsatz von Tracking-Cookies muss transparent und umfassend informiert werden, gerade auch in Einwilligungsfällen.

Im Einzelnen dazu:

## **1. Tracking-Cookies mit und ohne Einwilligung**

Über Cookies werden personenbezogene Daten verarbeitet. Dies ist bekanntlich nur zulässig, wenn ein Erlaubnistatbestand existiert. Für den Einsatz von Tracking-Cookies kommen insbesondere zwei Erlaubnistatbestände in Betracht – eine Einwilligung oder berechtigte Interessen ihres Verwenders. Die Schlussanträge des Generalanwalts sowie die jüngsten Positionierungen der deutschen Aufsichtsbehörden differenzieren nunmehr zwischen den verschiedenen Zwecken, zu denen Tracking-Cookies verwendet werden sowie dem Umfang, zu dem sie Daten von Nutzern erheben und verarbeiten.

Werden Tracking-Cookies dazu eingesetzt, Nutzern zielgerichtete Werbung zu präsentieren, ist dies nach den Schlussanträgen des Generalanwalts wohl nur noch mit Einwilligung des jeweiligen Nutzers zulässig. Dies gilt auch, wenn website-übergreifend detaillierte Surf-Profile eines Nutzers erstellt werden. Der Generalanwalt plädiert für eine klare Opt-In-Lösung beim Einsatz von Tracking-Cookies für nutzerdatenbasierte Werbung.

Allerdings muss nicht in jede Webanalyse durch Tracking-Cookies eingewilligt werden: Webanalysen zur Website-Optimierung, Erhöhung der Website-Sicherheit oder Reichweitenmessung können aus einem überwiegenden berechtigten Interesse des Website-Betreibers erlaubt sein. Nach der Berliner BDI besteht an der Analyse zur Reichweitenmessung oder Optimierung bzw. Sicherheit der Website regelmäßig ein überwiegendes berechtigtes Interesse des Website-Betreibers (Art. 6 Abs. 1 lit. f) DSGVO), wenn nicht das Surfverhalten der Nutzer detailliert dokumentiert und verfolgt wird.

## **2. Wirksame Einwilligung nur bei aktivem Tun**

Ist nun eine Einwilligung erforderlich, stellt sich die Frage nach den konkreten Anforderungen hieran. Im Markt werden bislang auch Tracking-Cookies meist noch ohne Einwilligung eingesetzt – eingeführt wurden lediglich weitgehend flächendeckend sog. „Cookie-Banner“, über die beim Besuch einer Website auf die Verwendung von Cookies hingewiesen wird. Formuliert sind diese i.d.R. entweder als „Widerspruchslösung“ mit dem Hinweis, dass die Verwen-

dung von Cookies etwa über die Browser-Einstellungen verhindert werden kann. Teils wird dagegen postuliert, dass sich der Nutzer mit dem Besuch der Website damit einverstanden erklärt, dass Cookies gesetzt werden: Diese Cookie-Banner sind so formuliert, dass sie auf eine Einwilligung hindeuten – allerdings kann der Website-Besucher weder entscheiden, für welche Cookies dies genau gilt, noch die Website ohne Cookies nutzen.

Wenn es nun nach den Schlussanträgen des Generalanwalts geht (der EuGH folgt diesen zumeist), sind derartige „Einwilligungen“, die allgemein durch den Website-Besuch abgegeben werden oder etwa in Ankreuzkästchen voreingestellt sind, unwirksam. Um Freiwilligkeit anzunehmen, ist laut der Schlussanträge erforderlich, dass die Einwilligung eine aktive Willensbekundung darstellt und gesondert erfolgt (Art. 4 Nr. 11, Erwägungsgrund 32 DSGVO). Der Nutzer müsse gesondert (durch einen „eigenen“ Klick) einwilligen; die Einwilligung dürfe nicht mit anderen Bestätigungen, z.B. der Teilnahme am Gewinnspiel, zusammen erfolgen. Dahingehend äußerte sich auch die Berliner BDI in ihrem [Jahresbericht 2018](#) (S. 150) und die Datenschutzkonferenz (DSK) in ihrer [Orientierungshilfe](#) für Anbieter von Telemedien (S. 5). Letztlich überrascht dies nicht: Eine wirksame Einwilligung erfordert regelmäßig ein aktives Tun, Einwilligungen dürfen nur im Ausnahmefall an eine andere Leistung – etwa das Website-Angebot oder eine Gewinnspielteilnahme – gekoppelt sein.

Zum Hintergrund: Anlass für die Schlussanträge war eine Vorlage des BGH an den EuGH. Der BGH hat in einem Verfahren die Wirksamkeit von Einwilligungen in die Verwendung von Tracking-Cookies durch den Online-Gewinnspielveranstalter Planet 49 zu beurteilen. Planet 49 hatte die Einwilligung in Ankreuzkästchen voreingestellt, sodass Nutzer, wenn sie nicht aktiv widersprachen (durch „Wegklicken“ des voreingestellten Hakens), mit Bestätigung der Teilnahme auch der Verwendung von Tracking-Cookies zustimmten. Dies aber ist letztlich eine Widerspruchslösung (Opt-Out) und keine wirksame Einwilligung.

### **3. Wirksame Einwilligung nur bei ausreichender Information**

Wirksam kann eine Einwilligung im Sinne von Art. 6 Abs. 1 lit. a) DSGVO ferner nur sein, wenn sie freiwillig und in Kenntnis der Sachlage erfolgt (Art. 4 Nr. 11, Art. 7 DSGVO). Die Informationen über die Verarbeitung personenbezogener Daten sollten jedenfalls

vollumfänglich die Vorgaben der DSGVO einhalten; so sieht es auch die Datenschutzkonferenz (DSK) in ihrer [Orientierungshilfe](#) (S. 5). Diskutiert wird dies, da das Zusammenspiel zwischen DSGVO, e-Privacy Richtlinie und TMG höchst komplex ist; für eine Erleichterung der Informationspflichten ist aber kaum etwas ersichtlich, in der Praxis sollte eine umfassende Information erfolgen (weiter zu dem Zusammenspiel zwischen e-Privacy Richtlinie und DSGVO [hier](#)).

Klare und umfassende Informationen beinhalten nach Ansicht des Generalanwalts neben Informationen über den Zweck und die Funktionsweise auch Informationen dazu, wie lange die Cookies die Daten (nicht nur personenbezogene) sammeln und ob Dritte Zugriff auf die Daten erhalten. Wird Dritten Zugriff gewährt, muss deren Identität offengelegt werden. Nur wenn auch über vorhandene oder fehlende Zugriffsmöglichkeiten Dritter informiert würde, könne der Nutzer die Konsequenzen seiner Einwilligung erkennen. Es bleibt abzuwarten, ob sich der EuGH den Schlussanträgen seines Generalanwalts anschließt. In den von uns entworfenen Datenschutzerklärungen haben wir auch bisher schon empfohlen, jeweils Cookie-spezifisch die Speicherdauer und Zugriffsmöglichkeiten anzugeben.

Konkretere Hinweise zu den Anforderungen an die Betroffeneninformation bei Verwendung von Tracking-Cookies gibt auch die Orientierungshilfe der DSK. Demnach ist insbesondere, wenn bei der betroffenen Person erhobene Daten von dem jeweiligen Diensteanbieter (inkl. eingebundener Dienste) website-übergreifend zusammengeführt und ausgewertet werden, folgendes zu berücksichtigen: Für eine wirksame Einwilligung müssen die betroffenen Personen vorab über jegliche Form der durchgeführten Datenverarbeitung sowie sämtliche Empfänger ausführlich informiert werden und die Möglichkeit erhalten, in die einzelnen Formen der Datenverarbeitung spezifisch einzuwilligen. Gemeinsam Verantwortliche müssen genannt und die Verarbeitungsaktivitäten der einzelnen Organisationen hinreichend beschrieben werden.



## **BVerwG zur Videoüberwachung – es bleibt beim Alten**

*Ein interessantes [Urteil](#) zur Videoüberwachung und dem zeitlichen Anwendungsbereich der DSGVO füllte das Bundesverwaltungsgericht („BVerwG“) Ende März. Das Urteil ist bisher nicht veröffentlicht, aber die ausführliche Pressemitteilung gibt die tragenden Urteilsgründe wieder: Nur eine „erforderliche“ Videoüberwachung ist auch zulässig; es ist Sache desjenigen, der die Überwachung nutzt, seine berechtigten Interessen daran darzulegen und nachzuweisen. Die Aufsichtsbehörden und Gerichte haben dies im hier entschiedenen Fall strikt überprüft.*

Folgender Sachverhalt lag der Entscheidung zugrunde: Die Klägerin betreibt eine Zahnarztpraxis. Ihre Praxis kann durch Öffnen der Eingangstür ungehindert betreten werden, auch, wenn der Empfangstresen nicht besetzt ist. Die Zahnärztin hatte oberhalb dieses Tresens eine Videokamera angebracht, deren Bilder in Echtzeit auf Monitoren in den Behandlungszimmern angezeigt werden (sog. Kamera-Monitor-System). Die Landesdatenschutzbeauftragte verlangte, die Videokamera so auszurichten, dass der Patienten und sonstigen Besuchern zugängliche Bereich vor dem Empfangstresen, der Flur zwischen Tresen und Eingangstür und das Wartezimmer nicht mehr erfasst werden. Das BVerwG hatte zu entscheiden, ob dies tatsächlich geboten war.

Dabei maß das Bundesverwaltungsgericht die Videoüberwachung nicht an den Vorgaben der erst seit dem 25. Mai 2018 geltenden DSGVO, sondern an dem Bundesdatenschutzgesetz (BDSG) alter

Fassung. Auch wenn das Urteil zur alten Rechtslage erging, ist es aber für die Auslegung der DSGVO hilfreich: Denn sowohl § 6b Abs. 1 BDSG a.F., als auch der heute für Videoüberwachungen regelmäßig relevante Erlaubnistatbestand des überwiegenden berechtigten Interesses nach Art. 6 Abs. 1 lit. f) DSGVO setzen voraus, dass die Verarbeitung zur Wahrnehmung der berechtigten Interessen erforderlich ist. Damit lassen sich dem Urteil Hinweise entnehmen, welche Argumente für die Erforderlichkeit einer Videoüberwachung sprechen können.

Zulässig ist eine Videoüberwachung mithin regelmäßig nur, wenn die Beobachtung und ggf. auch Speicherung durch ein Kamera-Monitor-System zur Wahrnehmung berechtigter Interessen erforderlich ist und schutzwürdige Interessen der Betroffenen nicht überwiegen. Dies muss sowohl für die Beobachtung als solche als auch für die konkrete Dauer einer etwaigen Speicherung gesondert beurteilt werden.

Vorliegend hatte die Zahnärztin bereits nicht ausreichend dargelegt, auf die Videoüberwachung angewiesen zu sein; tatsächliche Anhaltspunkte, dass Personen die Praxis betreten könnten, um Straftaten zu begehen, lagen nicht vor. Auch sei die Videoüberwachung nicht notwendig, um Patienten, die nach der Behandlung aus medizinischen Gründen noch einige Zeit im Wartezimmer sitzen, in Notfällen betreuen zu können. Damit fehlte es schon an einem hinreichend gewichtigen, berechtigten Interesse der Zahnärztin an der Videoüberwachung.

Auch unter der DSGVO verdeutlicht die Entscheidung zweierlei: Zum einen ist es stets Sache desjenigen, der eine Videoüberwachung nutzt, seine berechtigten Interessen hieran darzulegen und nachzuweisen; die DSGVO sieht dies explizit vor mit der von ihr vorgeschriebenen allgemeinen Rechenschaftspflicht und speziellen Dokumentationspflicht bei Rückgriff auf Art. 6 Abs. 1 lit. f) DSGVO. Zum anderen lässt bereits die Pressemitteilung erkennen, dass die Gerichte die Berechtigung derartiger Interessen strikt nachprüfen werden.



## **Abmahnungen wegen fehlender SSL/TLS-Verschlüsselungen**

*[Berichten](#) zufolge hat die Interessengemeinschaft Datenschutz e.V. („IGD“) im Frühjahr dieses Jahres 31 Website-Betreiber wegen fehlender SSL-Verschlüsselungen abgemahnt. Sie wurden zu der Abgabe einer strafbewehrten Unterlassungserklärung sowie dem Ersatz von Abmahnkosten in Höhe von 285,60 Euro inkl. MwSt. aufgefordert. Abgemahnt wurde der Umstand, dass die auf den Websites unterhaltenen Kontaktformulare personenbezogene Daten unverschlüsselt übermittelten. Erstaunlich ist hierbei auch, dass ein erst kurz zuvor gegründeter Verein die Abmahnungen aussprach – ob dieser hier wirklich aktiolegitimiert ist, wird zu Recht angezweifelt.*

Für gewerbliche Website-Betreiber dürfte die Pflicht zur Verschlüsselung ihrer Websites durch SSL- oder TLS-Zertifikate eigentlich nichts Neues sein. Sie waren bereits nach § 13 Nr. 7 Telemediengesetz dazu verpflichtet, den Datenverkehr ihrer Website wirksam zu verschlüsseln. Seit Inkrafttreten der DSGVO sind Website-Betreiber nun auch gemäß Art. 25 DSGVO verpflichtet, die technisch-organisatorischen Maßnahmen zu ergreifen, die zur Gewährleistung eines angemessenen Schutzniveaus im Sinne von Art. 32 Abs. 1 DSGVO erforderlich sind. Danach ist der Verantwortliche verpflichtet, bei der Verarbeitung von personenbezogenen Daten durch die Website ein angemessenes Schutzniveau zu gewährleisten. Dies gilt insbesondere auch dann, wenn der Website-Betreiber Vorrichtungen wie Eingabemasken einrichtet, in die Kunden ihre Daten

eingeben und an den Verantwortlichen übermitteln. Eine SSL- oder TLS- Verschlüsselung gewährleistet i.d.R. ein solches Schutzniveau.

Im Fall des IGD e.V. ist allerdings durchaus fraglich, ob dieser aktivlegitimiert ist – die DSGVO hat die Aktivlegitimation auch von Vereinen erweitert (vgl. Art. 80 DSGVO, vgl. auch § 8 Abs. 3 Nr. 2 UWG). Nach [Berichten](#) hat der IGD e.V. in Reaktion auf anwaltliche Drohungen, die Berechtigung vor Gericht feststellen zu lassen, auf die weitere Geltendmachung der Ansprüche verzichtet.



### **Reichweite und Beschränkungen des Auskunftsanspruchs nach Art. 15 DSGVO**

*Ende Dezember 2018 erging ein Urteil des Landesarbeitsgerichts Baden-Württemberg, in dem es auch zur Reichweite und zu Beschränkungen des Auskunftsanspruchs aufgrund von Geheimhaltungsinteressen Dritter (hier Whistleblower) Stellung bezog. Die Fragen der Reichweite des Auskunftsanspruchs aus Art. 15 DSGVO und etwaiger Einschränkungen sind Fragen von grundsätzlicher Bedeutung – das LAG hat angesichts dessen auch die Revision zugelassen. Wir haben hieraus für Sie die Aussagen des LAG zur Reichweite des Auskunftsanspruchs nebst der Verteidigungsmöglichkeiten Auskunftspflichteter aufbereitet. Die Implikationen dieses Urteils im Arbeits- und Beschäftigtendatenschutzrecht werden im Newsletter Arbeitsrecht aufbereitet werden (Anmeldung dazu [hier](#)).*

Zu entscheiden hatte das LAG Baden-Württemberg (Az. 17 Sa 11/18) u.a. über einen Auskunftsanspruch nach Art. 15 DSGVO, den der Kläger – eine Führungskraft des Stuttgarter Autokonzerns Daimler – neben anderen Aspekten geltend gemacht hatte. Das für interne Ermittlungen bei Daimler zuständige Business Practises Office (BOP) hatte auf Grundlage von Hinweisen Dritter gegen den Kläger ermittelt und einen Regelverstoß festgestellt. Der Kläger verlangte im Zuge eines Kündigungsschutzstreits nun Auskunft über „Verhaltens- und Leistungsdaten“, die in der BOP-Akte gespeichert waren. Außerdem begehrte er eine Kopie dieser Daten. Der Autokonzern verweigerte die Erfüllung der Ansprüche mit der Begründung, hierdurch werde die Identität von Hinweisgebern offengelegt.

Das LAG hielt nun mit allgemeiner Bedeutung für den Auskunftsanspruch aus Art. 15 DSGVO zunächst fest, dass die Geltendmachung eines solchen Anspruchs keine detaillierte Auflistung der personenbezogenen Daten erfordert, über die Auskunft oder von denen eine Kopie verlangt wird: „Es ist einem Auskunftsanspruch [...] immanent, dass der Anspruchsteller noch nicht die genauen Gegenstände seiner Auskunft kennt, die er erst einfordert. Eine weitere Konkretisierung ist dem Kläger nicht möglich, weil er nicht weiß, welche Daten die Beklagte über ihn verarbeitet.“

Sodann unterscheidet es gemäß der Struktur des Art. 15 DSGVO zwischen der Auskunftserteilung als solcher, deren Inhalt sich aus Art. 15 Abs. 1 Hs. 2 DSGVO ergibt, sowie der nach Abs. 3 der Vorschrift daneben zu übermittelnden Kopie. Dieses im Ausgangspunkt umfassende Auskunftsrecht kann durch berechtigte Interessen Dritter an einer Geheimhaltung eingeschränkt sein, wenn und soweit diese höherrangig zu gewichten sind (§ 34 Abs. 1 i. V. m. § 29 Abs. 1 S. 2 Bundesdatenschutzgesetz – BDSG). Die BDSG-Regelungen beruhen auf der Öffnungsklausel des Art. 23 Abs. 1 lit. i) DSGVO, wonach das Auskunftsrecht Betroffener zum Schutz der Rechte und Freiheiten anderer Personen beschränkt werden darf. Es ist damit eine Einzelfallabwägung zwischen dem Geheimhaltungsinteresse einerseits und dem Auskunftsinteresse andererseits vorzunehmen.

Von wesentlicher Bedeutung ist hierbei, dies bestätigt das LAG-Urteil, dass diese Einzelfallabwägung vom Verantwortlichen detailliert durchgeführt und dokumentiert wird; pauschale Aussagen genügen nicht, der Verantwortliche muss konkrete Sachverhalte

benennen, anhand derer geprüft werden kann, ob durch eine Auskunftserteilung tatsächlich Rechte und Freiheiten anderer Personen beschränkt würden. Eine Verweigerung von Auskunftserteilung oder auch Herausgabe (Kopie) insgesamt ist regelmäßig nicht zulässig; schützenswerte Daten Dritter können oftmals auch geschwärzt werden.

Die arbeitsrechtlichen Aspekte dieses Urteils einschließlich des Beschäftigtendatenschutzrechts werden im Newsletter Arbeitsrecht noch detailliert aufbereitet werden; für diesen können Sie sich [hier](#) registrieren.



### **DSK: Facebook Fanpages rechtswidrig**

*Facebook Fanpages stehen seit einiger Zeit in der datenschutzrechtlichen Kritik, da die Datenverarbeitung durch Facebook undurchsichtig bleibt. Nach dem EuGH-Urteil und Ermahnungen von der Datenschutzkonferenz (DSK) hatte Facebook im vergangenen Jahr zwar nachgebessert und die Nutzungsbedingungen für Fanpages um einen Abschnitt zur gemeinsamen Verantwortlichkeit ergänzt. Die DSK hat sich dazu indes jüngst negativ positioniert: Die bisherigen Änderungen reichen nicht. Danach ist ein datenschutzkonformer Betrieb von Fanpages derzeit letztlich nicht möglich. In der Verantwortung sind dabei auch die Fanpage-Betreiber selbst.*

„Sowohl Facebook als auch die Fanpage-Betreiber müssen ihrer Rechenschaftspflicht nachkommen. Die DSK erwartet, dass Facebook entsprechend nachbessert und die Fanpage-Betreiber ihrer Verantwortlichkeit entsprechend gerecht werden. Solange diesen Pflichten nicht nachgekommen wird, ist ein datenschutzkonformer Betrieb einer Fanpage nicht möglich.“ So schließt das Positionspapier der deutschen Datenschutzaufsichtsbehörden. Dass Fanpage-Betreiber selbst auch für die Verarbeitung der personenbezogenen Daten der Fanpage-Besucher durch Facebook mit verantwortlich sind, hatte der EuGH im vergangenen Jahr entschieden (dazu unser Newsletter-Artikel aus September 2018, den Sie [hier](#) abrufen können; zur gemeinsamen Verantwortlichkeit auch [hier](#)). Fanpage-Betreiber können derzeit ihrer Rechenschaftspflicht so, wie sie von der DSK verstanden wird, nicht nachkommen: Hierzu fehlen Informationen von Facebook etwa über die genaue Verarbeitung personenbezogener Daten, die über die Fanpages erhoben werden. Das rechtliche Risiko, eine Fanpage zu betreiben, ist damit jüngst gestiegen. Ob, wie und wann die Datenschutzaufsichtsbehörden tätig werden, bleibt abzuwarten – nach einem Tweet der LfDI BW sollen zunächst die Fanpages öffentlicher Stellen näher untersucht werden.

Und auch an anderer Stelle wird die Nutzung von Facebook-Tools riskanter: Der VGH München hat Ende März die Positionen von BayLDA und VG Bayreuth bestätigt, nach denen die Nutzung von „Facebook Custom Audience“ ohne Einwilligung datenschutzrechtlich unzulässig ist (dazu unser Newsletter-Artikel aus September 2018, den Sie [hier](#) abrufen können).

Hintergrundinformationen:

- Die Positionierung ist abrufbar unter:  
[https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Orientierungshilfen/Positionierung\\_Facebook\\_Fanpages.pdf](https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Orientierungshilfen/Positionierung_Facebook_Fanpages.pdf)
- Zu Facebook Custom Audience: VGH München, Beschluss vom 29.03.2019 – 5 CS 18.1157

**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



Dr. Lucyne Ghazarian  
+49 (0)221 65065-222  
lucyne.ghazarian@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