LOSCHELDER

Newsletter Datenschutzrecht
Oktober 2020

Sehr geehrte Damen und Herren,

der Datenschutzmonat Oktober ist, wie auch unser heutiger Newsletter, durch Bußgeldfälle geprägt. So hat die Hamburger Datenschutzbehörde das schwedische Modehaus H&M mit einem Rekordbußgeld von über 35 Mio. EUR belegt. Anlass dafür war die weitreichende Verarbeitung teils sensibler und höchstpersönlicher Daten von Mitarbeitern. Ebenfalls seit Anfang des Monats verhandelt das Landgericht Bonn über das Millionenbußgeld, das der Bundesbeauftragte für den Datenschutz Ende des letzten Jahres dem Telekommunikationsanbieter 1&1 auferlegt hatte. Wir waren für Sie vor Ort und berichten von den spannenden Grundsatzdiskussionen. In unseren weiteren Beiträgen befassen wir uns mit der Reichweite des Auskunftsanspruchs und der Zulässigkeit personalisierter Online-Werbung sowie der aktuellen Veröffentlichung der Aufsichtsbehörden zu „Microsoft Office 365“ – leider bleibt bereits unklar, welches Microsoft-Produkt exakt adressiert wird.

Inhalt

Millionenbußgeld gegen H&M

Urlaubserlebnisse, Krankheitsbilder und Diagnosen, familiäre Probleme und religiöse Bekenntnisse: Bei H&M wurde ein detailliertes Profil etlicher Arbeitnehmer angelegt. Diese Informationen lagen – versehentlich zeitweilig ungeschützt und für alle offen zugänglich – auf den Servern des Modekaufhauses. Dafür verhängte der HamBfDI kürzlich ein Rekordbußgeld in Höhe von 35,2 Mio. Euro. Der Fall, so außergewöhnlich er scheint, bestätigt sehr eindrücklich unsere Erfahrungen in der täglichen Praxis: Meist sind es Zufälle, Versehen und an sich unscheinbare Gegebenheiten, die Datenschutzverstöße zu Tage treten lassen und ein erhebliches Bußgeldrisiko begründen – wenn dann die interne Organisation nicht Hand in Hand zusammenarbeitet, wird dieses nochmals gesteigert.

„Sie waren doch im Urlaub, richtig? Wie war es denn? Was haben sie so gemacht?“ – „Ich habe gehört, Sie waren krank. Was hatten Sie denn? Geht es Ihnen besser?“ Wenn einen der Chef nach einer Abwesenheit so anspricht und ganz unverbindlich mit einem zu plaudern beginnt, ist das zunächst rücksichtsvoll und zuvorkommend. Problematisch wird es, soweit das Interesse über einen einfachen Plausch hinausgeht. Nutzt der Vorgesetzte nämlich die im Gespräch erlangten Informationen über die privaten Verhältnisse des Arbeitnehmers, um detaillierte Profile über seine Mitarbeiter zu erstellen, schlägt die nette Aufmerksamkeit schnell in einen Datenschutzverstoß um. Kombiniert mit Leistungsdaten der Arbeitnehmer können solche Informationen für ausführliche Analysen der Person genutzt werden. So geschehen beim Modekaufhaus H&M. Nach fast einjähriger Untersuchung des Falles verhängte der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit Caspar am 01.10.2020 ein Bußgeld in der Rekordhöhe von rund 35,2 Mio. €. Bekannt geworden ist auch dieser Fall übrigens – wie in der Praxis so häufig – durch ein Datenleck: Versehentlich waren die abgelegten Daten zeitweilig für sämtliche Mitarbeiter zugänglich.

Doch was genau war geschehen? Das schwedische Modehaus mit Deutschlandsitz in Hamburg betreibt ein Servicecenter in Nürnberg. Dort kam es seit mindestens 2014 zur systematischen Erfassung personenbezogener Daten von Mitarbeitern. Durch vermeintlich informelle „Welcome Back Talks“ und zwanglose Gespräche auf dem Flur, erlangten Vorgesetzte Wissen über

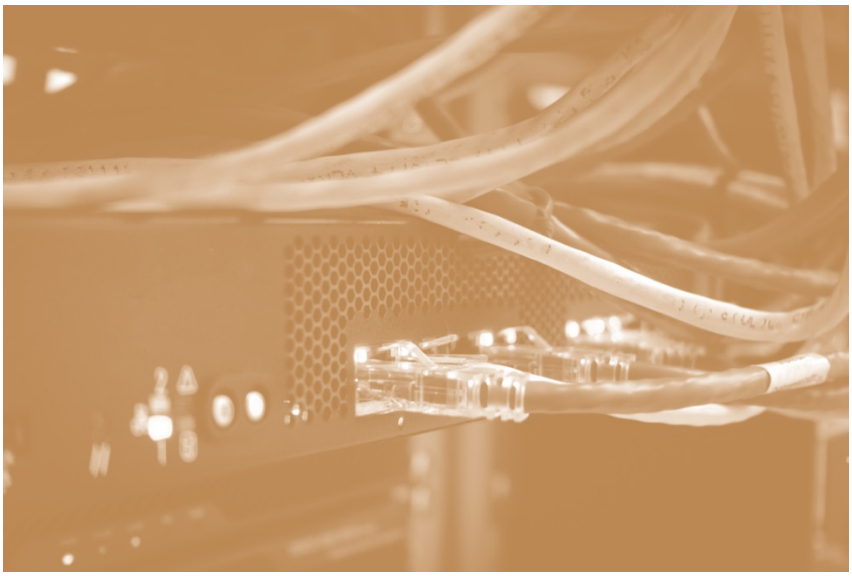
konkrete Urlaubserlebnisse, Krankheitsbilder und Diagnosen, familiäre Probleme sowie religiöse Bekenntnisse ihrer Mitarbeiter. Dieses Wissen wurde systematisch aufgezeichnet und digital so gespeichert, dass bis zu 50 Führungskräfte des Hauses darauf Zugriff hatten. Bekannt wurde das Geschehen, als die Daten im Oktober 2019 für einige Stunden versehentlich unternehmensweit frei einsehbar waren. Dies führte dazu, dass der Hamburgische Beauftragte für Datenschutz rund 60 Gigabyte an Daten zur Auswertung beschlagnahmte und sich das Geschehen von Zeugen bestätigen ließ. Zwar betont der Behördenleiter, dass H&M ein *„bislang beispielloses Bekenntnis zur Unternehmensverantwortung“* gezeigt und aktiv an der Aufklärung mitgewirkt hätte. Dennoch hält er in Anbetracht der Schwere der Verfehlung das Bußgeld in Rekordhöhe für angemessen.

Unter Geltung des alten BDSG war die Höhe eines möglichen Bußgeldes noch auf 300.000 € begrenzt. Die DSGVO zieht die Zügel hingegen wesentlich strammer, sieht sie doch ein Bußgeld bis zu 20 Mio. € bzw. bis zu 4% des Jahresumsatzes des Unternehmens vor. Es gilt jeweils der höhere Wert. In jedem Fall soll das Bußgeld aber wirksam, verhältnismäßig und abschreckend sein. Die Datenschutzaufsichtsbehörden veröffentlichten unlängst ein umstrittenes Bußgeldbemessungskonzept (wir berichteten im November 2019 und greifen dies auch in diesem Newsletter zum Bericht über das 1&1-Bußgeld nochmals auf), anhand dessen – ausgehend vom Umsatz – „Tagessätze“ für geringe, mittlere und schwerwiegende Verstöße ermittelt werden. Dieses Konzept führt bei hohen (Gruppen-) Umsätzen auch bei geringen Verstößen zu Millionenbußgeldern: „Rekordträger“ in Deutschland waren bisher noch die Deutsche Wohnen SE mit 14,5 Mio. € und 1&1 Drillisch mit 9,5 Mio. € für einen als eher gering eingestuften Verstoß. Das ggü. H&M verhängte Bußgeld ist nun nochmals deutlich höher – nicht nur wegen abweichender Gruppenumsätze, sondern auch, da die Behörde verdeutlicht, als wie schwerwiegend sie den Datenschutzverstoß eingeschätzt hat.

Zulässig war diese Form der Datenverarbeitung wohl nicht: Im Bereich des Beschäftigtendatenschutzes dürfen Daten insbesondere dann verarbeitet werden, wenn dies für die Begründung, Durchführung oder Beendigung eines Arbeitsverhältnisses erforderlich ist. Eine derart detaillierte Erfassung von Informationen dürfte für die Durchführung des Arbeitsverhältnisses kaum noch

erforderlich sein. Dies gilt erst recht, berücksichtigt man die erhebliche Eingriffstiefe in das Persönlichkeitsrecht des Mitarbeiters. Auch eine Einwilligung scheint im Fall von H&M eher fernliegend: Zwar haben die Mitarbeiter freiwillig berichtet, aber vermutlich nicht in Kenntnis der Erfassung ihrer Berichte in Form detaillierter Mitarbeiterprofile. Ohnehin ist eine Einwilligung im Beschäftigungskontext nur wirksam, sofern sie schriftlich oder elektronisch vorliegt.

Das Beispiel H&M verdeutlicht, wie folgenreich eine technische Datenpanne – im vorliegenden Fall waren die Daten versehentlich für einen weiten Kreis von Nutzern sichtbar – sein kann. In der Praxis sind es oft eben solche Vorfälle, die datenschutzrechtliche Unzulänglichkeiten und Verstöße zu Tage fördern. Das Aufdeckungsrisiko von Verstößen ist daher letztlich unkalkulierbar, da kein Unternehmen vor IT-Pannen, Hackerangriffen oder einem Einzelversagen von Mitarbeitern gefeit ist.



Auskunftsanspruch

Der Auskunftsanspruch ist das zentrale Betroffenenrecht in der Datenschutzgrundverordnung. Mithilfe dieses Anspruchs soll der Betroffene einen Überblick darüber bekommen, welche Daten wie und wozu konkret verarbeitet werden. In der Praxis stellt gerade dieser Anspruch die Unternehmen oft vor die Herausforderung, umfassende Datensätze zusammenstellen zu müssen. Die exakte Reichweite dieses Anspruchs ist gerade dann kritisch zu hinterfragen, wenn der Auskunftsanspruch strategisch im Rahmen anders gelagerter Auseinandersetzungen eingesetzt wird – etwa, um zivilgerichtlich eine bessere Position zu erreichen, oder im Rahmen von Kündigungsklagen. Dieser Beitrag soll einen Überblick darüber geben, was nach aktuellem Stand der Rechtsprechung im Rahmen der Auskunftserteilung zu beachten ist, um den Anforderungen des Art. 15 DSGVO (noch) zu genügen.

Wer von wem?

Der Auskunftsanspruch steht nur dem Betroffenen selbst zu. Betroffen ist immer nur die Person, die durch die Daten identifizierbar ist. Dieser limitierte Kreis der Rechteinhaber spielt in zwei Fällen eine besondere Rolle:

- Zwar darf ein Rechtsanwalt für seinen Mandanten die Auskunft über die Verarbeitung dessen personenbezogener Daten verlangen. Das setzt allerdings voraus, dass der Rechtsanwalt mit Vorlage einer Vollmacht nachweisen kann, dass er die Auskunft für seinen Mandanten in Anspruch nimmt. Teilweise wird sogar verlangt, dass eine Originalvollmacht vorgelegt wird (AG Berlin-Mitte, Urteil vom 29.07.2019 – 7 C 185/18 –, Rn. 16, juris).

- Anders verhält es sich beim Insolvenzverwalter: Dadurch, dass das datenschutzrechtliche Auskunftsrecht so eng mit der Person des Betroffenen und dem Schutz seiner Interessen verflochten ist, steht es im Insolvenzfall nicht dem Insolvenzverwalter zu. Der Insolvenzverwalter kann sein Auskunftsbegehren - beispielsweise über das Steuerkonto eines Insolvenzschuldners – also nicht auf Art. 15 DSGVO stützen (siehe etwa OVG Lüneburg, Beschluss vom 26.06.2019 – 11 LA 274/18 –, Rn. 13 - 14, juris, aber auch VG Gießen, Urteil vom 23.10.2019 – 4 K 252/19.GI).

Dem Betroffenen steht der Auskunftsanspruch immer nur gegen denjenigen zu, der im konkreten Fall seine Daten verarbeitet („Verantwortlicher"). Je nach Verarbeitungsvorgang kann es sich so um verschiedene Verantwortliche handeln. Ein Verantwortlicher kann nicht dazu verpflichtet werden, dem Betroffenen Auskunft darüber zu erteilen ob und welche personenbezogenen Daten des Betroffenen durch andere Unternehmen verarbeitet werden. Dies ist nur im Fall der gemeinsamen Verantwortlichkeit (Art. 26 DSGVO) denkbar.

Keine zwingende Präzisierung eines Auskunftsantrags

Der Betroffene kann im Vorhinein oft nicht wissen, welche personenbezogenen Daten beim Verantwortlichen verarbeitet werden. Daher kann und muss der Betroffene sein Auskunftsverlangen grundsätzlich nicht genauer konkretisieren (Landesarbeitsgericht Baden-Württemberg, Urteil vom 20.12.2018 – 17 Sa 11/18 –, Rn. 194, juris). Gleichwohl kann eine Präzisierung erbeten werden, wenn die Datensammlung entweder umfangreich oder erkennbar keine „Gesamtauskunft" gewollt ist. Erzwungen werden kann dies oft nicht: Gegen ein Auskunftsverlangen kann nicht mit Erfolg eingewandt werden, es entstünde ein unverhältnismäßiger Aufwand – jedenfalls dann nicht, wenn dieser wegen noch nicht angepasster Datenorganisation entsteht (AG München, Teilurteil vom 04.09.2019 – 155 C 1510/18 –, Rn. 71, juris).

Form der Auskunftserteilung:

Nach Ansicht des LG Wiesbaden schuldet der Verantwortliche dem Betroffenen die Zurverfügungstellung einer – jedenfalls erstmalig – kostenlosen und schriftlichen Datenkopie (LG Wiesbaden, Urteil vom 05.11.2018 – 5 O 214/18 –, Rn. 4, juris). Dieses Ergebnis gilt indes nicht uneingeschränkt, sieht Art. 15 Abs. 3 S. 3 DSGVO doch – jedenfalls bei elektronischer Antragstellung – eine elektronische Antwort vor. Bei einer Datenkopie handelt es sich nach Ansicht der Rechtsprechung zumindest um eine Liste, auf der die gespeicherten bzw. verarbeiteten Daten aufgezählt werden (ArbG Bonn, Urteil vom 16.07.2020 – 3 Ca 2026/19 –, Rn. 93, juris). Auch diese Aussage ist nicht uneingeschränkt gültig: Sicherlich kommt es auch darauf an, in welcher Form die Daten im Einzelfall überhaupt beim Unternehmen liegen. Der Verantwortliche muss sicherstellen, dass die Auskunft in präziser, transparenter, verständlicher und leicht

zugänglicher Form in einer klaren und einfachen Sprache übermittelt wird (ArbG Düsseldorf, Urteil vom 05.11.2020 – 9 Ca 6557/18 –, Rn. 65, juris). Die Auskunft muss unverzüglich, i.d.R. innerhalb eines Monats, nach Eingang des Auskunftsantrags beantwortet werden. Eine verspätete Auskunftserteilung begründete in einem Fall bereits einen Schadensersatz in Höhe von 1.000 Euro, eine fehlerhafte Auskunft einen Schadensersatzanspruch in Höhe von 500 Euro (ArbG Düsseldorf, Urteil vom 05.03.2020 – 9 Ca 6557/18 –, Rn. 97, juris).

Umfang der Auskunftserteilung:

Der Umfang des Auskunftsanspruchs richtet sich allgemein nach den Vorgaben in Art. 15 Abs. 1 2. Halbsatz Buchstabe a bis h DSGVO. Das bedeutet, dass der Betroffene unter anderem über den Verarbeitungszweck, die Kategorien der Daten, die Empfänger der Daten oder die Dauer der Verarbeitung, aber auch über die Herkunft der Daten und die möglichen Betroffenenrechte informiert werden muss. Ein weitergehender Auskunftsanspruch kann beispielsweise über eine Gesamtbetriebsvereinbarung geregelt werden (ArbG Bonn, Urteil vom 16.07.2020 – 3 Ca 2026/19 –, Rn. 88 f., juris).

Um den Betroffenen ausreichend in die Lage zu versetzen, Inhalt und Umfang seiner personenbezogenen Daten beurteilen und über ein weiteres datenschutzrechtliches Vorgehen entscheiden zu können, müssen vollständige und konkrete Angaben erfolgen; pauschale Ausführungen genügen regelmäßig nicht (ArbG Düsseldorf, Urteil vom 05.03.2020 – 9 Ca 6557/18 –, Rn. 66, juris; ArbG Düsseldorf, Urteil vom 05.03.2020 – 9 Ca 6557/18 –, Rn. 65, juris). Es besteht – über die gespeicherten bzw. verarbeiteten Daten hinaus – aber keine Pflicht zur Herausgabe zusätzlicher Unterlagen (ArbG Bonn, Urteil vom 16.07.2020 – 3 Ca 2026/19 –, Rn. 94, juris). Konkret bedeutet das:

- Kein Auskunftsanspruch über interne Vorgänge des Verantwortlichen, wie etwa Vermerke, Schriftverkehr, der dem Betroffenen bereits bekannt ist, rechtliche Bewertungen oder Analysen (vgl. LG Köln, Teilurteil vom 18.03.2019 – 26 O 25/18 – Rn. 19, juris; LG Köln, Urteil vom 19.06.2019, Az. 26 S 13/18; AG München, Teilurteil vom 04.09.2019 – 155 C 1510/18 –, Rn. 55, juris).

- Kein Auskunftsanspruch über Scores der betroffenen Person, die durch den Verantwortlichen auf Grundlage vorhandener Datensätze oder Algorithmen generiert wurden; insbesondere wenn diese Daten zur entgeltlichen Abfrage bereitgehalten werden (LG Wiesbaden, Urteil vom 05.11.2018 – 5 O 214/18 –, Rn. 33, juris; Sächsisches Finanzgericht, Urteil vom 08.05.2019 – 5 K 337/19 – Rn. 10, 15, 21, juris).

- Kein Auskunftsanspruch über die Verarbeitung personenbezogener Daten eines Dritten (VG Cottbus, Urteil vom 22.06.2020 – 8 K 444/17 –, Rn. 56, juris).

- Der Auskunftsanspruch beinhaltet in der Regel keinen Anspruch auf Akteneinsicht. Die Übersendung einer Akte muss nur dann erfolgen, wenn (und soweit) diese personenbezogene Daten des Betroffenen enthält (LG Köln, Urteil vom 24.06.2020 – 20 O 241/19 –, Rn. 46, juris; Finanzgericht des Saarlandes, Beschluss vom 03.04.2019 – 2 K 1002/16 –Rn. 11, juris).

Einschränkung des Auskunftsanspruchs:

Der Auskunftsanspruch des Betroffenen ist in der Regel dann einzuschränken, wenn überwiegende geschützte Interessen eines Dritten betroffen wären, also sofern etwa Daten eines Dritten dadurch offengelegt würden (LG Köln, Urteil vom 24.06.2020 – 20 O 241/19 –, Rn. 46, juris). Maßgeblich kommt es dann auf eine Interessensabwägung an (LAG Baden-Württemberg, Urteil vom 20.12.2018 – 17 Sa 11/18 – Rn. 202, 204, juris).

Besteht aus diesem oder einem sonstigen Grund eine Geheimhaltungspflicht für bestimmte Informationen, so soll eine Auskunftserteilung nicht ganz verwehrt werden. Vielmehr sollten Wege gefunden werden, um die Interessen der Beteiligten miteinander zu vereinbaren, beispielsweise durch Schwärzungen der Daten Dritter (LG Köln, Urteil vom 24.06.2020 – 20 O 241/19 –, Rn. 46, juris).

Streitwert:

Die Berechnung des Streitwerts hängt von dem konkreten Einzelfall und insbesondere vom Umfang des Auskunftsanspruchs und den damit verbundenen Schwierigkeiten ab. Als unverbindliche

Orientierung dienen hierbei allerdings Streitwertberechnungen von Gerichten, die sich mit dem Auskunftsanspruch befassten:

- In Fällen, in denen es dem Betroffenen allein um die Befriedigung seines allgemeinen Informationsinteresses geht, bezifferten Gerichte den Streitwert etwa mit 500 Euro (u.a. Landesarbeitsgericht Nürnberg, Beschluss vom 28.05.2020 – 2 Ta 76/20 –, Rn. 14, juris).

- In Fällen, in denen es zu besonderen Beeinträchtigungen des Persönlichkeitsrechts kommt, sind meist mehr Schwierigkeiten und demnach ein höherer Umfang zu erwarten, weshalb bereits Streitwerte von 600,00 Euro bis zu 5.000,00 Euro angesetzt wurden (LAG Düsseldorf a.a.O. unter Verweis auf OLG Köln, 05.02.2018 - 9 U 120/17, juris; OLG Köln, Beschluss vom 03.09.2019 - 20 W 10/18; AG München, Teilurteil vom 04.09.2019 – 155 C 1510/18, Rn. 69 – 71).

„Diese Produkte könnten Sie auch interessieren…“

Dass personenbezogene Daten von der Werbebranche im Internet für personalisierte Werbung genutzt werden, ist nichts Neues. Immer wieder bemühen sich Datenschützer mit Instrumenten der DSGVO dagegen vorzugehen. So nun auch das European Data Protection Board (edpb), das in einer umfassenden Leitlinie erörtert hat, wie ein DSGVO-konformes System der personalisierten Werbung im Social Media Kontext aussehen könnte. Die wichtigsten Punkte dieser Leitlinie stellen wir Ihnen vor.

Social Media Nutzer haben sich schon lange daran gewöhnt, dass sich ihre Suchhistorie und ihr Verhalten in sozialen Netzwerken in der ihnen eingeblendeten Werbung und den angezeigten Inhalten widerspiegeln. Stichworte sind „personalisierte Werbung“ und „Filterblasen“. Während sich mancher Nutzer an dem zugeschnittenen Angebot erfreut, betrachten Datenschutzbehörden diese Praxis kritisch – vor allem wegen der hierfür genutzten Daten und angemahnter Transparenz. Der Zusammenschluss europäischer Datenschutzbehörden, das European Data Protection Board (edpb), hat sich umfassend mit den verschiedenen Akteuren und Praktiken befasst und in einer Leitlinie (Guidelines 8/2020 vom 2. September 2020) dargestellt, wie dies aus ihrer Sicht datenschutzkonform ausgestaltet werden kann.

Kein Verbot, sondern Achtung des Datenschutzes

Ziel des edpb ist es dabei nicht, die Branche und Praktik des sogenannten *Targeting* gänzlich zu verteufeln oder zum Verbot aufzurufen. Obwohl sehr umfassend auf die Risiken, die sich für Internetnutzer und ihre Daten ergeben, eingegangen wird, geht es dem edpb letztlich um die Darstellung der Pflichtenverteilung und Verantwortlichkeit in einem unübersichtlichen Gefüge aus Datensammlern, Aufbereitern, Werbeunternehmen und Sozialen Netzwerken. Mithilfe der Leitlinie soll es also möglich sein, personalisierte Werbung und Inhalte unter Beachtung der datenschutzrechtlichen Vorgaben zu schalten.

Zentraler Punkt ist dabei die Analyse, wann eine **gemeinsame Verantwortlichkeit** zwischen den werbeschaltenden Social Media Plattformen, den Werbenden selbst und sonstigen Datensammlern, Werbeplattformen und Anbietern besteht. Zur Erinnerung: Bei gemeinsamer Verantwortlichkeit haften alle Verantwortlichen innerhalb der DSGVO voll für etwaige Rechtsverletzungen –

unabhängig davon, wer konkret die Pflichtverletzung begangen hat. Der EuGH hat in den letzten Jahren mehrere Entscheidungen zur gemeinsamen Verantwortlichkeit von Werbenden und Social Media Netzwerken, vor allem Facebook, gefällt. Danach kann diese schon angenommen werden, soweit ein Akteur auch nur über einen Teil der Verarbeitung entscheidet – Rechtsprechung, deren Konsequenzen nun in der Leitlinie des edpb aufgenommen werden. Besteht eine gemeinsame Verantwortlichkeit, sind die jeweiligen Pflichten vertraglich zu regeln und der wesentliche Inhalt den Betroffenen mitzuteilen (Art. 26 DSGVO).

Gemeinsame Verantwortlichkeit, unterschiedliche Pflichten

Das edbp geht in seiner Analyse gewohnt kleinteilig vor. Er stellt verschiedene Konstellationen zum Schalten personalisierter Werbung und Inhalte beispielhaft vor, gibt mögliche Erlaubnisgrundlagen für die Datenverarbeitung, Problempunkte und die konkreten Pflichten der Akteure an. Vor allem fordert das edbp umfassende Verträge (sogenannte Joint-Control Agreements) zwischen Netzwerkbetreibern und Werbenden, die das jeweilige konkrete Pflichtenprogramm der Parteien regeln. Dabei wird dargestellt, in welchen Konstellationen die gemeinsame Verantwortlichkeit vorliegt und welche Pflichten die Akteure jeweils zur Wahrung des Datenschutzes haben. Besonderen Fokus legt das edbp auch auf die Informationspflichten gegenüber Betroffenen. Ist die Nutzung von Daten für diese unvorhersehbar und unerwartet, scheitert regelmäßig eine Rechtfertigung der Verarbeitung auf Grundlage berechtigter Interessen nach Art. 6 Abs. 1 lit. f. DSGVO.

Risiken für Freiheit und Privatsphäre

Sowieso ist die Unvorhersehbarkeit des Umfangs der Verarbeitung ein wesentlicher Punkt für das edpb: Vielfach sei es für Verbraucher überraschend, wie weite Kreise die von ihnen angegebenen Daten durch die *Targeting*-Branche ziehen, um dann schließlich für personalisierte Werbung genutzt zu werden. Dabei ist vor allem die Anzahl der Werbepartner und Datenaufbereiter, an die die Daten gegeben werden, oft unvorhersehbar.

Das edpb sieht im *Targeting* darüber hinaus auch die Gefahr der Diskriminierung und Manipulation: Schlussfolgerungen aus gesammelten Daten könnten etwa beim Credit-Scoring eine Rolle

spielen oder immer dann Werbung für bestimmte Produkte angeboten werden, wenn diese laut Datenanalyse der Gemütslage des potentiellen Kunden entsprechen. So mancher freut sich wahrscheinlich, wenn ihm passend zum Herbstbeginn Gummistiefel und Kaschmirpullover angeboten werden, die Gefahr der Manipulation spielt aber auch noch auf einer weiteren Ebene: Erfahrungen aus verschiedenen Wahlkämpfen und nicht zuletzt im Rahmen der Corona-Pandemie zeigen, dass diese Mechanismen auch für die gezielte politische Manipulation und Missinformation genutzt werden können. Ein Umstand, der eine ernsthafte Bedrohung für den demokratischen Prozess darstellen könnte.

Auf Kompromisse bedacht

Trotz dieser deutlichen Worte ist die Leitlinie des edpb im Großen und Ganzen als Handreichung in Richtung Datenwirtschaft und Werbeindustrie zu verstehen. Die europäischen Datenschützer sind bemüht, zu einem Kompromiss zwischen der Nutzung der Daten in der Wirtschaft und dem Datenschutz beizutragen.

Die Leitlinien beschränken sich zwar auf Ausführungen zur personalisierten Werbung an Nutzer sozialer Netzwerke, lassen jedoch auch grundsätzliche Handlungsempfehlungen erkennen. Wesentliche Bedeutung kommt hier einer größtmöglichen Transparenz zu: Die richtige und umfassende Unterrichtung der Betroffenen ist entscheidend bei der Überprüfung. Nicht im Detail adressiert wird allerdings die virulente Frage, wann genau online erfasste Daten überhaupt personenbezogen sind – und wann nicht womöglich ausschließlich das ePrivacy-Recht greift. Diese Diskussion ist etwa zu vergebenen IDs zu führen, wenn über diese nur sehr wenig detaillierte Informationen erfasst werden.

Aufsichtsbehörden die Xte: Office 365 ist nicht datenschutzkonform nutzbar – oder doch?

Die Nutzung von IT-Infrastruktur US-amerikanischer Anbieter bietet den Aufsichtsbehörden nicht nur wegen der jüngsten EuGH-Entscheidung zur Datenübermittlung in die USA immer wieder Anlass zur Stellungnahme. Auch die sonstige Datenverarbeitungspraxis wird unter die Lupe genommen. Seit einigen Monaten etwa steht der Microsoft-Konzern mit seinen cloudbasierten Anwendungen wiederholt im Kreuzfeuer der Datenschutzaufsichtsbehörden. Dabei bleibt bereits wiederholt unklar, welches Produkt genau adressiert wird (Office 365 / Microsoft 365). Zuletzt hat der Zusammenschluss der nationalen Datenschutzaufsichtsbehörden, die Datenschutzkonferenz (DSK), mit 9:8 Stimmen beschlossen, dass die Ausgestaltung der Auftragsverarbeitungsverträge unzureichend und Microsoft bzw. Office 365 deshalb nicht datenschutzkonform einsetzbar sei. Diese Entscheidung ist indes schon unter den Aufsichtsbehörden selbst umstritten und bezieht sich überdies auf zwischenzeitlich mehrfach überarbeitete Vertragsdokumente. Was konkret beschlossen wurde, welche Kritik geübt wird und was für praktische Konsequenzen zu erwarten sind, stellen wir Ihnen in diesem Beitrag vor.

Für Furore sorgte Anfang Oktober ein Beschluss des Zusammenschlusses der Datenschutzaufsichtsbehörden, der DSK, zu den beliebten Office-Programmen „365“ des Microsoft-Konzerns.

Wie einer Pressemitteilung des Landesbeauftragten für Datenschutz und Informationsfreiheit Rheinland-Pfalz zu entnehmen war, hatte die DSK mit einer knappen Mehrheit von 9 zu 8 Stimmen dem Untersuchungsergebnis eines Arbeitskreises zugestimmt, das den Programmen den datenschutzkonformen Einsatz absprach. Prompt folgte die gemeinsame Stellungnahme einiger Aufsichtsbehörden, die anderer Ansicht waren. Der Hauptkritikpunkt: Die Prüfung sei zu undifferenziert. Zweifel an der Datenschutzrechtskonformität äußern indes auch diese Behörden. Schnell wurden Stimmen laut, die eine Zersplitterung der rechtlichen Bewertung zur Nutzung von Microsoft und der damit einhergehenden Rechtsunsicherheit für alle Benutzer befürchteten. Da nun aber nach einer Anfrage der NGO Frag den Staat eine erste Version des Beschlusses selbst verfügbar ist, lohnt sich die genauere Analyse der Kontroverse.

Unzureichende Informationen in Auftragsverarbeitungsverträgen

Gegenstand der Untersuchung des Arbeitskreises waren die cloudbasierten Programme des Microsofts-Konzerns, die insbesondere unter „Office 365“ und „Microsoft 365“ als online oder Abonnement-Dienste vertrieben werden, sowie die dazugehörigen Auftragsverarbeitungsverträge. Diese werden rechtlich durch die Online Service Terms (OST) und das Data Processing Addendum (DPA) ausgestaltet, die Microsoft seinen Partnern als Vertragsbedingungen stellt. Der Arbeitskreis untersuchte nur diese rechtlichen Gegebenheiten in der Version aus Januar 2020, nicht aber die technische Umsetzung. Die Verträge wurden zwischenzeitlich bereits mehrfach überarbeitet (die aktuellen OST stammen aus Oktober 2020, das aktuelle DPA aus Juli 2020). Der Arbeitskreis überprüfte, ob die Verträge den Anforderungen des Art. 28 Abs. 3 DSGVO entsprechen, vor allem, ob sie Vertragspartnern als datenschutzrechtlich Verantwortliche hinreichend Informationen über die Verarbeitungspraxis gewähren und ob Verantwortliche mit diesen eine objektive Entscheidung über die Risiken der Verwendung der Microsoft-Produkte treffen können.

Erster Kritikpunkt waren insofern die von Microsoft in den Verträgen gegebenen Informationen: Zwar gibt Microsoft durchaus in allgemeinen Formulierungen an, welche Daten sie zu welchen Zwecken entweder als Auftragsverarbeiter für Nutzer der Programme oder als Verantwortliche verarbeiten. Dem Arbeitskreis und der DSK waren diese Angaben aber nicht detailliert genug. Sie

fordern, dass insbesondere bei der Beschreibung der Art der personenbezogenen Daten und der Zwecke der Verarbeitung der „Abstraktionsgrad verringert“ wird, Freifelder eingesetzt werden oder in Einzelfällen sogar konkrete Benennungen erfolgen sollten. Ansonsten sei es nicht möglich, aus dem Auftragsverarbeitungsvertrag konkret zu erkennen, welche Daten für welche Zwecke verwendet würden, was wiederum die Fähigkeit zur Risikoanalyse von Verantwortlichen und Nutzer der Programme beeinträchtige.

Gleiches gelte auch hinsichtlich der Informationen über die technischen und organisatorischen Maßnahmen zur Datensicherung, die Microsoft auch als Auftragsverarbeiter nach Art. 32 DSGVO erfüllen muss. Vertragspartnern würde Zugang zu diesen Informationen erst nach Vertragsschluss gewährt, sodass auch hierdurch die Abschätzung der Risiken der Datenverarbeitung zum Nachteil der Verantwortlichen erschwert wird.

Darüber hinaus seien die Verträge auch hinsichtlich der Bestimmungen zur Offenlegung und Preisgabe der verarbeiteten Daten unzureichend formuliert. Es werde nur bestimmt, dass Daten herausgegeben werden könnten, soweit die Datenschutzbestimmungen es vorsehen oder dies gesetzlich vorgeschrieben ist. Der DSK reicht dies nicht, vor allem, da dies nicht auf die Gesetze der EU-Mitgliedstaaten beschränkt sei. Sie fordert eine eindeutige Formulierung, dass sich die Herausgabe für europäische Kunden rein nach dem europäischen Datenschutzrecht, also der DSGVO oder dem Recht der Mitgliedstaaten, richtet. Damit nimmt die DSK inzident Bezug auf die Debatte um den US-Cloud Act, der US-amerikanischen Sicherheitsbehörden den Zugriff auf die Daten in Clouds US-amerikanischer Unternehmen erlaubt. Da diese Frage aber noch ungeklärt sei und sowieso die Datenübermittlung in die USA nach dem Schrems II-Urteil des EuGH (wir berichteten in unserem Sondernewsletter sowie hier über dieses folgenreiche Verfahren) neu zu bewerten sei, müsse dieser Punkt noch weiter untersucht werden.

Schließlich hätte Microsoft Nutzer der Programme noch proaktiver – etwa über Push-Benachrichtigungen – über den Wechsel oder den Einsatz von Unterauftragsverarbeitern zu unterrichten. Dabei müsse dies stets auf solche Unterauftragnehmer aufsetzen, die zuvor bei Abschluss des Auftragsverarbeitungsvertrags in einer

Liste vorlagen und vom Auftragsgeber, d.h. dem Nutzer, genehmigt wurden.

Telemetrie, Informationspflichten und Behörden

Ansonsten richtete sich das Augenmerk der DSK vor allem auf die Erhebung von Telemetrie- und Performancedaten durch Microsoft. Der Konzern selbst gibt in den OST und DPA an, hierbei Verantwortlicher im datenschutzrechtlichen Sinne zu sein. In der Konsequenz steht diese Datenerhebung neben der Datenverarbeitung aus dem Auftragsverarbeitungsverhältnis. Microsoft agiert hier zu eigenen Zwecken.

Die DSK kritisiert, dass Microsoft nicht hinreichend deutlich darüber informiert, welche Daten sie als Verantwortliche erheben, was mit diesen geschieht und vor allem, wie lange sie gespeichert und für „eigene Zwecke" gehalten werden. Auch dies sind Informationen, die ein potentieller Vertragspartner zur Risikoanalyse kennen müsse, würden die Telemetrie- und Performancedaten doch gerade aus seiner Nutzung der Programme gewonnen. Auch hier fordert die DSK also Nachbesserung hinsichtlich der Transparenz.

Bei der Erhebung und Verarbeitung von Telemetrie-Daten vermutet die DSK zudem das Fehlen einer Erlaubnisgrundlage – zumindest was den Einsatz von Office 365 oder Microsoft 365 durch Behörden und öffentliche Stellen betrifft. Während bei privaten Nutzern ein berechtigtes Interesse von Microsoft an der Erhebung und Verarbeitung der Telemetriedaten im Sinne des Art. 6 Abs. 1 lit. f DSGVO vorliegen könnte, ist dieser Erlaubnisgrund auf Behörden und öffentliche Stellen nach Art. 6 Abs. 1 S. 2 DSGVO nicht anwendbar. An einer anderen Erlaubnisgrundlage, die zulassen würde, dass Behörden Daten von Bürgern oder Beschäftigten an Microsoft weitergeben, würde es dagegen in der Regel fehlen.

In der Zusammenschau dieser Erkenntnisse kommt der Arbeitskreis – und mit ihrem Beschluss auch knapp mehrheitlich die DSK – zu dem Ergebnis, dass Microsoft 365 / Office 365 jedenfalls im Januar 2020 nicht datenschutzkonform eingesetzt werden konnte.

Andere Ansicht: Aufsichtsbehörden

Diese Ansicht teilten 8 der 17 Aufsichtsbehörden nicht. In einer gemeinsamen Stellungnahme von 5 von ihnen legten diese ihre

Gründe für das „Nein"-Votum dar (Landesbehörden aus Baden-Württemberg, beide Behörden aus Bayern, Hessen und Saarland).

Die Kritik richtete sich nicht gegen die grundsätzliche Feststellung, dass es bei den Auftragsverarbeitungsverträgen und der sonstigen Datenverarbeitung durch Microsoft durchaus Verbesserungspotential gebe. Jedoch wollten die Aufsichtsbehörden das Ergebnis des Arbeitskreises deshalb nicht mittragen, weil es ihnen zu undifferenziert gewesen sei. So wurde kritisiert, dass die Vertragsfassungen der OST und DPA von Anfang 2020 die Grundlage der Untersuchung bildeten. Diese seien allein in dem Zeitraum bis zur Entschlussfassung im Juli 2020 zweimal überarbeitet worden. Auch hätten die Konsequenzen der Schrems II-Rechtsprechung des EuGH in der Analyse mehr Beachtung finden müssen. Schließlich wurde bemängelt, dass Microsoft vor der Beschlussfassung und auch durch den Arbeitskreis nicht angehört wurde – etwas, das in einem fairen, rechtsstaatlichen Verfahren eigentlich selbstverständlich ist.

Von Namen und technischen Einstellungen

Dieser Einschätzung schlossen sich auch Beobachter aus interessierten Kreisen an. Zusätzlich wurde kritisiert, dass die Betrachtung der Arbeitsgruppe sich rein auf die (veralteten) rechtlichen Aspekte der Auftragsverarbeitung konzentrierte, die technische Seite jedoch völlig außer Acht ließ. Dabei wurde auf die technischen Möglichkeiten, Einstellungen anzupassen, um den Datentransfer an Microsoft zu beschränken, überhaupt nicht eingegangen.

Hinzu kommt ein besonderes Schmankerl: Alle Aufsichtsbehörden nutzen in ihren Erläuterungen einen falschen Namen für das untersuchte Produkt. „Microsoft Office 365", so die behördliche Terminologie, gibt es nicht. Dafür jedoch „Microsoft 365" sowie „Office 365", das die klassischen Büro-Programme umfasst und nunmehr Teil der Produktpallette ist, die durch „Microsoft 365" abonniert werden kann. Für einige Beobachter scheint dieser Fehler die Oberflächlichkeit der Untersuchung zu bestätigen.

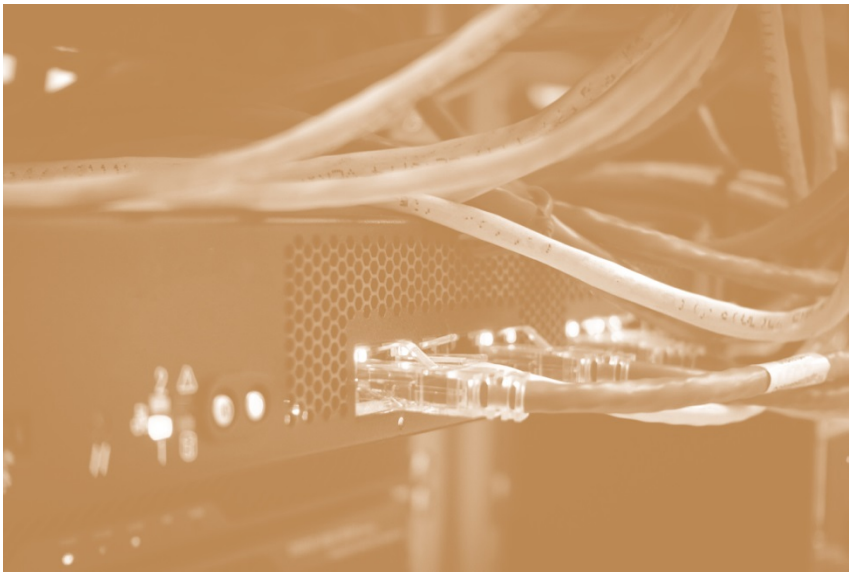
Verbot, ja oder nein?

Nun stellt sich die Frage, ob mit dem Beschluss die Verwendung von Microsoft 365 / Office 365 zumindest in den zustimmenden

Bundesländern untersagt ist. Dies ist nicht der Fall: Die DSK hat lediglich beschlossen, dass die Verarbeitung auf der Grundlage der Verarbeitungsverträge in der Fassung von Anfang Januar aus ihrer Sicht nicht datenschutzkonform möglich war. Über die derzeitigen Fassungen hat sie damit keine direkte Aussage getroffen. Insofern ist der Beschluss weniger aussagekräftig als anfangs vermutet und kann schon heute beinahe als historische Einschätzung verbucht werden. Hinzu kommt, dass der Beschluss bis heute nicht formal und final veröffentlicht ist.

Zudem ist die Untersuchung des Microsoft-Konzerns noch nicht abgeschlossen: Es wurde ein neuer Arbeitskreis eingesetzt, der – dieses Mal in Kooperation mit Microsoft – die Datenverarbeitungspraxis untersuchen und gemeinsam eine Lösung für die datenschutzkonforme Anwendung finden soll, vor allem auch, was die Thematik der Datenübermittlung in die USA angeht. Gerade die bislang fehlende Anhörung von Microsoft ist denn wohl auch der gravierendste und offensichtlichste Kritikpunkt am bisherigen Verfahren: Es ist nach wie vor gut möglich, dass im Austausch mit dem Hersteller eine auch aus Sicht der Aufsichtsbehörden oder jedenfalls der Gerichte datenschutzkonforme Lösung erreicht werden kann. In der Vergangenheit hat Microsoft etwa auch bereits mit der Datenschutzaufsichtsbehörde aus den Niederlanden konstruktive Lösungen gefunden.

Damit heißt es für alle Nutzer der Microsoft-Produkte erstmal weiterhin abzuwarten. Die Hoffnung bleibt, dass mit dem neuen Arbeitskreis zügig ein Ergebnis gefunden wird, das die berechtigten Bedenken der Datenschützer mit praktisch umsetzbaren Lösungen für Nutzer vereint. Ein klares „Ja“ zum rechtskonformen Einsatz von Microsoft 365 oder Office 365 kann aktuell nämlich ebenfalls nicht gegeben werden. Wir werden berichten.



Millionenbußgeld gegen 1&1: LG Bonn entscheidet über Grundsatzfragen

Seit Anfang Oktober verhandelt das Landgericht Bonn über das durch den BfDI verhängte Millionenbußgeld gegen den deutschen Telekommunikationsanbieter 1&1. Die Behörde wirft 1&1 vor, vor telefonischen Auskünften über Einzelverbindungen und Vertragsdetails keine hinreichend sichere Authentifizierung des Anrufers vorgenommen zu haben. Neben der mitunter technischen Fragestellung, welche Authentifizierungssysteme als Stand der Technik gegolten haben, hat das Landgericht erstmalig Gelegenheit, zu ganz grundlegenden Fragen der Bußgeldhaftung Stellung zu nehmen. So geht es etwa um das Bußgeldbemessungskonzept der Aufsichtsbehörden und die Frage, an wen ein Bußgeld überhaupt adressiert werden kann. Wir verfolgen das Verfahren für Sie vor Ort und berichten nachfolgend über die ersten Verhandlungstage.

Vorab ein Wort zum Verfahren selbst: Der Einspruch gegen den Bußgeldbescheid des BfDI mit Amtssitz in Bonn wird vor dem örtlich zuständigen Landgericht Bonn verhandelt. Im Verfahren selbst tritt neben der Datenschutzbehörde auch die Staatsanwaltschaft auf. Die Sache wird mündlich verhandelt, einschließlich der Vernehmung von Zeugen. So sagte am ersten Prozesstag bereits die Datenschutzbeauftragte von 1&1 als Zeugin aus.

Unmittelbares Unternehmensbußgeld?

Der Bußgeldbescheid des BfDI war ausschließlich gegen das Unternehmen gerichtet und nicht gegen persönlich handelnde Unternehmensvertreter. Die Verteidigung von *1&1* wirft im Verfahren nun die Frage auf, ob ein Unternehmensbußgeld nach deutschem Ordnungswidrigkeitenrecht hier überhaupt verhängt werden durfte. Nach § 30 OWiG kann ein Bußgeld nämlich nur unter besonderen Voraussetzungen gegen das Unternehmen selbst verhängt werden. Die Behörde äußerte dagegen, dass die Bußgeldhaftung eines Unternehmens im vorliegenden Fall unmittelbar aus der DSGVO folge und § 30 OWiG bei der Beantwortung der Frage außen vor bleiben müsse, auch weil die DSGVO das Verfahren in Art. 83 DSGVO abschließend regele.

Die Beantwortung dieser Rechtsfrage durch das Landgericht Bonn darf mit ganz besonderer Spannung erwartet werden. Hier geht es nicht nur um das grundlegende Verhältnis zwischen DSGVO und nationalen Bußgeldordnungen, sondern auch um die Frage, ob künftig natürliche Personen als Unternehmensvertreter Adressat von Bußgeldern sein werden. Denn das wäre wohl die Konsequenz einer Anwendung von § 30 OWiG und entspräche beispielsweise auch der Praxis des Bundeskartellamts bei Kartell-Bußgeldverfahren. Denkbar wäre auch, dass das Landgericht diese Frage dem EuGH zur Entscheidung vorlegt.

Bußgeldkonzept

Wie zu erwarten, war auch das von den deutschen Datenschutzaufsichtsbehörden veröffentlichte Bußgeldbemessungs-konzept Gegenstand reger Diskussionen. So äußerte bereits am ersten Prozesstag das Gericht, ob eine Kopplung des Bußgeldes an den Umsatz womöglich problematisch sei, wenn auch nicht aus der Luft gegriffen. Zumindest müsse man beachten, dass das Bußgeld nach dem Willen des Gesetzgebers in Art. 83 Abs. 1 DSGVO „abschreckend“ sein müsse.

Dass auch hier die Ansichten von Behörde und Bußgeldadressat weit auseinanderliegen, dürfte nicht verwundern. Zur Erinnerung: Das Bußgeldkonzept hatte für großen Wirbel gesorgt, weil es eine Art Tagessatzberechnung vorsieht, die sich am Jahresumsatz der gesamten Unternehmensgruppe, also einschließlich Mutter – und Konzernunternehmen orientiert, und nur geringen Spielraum für

eine Gewichtung des Inhalts der Verstöße belässt: Die Methodik führt bei großen Konzernen zu schwindelerregenden Bußgeldern selbst für kleine Verstöße.

Der BfDI ist im vorliegenden Verfahren der Auffassung, dass das Bußgeldkonzept die gesetzlichen Anforderungen nicht überspanne und letztlich Ausfluss des behördlichen Ermessens sei. Am Rande erwähnt die Behörde, dass ein neues Bußgeldkonzept in Arbeit sei, das aber noch nicht veröffentlicht werde.

Stand der Technik

Ferner wird das Landgericht Bonn die Möglichkeit haben, zur Auslegung des Art. 32 DSGVO Stellung zu nehmen und hier insbesondere zum Begriff des „Stands der Technik“. Der BfDI will hier in erster Linie auf die Marktverfügbarkeit abstellen. Daraus folgt, dass sich der Stand der Technik immer nach der sichersten Technik richtet, die am Markt verfügbar ist. 1&1 argumentiert, dass sich der Stand der Technik vielmehr aus einem Marktstandard ergebe, also den technischen Maßnahmen, die im Schnitt von allen Unternehmen am Markt implementiert werden. Zur Frage des „Stands der Technik“ soll nun ein Gutachten eingeholt werden, bevor die Verhandlung Ende Oktober fortgesetzt werden wird.

Mit großer Spannung darf der weitere Verlauf dieses Verfahrens erwartet werden.

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

Claudia Willmer
+49(0)221 65065-337
claudia.willmer@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