LOSCHELDER

Newsletter Datenschutzrecht

Februar 2020

Sehr geehrte Damen und Herren,

wir melden uns in diesem Monat deutlich früher bei Ihnen, als gewohnt. Dies hat seinen guten Grund: In der Sagen umwobenen Cookie-Debatte hat der BGH am 30. Januar 2020 einen Meilenstein gesetzt. Wir waren vor Ort und berichten für Sie aus erster Hand.

Zudem ein Hinweis in eigener Sache: Die Anforderungen an Organisation und Struktur des Compliance- und Krisen-Managements im Unternehmen ändern sich mit der digitalen Transformation. Zugleich bringt dies neue Möglichkeiten auch für diesen Bereich mit sich. Diesem so wichtigen Themenkomplex widmen wir uns am **12. Februar 2020** in unserer nächsten Veranstaltung im Forum Digitalisierung. Ein Fokus liegt dabei auf dem Handling von Datenpannen und dem Verlust von Betriebs- und Geschäftsgeheimnissen. Über Ihr Interesse an dieser Veranstaltung würden wir uns sehr freuen!

Weitere Informationen dazu und die **Möglichkeit zur Anmeldung** finden Sie auf unserer Homepage.

Darüber hinaus haben wir Ihnen in unserem Februar-Newsletter auch einige weitere spannende Themen mitgebracht, etwa zu Entschädigungsansprüchen Betroffener aufgrund von Datenschutzverstößen und den Voraussetzungen für eine Abberufung von Datenschutzbeauftragen.

Inhalt

Cookie-Debatte: Jetzt kommt der BGH

Spätestens seit dem Planet 49 Urteil des EuGH im Oktober 2019 in ist die Cookie-Debatte in vollem Gange: Headlines wie „Keine Cookies mehr ohne Einwilligung" und Mailings geschäftstüchtiger Datenschutzberater mit entsprechenden Meldungen haben viel Unruhe gestiftet. In der sachlichen Diskussion sind etliche Punkte umstritten, die Aufsichtsbehörden haben sich insbesondere zu Google Analytics kritisch geäußert. Offen war bei alledem bislang jedoch schon im Grundsatz, ob und wie die eigentlich im Fokus stehende Vorschrift der ePrivacy-Richtlinie in Deutschland überhaupt Anwendung finden sollte. Hierzu hat der BGH nun (im Nachgang zum EuGH-Urteil, das in einem von ihm initiierten Vorlageverfahren erging) am 30. Januar 2020 mündlich verhandelt. Wir waren vor Ort und berichten aus erster Hand zum aktuellen Stand.

In der mündlichen Verhandlung am 30. Januar 2020 in der Sache Planet49 (Az.: I ZR 7/16) ließ der Senat durchblicken, in welche Richtung er tendiert. Entschieden wurde die Sache aber noch nicht; ein Verkündungstermin steht noch aus. Wesentliche Themen in der mündlichen Verhandlung waren zum einen die spezifischen Anforderungen an eine wirksame Einwilligung, zum anderen die Frage der zulässigen Cookie-Verwendung. Zu letzterem hielt der Senat fest, dass seiner Ansicht nach eine richtlinienkonforme Auslegung des Telemediengesetzes in Betracht kommt – dies war bisher weit überwiegend abgelehnt worden.

Aber was bedeutet dies in der Praxis? Kurz gefasst: Wir alle haben das Telemediengesetz bisher falsch verstanden. Es ist mit dem BGH nach seiner Tendenz in der mündlichen Verhandlung so zu lesen, dass Cookies und andere Informationen nur dann auf den Endgeräten der Nutzer gespeichert werden dürfen, wenn sie entweder für die Bereitstellung des Dienstes unbedingt erforderlich sind oder eine Einwilligung vorliegt.

In der Praxis wird sich angesichts dessen nun die Diskussion weiter intensivieren, was „unbedingt erforderlich" für die Bereitstellung des jeweiligen Dienstes ist – dies wird für unterschiedliche Dienste womöglich auch unterschiedlich zu beantworten sein.

Zur Einordnung: Cookies, PlugIns, Pixel & Co helfen bei der Bereitstellung und Optimierung der eigenen Online-Angebote, etwa der Unternehmens-Homepage, ebenso wie beim Marketing. Die Zwecke, zu denen sie eingesetzt werden können, sind vielfältig: Es be-

ginnt bei der Nutzung von Cookies - etwa für eine Warenkorbfunktion, ein Benutzerkonto oder einfach die Navigation auf der Website. Überdies können derartige Tools zu Analysezwecken (etwa Reichweite der Website) ebenso eingesetzt werden, wie für ein Tracking einzelner Nutzer, um diesen z.B. personalisierte Werbung auszuspielen. In vielen dieser Fälle werden dabei personenbezogene Daten erhoben, da die jeweiligen Internet-Nutzer identifizierbar werden, z.B. über User-IDs in den Cookies. Ist dies der Fall, ist das Datenschutzrecht mit der DSGVO und – in Deutschland – dem Bundesdatenschutzgesetz unmittelbar anwendbar. Derartige Cookies & Co dürfen dann nur gesetzt werden, wenn eine DSGVO-Erlaubnisgrundlage vorhanden ist – insbesondere eine Einwilligung oder eine Erlaubnis aus berechtigten Interessen – und über die Cookie-Verwendung transparent informiert wird. Darüber hinaus gilt das ePrivacy-Recht, unabhängig von einem Personenbezug, also auch bei nicht-personenbezogenen Cookies & Co. Hier schreibt Art. 5 Abs. 3 der ePrivacy-Richtlinie aus 2002 vor, dass Cookies & Co nur dann ohne Einwilligung gesetzt werden dürfen, wenn sie für die Erbringung des Dienstes „unbedingt erforderlich" sind. Überdies verlangt auch das ePrivacy-Recht eine transparente Information.

Diese Richtlinienvorschrift aber ist nach der bisher überwiegenden Meinung nicht in das deutsche Recht umgesetzt worden. Zur Erinnerung: Eine EU-Richtlinie muss i.d.R. in nationales Recht umgesetzt werden, um unmittelbare Wirkung, gerade auch für Private zu entfalten. Eine EU-Verordnung – wie die Datenschutzgrundverordnung – gilt dagegen unmittelbar. Über all dies haben wir auch bereits ausführlich in unserem Oktober-Newsletter berichtet. Der BGH tendiert nun in eine andere Richtung und scheint für eine richtlinienkonforme Auslegung zu plädieren. Dies sei, so der Senat in der mündlichen Verhandlung, trotz des scheinbar anderslautenden Wortlauts – der die Möglichkeit zum Widerspruch ausreichen lässt – möglich, da auch die Intention des Gesetzgebers zu berücksichtigen sei, unionsrechtskonform zu handeln. Es bleibt abzuwarten, wie der BGH dies in den Entscheidungsgründen formuliert.

Für die Praxis bedeutet dies heute:

- Unternehmen sollten die Verwendung von Cookies, Pixel, PlugIns & Co in ihren Online-Präsenzen überprüfen. Dabei gilt keinesfalls, dass sämtliche dieser Tools nur mit Einwilligung verwendet werden dürfen. Vielmehr ist es – wie so oft

im Recht – eine Frage des Einzelfalls mit präziser Betrachtung insbesondere von Zweck, Nutzen und Konfiguration.

- Unternehmen sollten auch ihre Cookie- bzw. Content-Banner auf den Websites kritisch überprüfen. Diese müssen korrekt beschreiben, was passiert und, wo nötig, wirksam Einwilligungen einholen. Für wirksame Einwilligung ist dabei entscheidend, dass (i) die Nutzung der Website auch ohne Einwilligung möglich ist (und keine Cookies etc. vor Einwilligung gesetzt werden), (ii) die Einwilligung nicht „global", sondern gesondert für spezifische Zwecke eingeholt wird und (iii) über die verschiedenen Tools transparent informiert wird. Wichtig zudem: Impressum und Datenschutzerklärung der Website müssen immer auch ohne Einwilligung, also auch ohne Setzung einwilligungsbedürftiger Cookies & Co. erreichbar sein.

- Noch einige Zeit dauern wird es, bis die Frage, welche Cookies & Co. denn nun „unbedingt erforderlich" und im „berechtigten Interesse" der Unternehmen ohne Einwilligung verwendet werden dürfen. Wir haben hierzu bereits im Oktober-Newsletter eine Cookie-Ampel entwickelt, die nach wie vor relevant ist.

LAG Mecklenburg-Vorpommern: Entschädigung und ihre Kriterien

Allseits bekannt ist, dass Datenschutzverstöße empfindliche Bußgelder nach sich ziehen können. Ein Verstoß gegen datenschutzrechtliche Vorschriften hat aber nicht bloß Auseinandersetzungen mit den Aufsichtsbehörden zur Folge, sondern kann auch zu Schadensersatz- oder Entschädigungszahlungen an die Betroffenen führen. Wann und wie Schadensersatz oder Entschädigungen tatsächlich zu zahlen sind, illustriert ein Urteil des LAG Mecklenburg-Vorpommern aus dem vergangenen Jahr.

Ausgangspunkt der Entscheidung war eine rechtswidrige Videoüberwachung von Beschäftigten, welche das LAG als Verletzung des Rechts auf informationelle Selbstbestimmung wertete. Das LAG erkannte dem Kläger die beantragte Entschädigung über 2.000 Euro zu. Zu beachten: Eine Entschädigung errechnet sich nach Billigkeitsgesichtspunkte und ist im Gegensatz zum Schadensersatz keine Kompensation von Vermögensschäden. Interessant ist das Urteil daher vor allem wegen der Kriterien, die das LAG der Beurteilung der angemessenen Höhe der Zahlung zugrunde legte:

- **Zeit/Dauer**: Entscheidend ist, wie oft es tatsächlich zu einem Verstoß gegen die datenschutzrechtliche Bestimmung gekommen ist. Nur daraus ist nachvollziehbar, wie intensiv das Recht auf informationelle Selbstbestimmung tatsächlich verletzt worden ist. Für den konkreten Fall der Videoüberwachung ging das LAG noch einen Schritt weiter und stellte klar, dass eine dauerhafte Überwachung einen Verstoß gegen die Menschenwürde darstellen würde.

- **Intransparenz**: Daneben berücksichtigte das Gericht die Tatsache, dass die Kameras teilweise versteckt und die Arbeitnehmer über diese nicht aufgeklärt wurden. Dies lässt sich auch auf andere Verarbeitungsformen personenbezogener Daten übertragen: Wenn der Betroffene über die stattfindende Verarbeitung seiner Daten informiert ist, kann er abschätzen, dass und inwieweit seine Daten verarbeitet werden. Mit anderen Worten: Je transparenter der Betroffene über die vorgenommene Verarbeitung aufgeklärt wird, desto geringer fällt die zu zahlende Entschädigung am Ende aus.

- **Schwere:** Weiterhin stellt sich das LAG die Frage, wie schwerwiegend die Auswirkungen des Verstoßes für den Einzelnen sind; je intensiver der Betroffene durch den Verstoß getroffen wird, desto höher soll seine Entschädigung am Ende ausfallen. Die Intensität der Verletzung ist äquivalent zur Sensibilität der Daten. Dabei unterscheidet das Gericht drei Bereiche; die sog. „Sozial-, Privat- und Intimsphäre". Dabei ist eine Verarbeitung wenig sensibler Daten – das LAG verstand auch die Verhaltensweisen der gefilmten Arbeitnehmer als wenig sensible Daten – eher in die Sozial-, die Verarbeitung von sensiblen Daten – z.B. Gesundheitsdaten – hingegen eher in die Intimsphäre einzuordnen.

- **Haltung des Verantwortlichen:** Besonders in die Entscheidung des LAG floss jedoch ein, inwieweit sich der Verantwortliche mit den Rechten der betroffenen auseinandergesetzt hat. Das LAG erkannte in dem Fall ein „Desinteresse" an den Schutzinteressen des Beschäftigten, das sich auf dessen Recht auf informationelle Selbstbestimmung „besonders verletzend" und somit auch auf die Höhe der Entschädigungszahlung auswirkte.

Insgesamt ließ das Gericht alle Kriterien in eine Gesamtabwägung einfließen. Das Ausmaß der Entschädigung ist von dem Ausmaß des Verstoßes gegen datenschutzrechtliche Vorschriften und damit gleichzeitig gegen das Recht auf informationelle Selbstbestimmung abhängig.

Im Ergebnis sind diese aufgelisteten Kriterien nicht neu, sondern werden auch bei Zahlungsansprüchen abseits des Datenschutzrechts relevant. Allerdings bedeutet dies nicht automatisch, dass hinsichtlich der Höhe auf Entscheidungen aus anderen Bereichen zurückgegriffen werden kann. Diese Kriterien sollen vielmehr dazu dienen, eine angemessene Höhe für den konkreten Fall zu ermitteln, sodass sich getroffene Beurteilungen auch immer nur auf den konkreten Fall beziehen und in einer minimal abweichenden Konstellation bereits ganz anders ausfallen können.

Das Urteil hilft aber, das Risiko einer Entschädigungszahlung einzuschätzen.

Betrieblicher Datenschutzbeauftragter

Mit Inkrafttreten der DSGVO haben sich auch die rechtlichen Rahmenbedingungen für den betrieblichen Datenschutzbeauftragten (DSB) verändert (Art. 37 ff. DSGVO, § 38 BDSG). Die Diskussion kreist auch darum, was der Benachteiligungsschutz des DSB konkret für Unternehmen bedeutet (Art. 38 Abs. 3 DSGVO). Dies wird besonders interessant, wenn das Unternehmen über einen Wechsel des DSB nachdenkt. Eine neuere Entscheidung des LAG Sachsen (Az. 08.10.2019, 7 Sa 128/19) zur Abberufung wegen eines Interessenkonflikts und die Stellungnahme des LDI NRW zu den FAQ um Datenschutzbeauftragte, möchten wir zum Anlass nehmen, uns diese Thematik näher anzuschauen.

Zunächst zur Benennung: Die DSGVO verlangt die Benennung, wenn sich das Unternehmen hauptsächlich und so sehr mit personenbezogenen Daten befasst, dass eine intensivere Überwachung erforderlich ist (Art. 37 Abs. 1 lit. b) DSGVO). Darüber hinaus ist ein Unternehmen nach dem BDSG zur Benennung verpflichtet, wenn mindestens 20 Mitarbeiter mit der Verarbeitung personenbezogener Daten befasst sind (§ 38 Abs. 1 BDSG). Das Unternehmen kann dabei frei entscheiden, ob es mit der Aufgabe einen Mitarbeiter oder einen Externen befasst. Besonders wichtig ist dabei aus Sicht von DSGVO und BDSG die fachliche und persönliche Eignung des Ausgewählten. Falls ein Mitarbeiter bestellt wird, kann das Unternehmen auch entscheiden, diesen noch mit weiteren Aufgaben im Betrieb zu beauftragen. In diesen Fällen ist aber darauf zu achten, dass der Mitarbeiter nicht in eine Situation gebracht wird, in der er sich

selbst kontrollieren müsste. Zu den Fragen der Benennung gibt die Stellungnahme des LDI NRW Hinweise. Eine Interessenskollision, die eine Benennung als DSB ausschließt, sieht das LDI NRW etwa beim Leiter der IT- oder Personal-Abteilung sowie bei Beschäftigen in diesen Abteilungen, wenn diese die Datenverarbeitungsprozesse bestimmen oder jedenfalls wesentlich beeinflussen können. Stehen ihnen solche Kompetenzen nicht zu, kann mithin auch ein Mitarbeiter von IT- oder Personal-Abteilung als DSB bestellt werden. Der Ausschluss der Selbstkontrolle gilt in dieser strengen Form indes nur für den Datenschutzbeauftragten, nicht für den Datenschutzkoordinator, dem andere, vermehrt operative und strategische Aufgaben obliegen.

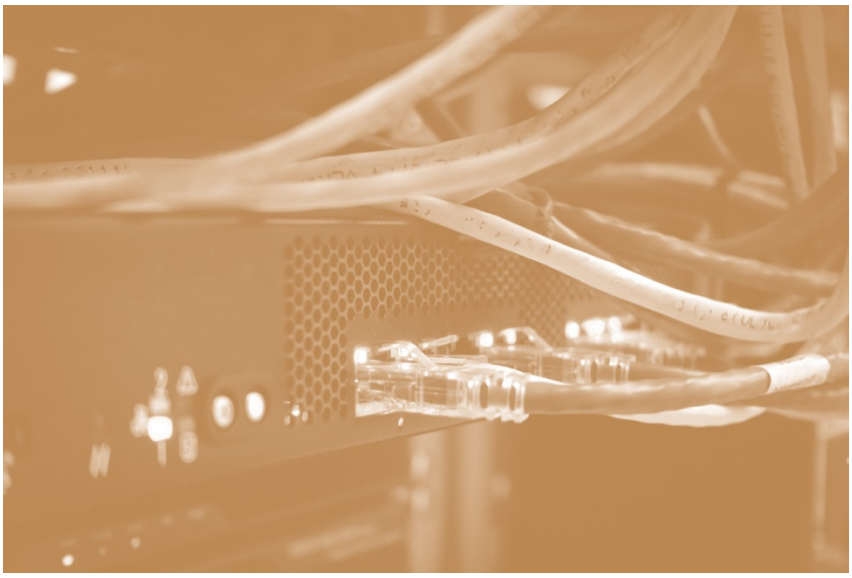
Kommt es bei der Zusammenarbeit mit dem DSB zu Unstimmigkeiten, steht schnell die Frage nach dessen Abberufung im Raum. Um einen Benachteiligungsschutz zu gewährleisten, hat der Bundesgesetzgeber für verpflichtend bestellte interne DSB strenge Voraussetzungen an deren Abberufung und Kündigung vorgesehen (§ 38 Abs. 2 S. 2, § 6 Abs. 4 BDSG). Die Ablösung von der Position als DSB ist nur möglich, wenn ein wichtiger Grund vorliegt, der die Weiterarbeit für beide Seiten unzumutbar macht. Auch kann eine Kündigung des Arbeitsverhältnisses nicht „missbraucht“ werden, um den DSB auszuwechseln: Eine Kündigung ist ebenfalls nur zulässig, wenn ein wichtiger Grund vorliegt. Selbst wenn der Posten des DSB (freiwillig) aufgegeben wurde, kann dem Mitarbeiter für ein Jahr nur gekündigt werden, wenn ein wichtiger Grund vorliegt.

Bei der Ermittlung des wichtigen Grundes kann zum einen auf die Fähigkeit oder Eignung des DSB, seine Position unabhängig wahrzunehmen und zum anderen auf Begleitumstände – außerhalb der Erfüllung seiner Aufgabe – Bezug genommen werden. So genügte dem LAG Sachsen (Az. 08.10.2019, 7 Sa 128/19) das Fortbestehen eines Interessenskonflikts, der bereits 15 Jahre vor Anwendbarkeit der DSGVO bestand. In seinem Urteil kam das LAG zu dem Ergebnis, dass die DSGVO zwar keine eigene gesetzliche Grundlage für die Auflösung der Rechtsstellung eines Datenschutzbeauftragten biete, der Verantwortliche aber auch nicht dazu verpflichtet sei, einen Interessenkonflikt weiter bestehen zu lassen. Gegen das Urteil wurde Revision eingelegt; es bleibt also abzuwarten, ob das BAG diese Ansicht bestätigen wird. Bis zu einer entgegenstehenden Entscheidung lohnt es sich demnach – wenn man über den Wechsel

seines DSB nachdenkt – einen Blick darauf zu werfen, ob die Voraussetzungen für die Ernennung überhaupt noch vorliegen.

Ist der DSB extern bestellt, gelten die vorigen strengen Voraussetzungen an Abbestellung oder Kündigung nicht. Weder die DSGVO noch das BDSG treffen klare Aussagen, welche Voraussetzungen anstelle dessen gelten sollen. Das bedeutet, dass für die Kündigung eines externen Datenschutzbeauftragten in erster Linie die Vereinbarungen über Laufzeit und Kündigung aus dem zugrundeliegenden Vertrag zu berücksichtigen sind. Bei der Ausgestaltung des Vertrages ist auf eine angemessene Vertragslaufzeit zu achten, um der Unabhängigkeit des Datenschutzbeauftragten ausreichend Rechnung zu tragen. Wie lang die Laufzeit sein sollte, um eine ausreichende Unabhängigkeit zu sichern, wird noch diskutiert; in Rede stehen Laufzeiten zwischen 2 und 5 Jahren.

Die Abbestellung kann – auch im Fall eines freiwillig bestellten internen DSB, für den die genannten strengen Voraussetzungen ebenfalls nicht gelten – durch eine einfache Anweisung erfolgen. Aber Achtung: Für freiwillig bestellte, interne DSB gelten die arbeitsvertraglichen Pflichten trotz der Abbestellung fort; insbesondere die Kündigungsschutzvorschriften bestehen weiter. Für externe DSB gelten die sonstigen dienstvertraglichen Pflichten fort.



Zu guter Letzt: Geldbußen und Kuriositäten des Monats

In Sachen Geldbußen und Kuriositäten gibt es auch aus dem vergangenen Monat Spannendes zu berichten. Dazu gehört ein hohes Bußgeld aus Italien, das für unlautere Werbemaßnahmen verhängt wurde und ein Einbrecher, der gegen einen Hausbesitzer wegen dessen Videoüberwachung vorgegangen ist und das Verfahren bis zum EuGH brachte. Und auch der Brexit ist datenschutzrechtlich relevant.

- **Brexit und dann?**

Mit Wirkung zum 1. Februar 2020 ist das Vereinigte Königreich (UK) aus der Europäischen Union (EU) ausgetreten. Unmittelbare Auswirkung auf Datengeschäfte mit Unternehmen in UK hat dies (noch) nicht gehabt. Aufgrund des ausgehandelten Übergangszeitraums bleiben die datenschutzrechtlichen Beziehungen zwischen EU und UK jedenfalls bis Ende 2020 unberührt. Bis dahin gilt UK nicht als Drittstaat mit der Folge, dass der Datenaustausch mit UK noch wie innerhalb der EU erfolgen kann. Es ist (noch) nicht erforderlich, für einen Datentransfer „auf die Insel" durch zusätzliche Garantien ein angemessenes Datenschutzniveau zu sichern. Dies wird sich nach aktuellem Stand allerdings Ende 2020 ändern. Dann gilt UK nach aktuellem Stand als Drittstaat und es sind zusätzliche Garantien erforderlich, um ein angemessenes Datenschutzniveau zu sichern. Dies könnten zusätzliche bilaterale vertragliche Absprachen sein oder auch ein Angemessenheitsbeschluss der EU-Kommission. Es darf mit Spannung erwartet werden, auf welchen langfristigen datenschutzrechtlichen Mechanismus sich UK und EU einigen. Für Unternehmen mit Geschäftsbeziehungen auf „der Insel" gilt bereits heute, datenschutzrechtlichen Handlungsbedarf zu prognostizieren und identifizieren. Dieser mag sich darin erschöpfen, bestehende Vereinbarungen anzupassen, kann aber auch bedeuten, ganze Geschäftsmodelle zu überdenken, vor allem, wenn sensible Daten wie Gesundheitsdaten verarbeitet werden.

- **Italien**

Wegen erheblichen strukturellen Problemen bei dem Umgang mit Kundendaten wurde gegen einen italienischen Energieversorger (Eni Gas e Luce) von der nationalen Aufsichtsbehörde ein Bußgeld in Höhe von 11,5 Mio. Euro verhängt. Das Unternehmen hatte Kundendaten für Werbeanrufe genutzt und zudem Änderungsverträge mit gefälschten Unterschriften versehen. Ein (automatisiertes) System, um Widersprüche oder Unterlassungsaufforderungen zu

sammeln, gab es nicht. Angesichts der Verbreitung der Kundendaten, ihrer Dauer und dem Umfang der resultierenden Belästigungen der Kunden sah die Aufsichtsbehörde ein Bußgeld in Höhe von 8,5 Mio. Euro als angemessen an. Die Fälschungspraxis wurde „nur“ mit einem Bußgeld von 3 Mio. Euro bedacht.

- **Datenschutz als Einbrecher-Schutz?**

Den Schirm des Datenschutzes suchte bereits vor einigen Jahren ein Einbrecher, der sich von der Videoüberwachung eines Hauseigentümers gestört fühlte und das bis zum EuGH – eindeutig ein Fall für das Kuriositätenkabinett. Der EuGH gab dem Einbrecher gar Recht, allerdings nicht, weil er bei seinen „beruflichen Tätigkeiten“ gestört wurde. Schlüssel zum Erfolg war vielmehr eine falsche Kameraausrichtung: Überwacht wurde auch der öffentliche Straßenraum vor dem Grundstück in unzulässiger Weise (EuGH – Rs. C-212/13).

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