rechtAktuell

Sonderausgabe Datenschutzrecht

LOSCHELDER

Inhalt

rechtAktuell

Sonderausgabe Datenschutzrecht

Lieber Leserinnen und Leser,

Sie halten unsere Sonderausgabe anlässlich des Inkrafttretens der europäischen Datenschutz-Grundverordnung (DSGVO) am 25. Mai 2018 in den Händen. Unabhängig davon, ob die DSGVO Sie seit mehreren Monaten oder gar Jahren oder erst seit wenigen Wochen beschäftigt, ist eines sicher: Sie wird es auch weiterhin tun.
Die DSGVO hält in umfangreichen und oft unbestimmten Ausführungen zahlreiche offene Fragen bereit, die es in Zukunft zu klären gilt. Mit großem Interesse erwarten wir daher die ersten konkreten und verlässlichen Äußerungen von Behörden sowie die ersten Gerichtsverfahren.
Wir freuen uns darauf, Sie wie bisher rechtssicher und risikoangemessen durch die Untiefen des Datenschutzrechts zu begleiten, sei es bei der internen Organisation, im Bereich des Beschäftigtendatenschutzes oder beim Vertrieb Ihrer Leistungen und Produkte.
In dieser Sonderausgabe haben wir zahlreiche datenschutzrelevante Themen aus unseren verschiedenen Arbeitsbereichen zusammengetragen. Mit Sicherheit ist auch für Sie etwas dabei!

Viel Spaß beim Lesen wünschen Ihnen:

Dr. Detlef Grimm,
Dr. Kristina Schreiber,
Dr. Simon Kohm,
Dr. Jonas Kühne

Datenschutzrecht

Informationspflichten gem. Art. 13, 14 DSGVO

Einen wesentlichen Bestandteil des neuen Datenschutzrechts bildet der Transparenzgrundsatz (Art. 5 Abs. 1 lit. a DSGVO), der sich insbesondere in umfassenden und bisher so nicht im Gesetz existierenden Informationspflichten äußert. Zukünftig sind die Betroffenen über die Einzelheiten der Datenverarbeitung in angemessener Art und Weise zu informieren. Für Unternehmen stellen sich diese rechtlichen Pflichten mehr und mehr als Herausforderung dar.

Zeitpunkt der Information

Der Zeitpunkt der Information bestimmt sich danach, ob es sich um eine Datenerhebung beim Betroffenen selbst oder bei einem Dritten handelt. So hat regelmäßig die Unterrichtung bereits bei Erhebung zu erfolgen oder, wenn die Erhebung beim Dritten erfolgt, unverzüglich im Anschluss an den Erhalt der Daten.

Form und Inhalt der Information

Auch die Wahl der Form und des Inhalts der Information trägt maßgeblich zur Herstellung größtmöglicher Transparenz bei. Die Informationen sind in einer Art und Weise zugänglich zu machen, in der sie gut wahrnehmbar sind. Das bedeutet, dass regelmäßig der Informationsweg zu nutzen ist, welcher üblicherweise bei der Korrespondenz mit dem Betroffenen genutzt wird (also z.B. per E-Mail, falls mit dem Betroffenen per E-Mail korrespondiert wird).

Erforderlich ist zudem, dass der Inhalt der Information konkret, detailliert und verständlich formuliert wird. Es muss ein Maß gefunden werden, welches über die abstrakte Angabe hinausgeht, aber nicht dazu führt, dass Informationen unverständlich werden.

Allgemeine Informationspflichten

Folgende Informationspflichten bestehen für jegliche personenbezogene Datenverarbeitung mit einzelnen Modifikationen je nach Art der Verarbeitung:

- Kontaktdaten des Verantwortlichen und des Datenschutzbeauftragten (wenn notwendig und bestellt): Für den Betroffenen ist es von enormer Bedeutung, einen Ansprechpartner für die Ausübung seiner Rechte zu haben und diesen auf einfachem Wege erreichen zu können.

- Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen

- Kategorien der verarbeiteten personenbezogenen Daten
- Rechtsgrundlagen der Verarbeitung: Neben der Verarbeitung aufgrund einer Einwilligung ist die bedeutsamste Rechtsgrundlage die Verarbeitung aufgrund eines überwiegenden berechtigten Interesses. Bei letzterem ist auf die Darlegung der Kernaspekte der Interessenabwägung zu achten.
- Ggf. Empfänger oder Kategorien von Empfängern der personenbezogenen Daten
- Ggf. Absicht einer Drittlandübermittlung: Dabei müssen die getroffenen Schutzvorkehrungen, die ein hinreichendes Datenschutzniveau im Zielland absichern, angegeben werden.
- Speicherdauer: Die Speicherdauer sollte möglichst angegeben werden oder, falls dies nicht umsetzbar ist, die Kriterien, nach denen die Dauer festlegt wird.
- Betroffenenrechte: Hinweise auf das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten, sowie auf Berichtigung, Löschung, Einschränkung der Verarbeitung, eins Widerrufs- oder Widerspruchsrecht gegen die Verarbeitung und das Recht auf Datenübertragbarkeit müssen dem Betroffenen zur Verfügung gestellt werden. Dabei ist das Widerrufs- oder Widerspruchsrecht hervorzuheben.

Online-Präsenz

Unternehmen müssen auch frühzeitig die datenschutzkonforme Gestaltung ihres Online-Auftritts vorbereiten. Viele Websites – aber noch lange nicht jede – haben bereits eine Datenschutzerklärung, welche jedoch der Anpassung an die neue Rechtslage bedarf und im Hinblick auf den Inhalt der Informationen umfangreicher zu gestalten ist. Beispielsweise ist zukünftig über die Rechtsgrundlage jeder einzelnen Datenverarbeitung genauso zu informieren wie über die Speicherdauer und den/die Zweck(e), der/die die Datenverarbeitung in diesem Umfang rechtfertigt/rechtfertigen. Dabei muss jede Funktion der Website gesondert betrachtet und bewertet werden, um den im Gesetz vorgesehenen Informationspflichten gerecht zu werden.
Je nach Ausmaß der genutzten Funktionen (Cookies, Social Media, Webanalyse etc.) wird es nicht ausbleiben, dass der Umfang der Datenschutzerklärung weiter zunehmen wird.

Um dem Erfordernis des Informationszeitpunkts („bei Erhebung“) gerecht zu werden, sollte die Datenschutzerklärung über einen Klick, beispielsweise im Header oder im Footer neben dem Impressum, erreichbar sein.


Datenschutzerklär
htigt werden, die wi
e vorgenommen hab
g zu Transparenz be
ufbewahrung Ihrer D
ngen vorgenommer
opäischen

Die neue und vielschichtige Terminologie der DSGVO

Einwilligung, Opt-in/Opt-out, Informationspflichten, Datenschutzerklärung: Die DSGVO macht es dem Anwender nicht leicht, die verschiedenen datenschutzrechtlichen Begrifflichkeiten und Instrumente auseinanderzuhalten. Zeit und Anlass für uns, mit der nachfolgenden Darstellung Unklarheiten zu beseitigen.

Die Einwilligung als datenschutzrechtliche Erlaubnis

Die Einwilligung dient dazu, eine Datenverarbeitung individuell zu erlauben. Sie erweitert also die Rechte der verantwortlichen Stelle, erfordert aber auch eine eindeutige und nachweisbare Willensbetätigung des Kunden (im Onlinebereich bspw. durch eine Klickbox sichergestellt, im Offlinegeschäft durch eine Unterschrift).
Das klingt zunächst realisierbar. Die Einwilligung hat in der Praxis aber auch zahlreiche Nachteile. So kann sie regelmäßig nicht mit dem Abschluss eines Vertrages oder der Erbringung einer Leistung gekoppelt werden und der Betroffene kann sie jederzeit widerrufen. Unternehmen tun daher gut daran, stets vorab zu prüfen, ob eine Einwilligung überhaupt erforderlich ist oder ob nicht die Datenverarbeitung aus Gründen der Vertragserfüllung oder aufgrund des eigenen berechtigten Interesses erlaubt ist. Der Betroffene muss dann weder einwilligen noch „zustimmen“ oder sich auf andere Art und Weise einverstanden erklären.

Die Betroffeneninformation als datenschutzrechtliche Pflicht

Unabhängig davon, ob eine Datenverarbeitung aufgrund einer Einwilligung erfolgt oder gesetzlich erlaubt ist, muss der Betroffene künftig über die Einzelheiten der Datenverarbeitung informiert werden (Art. 13, 14 DSGVO). Für das Verständnis ist wichtig, dass diese Informationspflicht die Rechte der verantwortlichen Stelle nicht erweitert; mit der Information kann also keine datenschutzrechtliche Erlaubnis herbeigeführt werden. Unter anderem deswegen muss der Betroffene diese Information auch nicht „bestätigen“ oder in sie „einwilligen“. Ausreichend ist, dass er sie in angemessener Art und Weise zur Kenntnis nehmen kann. Im Onlinebereich erfolgt dies regelmäßig über eine zentral hinterlegte „Datenschutzerklärung“, wobei dieser Begriff nicht zwingend genannt oder verwen-

det werden muss. Aus dem zuvor Gesagten folgt, dass der Nutzer einer Website an keiner Stelle bestätigen oder ausdrücklich erklären muss, dass er mit der Datenschutzerklärung einverstanden ist oder sie gelesen hat etc.

Schnittmenge zwischen Einwilligung und Betroffeneninformation

Die Schnittmenge zwischen Einwilligung und Betroffeneninformation ist erreicht, wenn die DSGVO eine informierte Einwilligung verlangt, der Betroffene also letztlich wissen muss, in was er einwilligt. In vielen Fällen mag es sich dann anbieten, die Einholung der Einwilligung mit der Informationspflicht zu verbinden, wobei dann darauf zu achten ist, dass die Einwilligungserklärung deutlich hervorgehoben wird.

Sonstiges

Daneben ist die Verwendung der Begriffe „Opt-in“ und „Opt-out“ gebräuchlich, wobei ersterer regelmäßig eine Situation meint, in welcher der Betroffene im Rechtssinne einwilligt und letzter eine Situation, in welcher der Betroffene die Möglichkeit erhält, eine laufende Datenverarbeitung mit Wirkung für die Zukunft zu stoppen. Aktualität haben diese Begriffe derzeit auch, weil die deutschen Datenschutzbehörden mit einem neuen Positionspapier Furore machen, wonach die Verwendung von Web-Tracking-Anwendungen nur nach einer Einwilligung möglich sein soll. Hier müsste der Nutzer also per „Opt-in“-Banner auf der Startseite einwilligen.

Gilt die DSGVO auch für Softwarehersteller?

Das Inkrafttreten der DSGVO hat auch Einfluss auf Entwickler und Anbieter von Software, Apps und Online-Anwendungen, die anderen Unternehmen die (elektronischen) Werkzeuge für die Verarbeitung personenbezogener Daten zur Verfügung stellen. Dass sie deswegen jedenfalls mittelbar von den Anforderungen der DSGVO betroffen sind, zeigt dieser Beitrag.

Bußgelder für Softwarehersteller?

Die DSGVO enthält in Art. 25 DSGVO spezielle Verpflichtungen zu datenschutzfreundlichen Technikgestaltungen und zu datenschutzfreundlichen Voreinstellungen. Das beinhaltet unter anderem, wenn möglich eine Anonymisierung personenbezogener Daten vorzunehmen oder die Software derart zu gestalten, dass der Verantwortliche die Möglichkeit erhält, Daten möglichst sparsam verarbeiten und auch löschen zu können. Die DSGVO adressiert diese Rechtspflichten nach weit vorherrschender Meinung allerdings an die datenschutzrechtlich Verantwortlichen, also an die Personen und Unternehmen, die über die Zwecke und Mittel einer Datenverarbeitung in eigener Verantwortung entscheiden. Nach Erwägungsgrund 78 sollen die Hersteller von Software allenfalls „ermutigt“ werden, die datenschutzrechtlichen Vorgaben zu berücksichtigen und sicherzustellen, dass etwa die Verantwortlichen ihren datenschutzrechtlichen Pflichten nachkommen können. Softwarehersteller müssen daher nicht damit rechnen, unmittelbar Adressat behördlicher Maßnahmen wie Abstellungsverfügungen oder Bußgeldbescheiden zu werden. Anders sind allerdings Fälle zu beurteilen, in denen Softwarehersteller ihrerseits Cloud-Leistungen anbieten oder per Fernwartung auf den Systemen von Kunden personenbezogene Daten verarbeiten. In diesen Fällen stellen die Softwarehersteller nicht bloß ein Werkzeug zur Datenverarbeitung zur Verfügung und müssen daher unmittelbar die datenschutzrechtlichen Pflichten aus der DSGVO erfüllen.

Vertragliche Risiken

Auch in anderen Fällen können Softwarehersteller die Anforderungen an die DSGVO nicht ignorieren. Auch wenn sie nicht selbst und unmittelbar Adressat behördlicher Maßnahmen sein können, gehen mit der Einführung der DSGVO erhebliche Risiken für Softwarehersteller einher. Diese liegen im vertraglichen Bereich und realisieren sich dann, wenn der Hersteller den Kunden vor Kauf/Miete und Aktivschaltung der Software nicht über datenschutzrechtliche Risiken und Voreinstellungen informiert oder wenn sich ein Produkt angesichts der Produktbeschreibung als mangelhaft herausstellt. In diesen Fällen kann der Kunde je nach Einzelfall Nachbesserung/Mangelbeseitigung fordern oder wenn der Hersteller den Mangel zu verschulden bzw. den Kunden schuldhaft nicht aufgeklärt hat, Schadensersatz verlangen. Im äußersten Fall mag dieser Schadensersatz sogar ein behördliches Bußgeld umfassen.

Vorsorge und Strategie

Hersteller tun daher gut daran, diesen Risiken aktiv zu begegnen. Dazu gehört zunächst, den Kunden je nach Kenntnisstand hinreichend über datenschutzrechtliche Risiken aufzuklären und ihm die datenschutzrelevanten Funktionalitäten

(bspw. Löschfunktionalitäten) transparent zu erläutern. Bezüglich ihrer Art und ihres Umfangs muss eine solche Aufklärung im Einzelfall und mit Augenmaß betrieben werden. Ferner sollten Hersteller ihre Vertragsunterlagen durchsehen und prüfen, ob hier Fallstricke lauern, vor allem die Nachbesserung bereits verkaufter/vermieteter Produkte betreffend. Zu den Vertragsunterlagen gehören nicht nur eine – wenn überhaupt vorhandene – Vertragsurkunde, sondern in der Praxis regelmäßig auch die AGB zum Softwarekauf, zur Miete und/oder Pflege und Wartung sowie Aussagen aus der Produktbeschreibung (online und offline).

Für Softwarehersteller wird es in Zukunft ein Wettbewerbsvorteil und ein „unique selling point" sein, das eigene Produkt als „100% DSGVO konform" oder „DSGVO-compliant" bewerben zu können. Allerdings muss dies dann unter Berücksichtigung des aktuellen Rechtsstandes eindeutig sein, weil die Risiken der Mängelgewährleistung und des Schadensersatzes ansonsten erheblich sind. Ob und inwieweit der Markt künftig nur noch derartige Produkte erwartet, bleibt abzuwarten und hängt vor allem mit der datenschutzrechtlichen Sensibilität der Kunden und wiederum deren Endkunden zusammen.

Bei Fragen zum Datenschutzrecht stehen Ihnen gerne zur Verfügung:

Dr. Kristina Schreiber
+49 (0) 221 650 65-337
kristina.schreiber@loschelder.de

Dr. Simon Kohm
+49 (0) 221 650 65-200
simon.kohm@loschelder.de

Beschäftigtendatenschutzrecht

Der datenschutzrechtliche „Beipackzettel“ zum Arbeitsvertrag

Art. 13, 14 DSGVO verpflichten datenverarbeitende Stellen, gegenüber Betroffenen umfangreiche Hinweise zu erteilen, wenn sie deren personenbezogene Daten automatisiert oder in Dateisystemen verarbeiten. In sämtlichen Beschäftigungsverhältnissen kommt es zwingend zu hinweispflichtigen Datenverarbeitungsprozessen. Alle Unternehmen müssen deshalb datenschutzrechtliche Hinweisschreiben entwerfen und sämtlichen Arbeitnehmern, Auszubildenden und Praktikanten vorlegen. Dies erfolgt typsicherweise als „Beipackzettel“ zum Arbeitsvertrag.

Werden Daten automatisiert oder in Dateisystemen verarbeitet, muss die datenverarbeitende Stelle die Betroffenen gemäß Art. 13, 14 DSGVO informieren. Dem Betroffenen müssen die Kontaktdaten des verantwortlichen Rechtsträgers, die Kontaktdaten des Datenschutzbeauftragten, der Zweck der Datenverarbeitung, die Rechtsgrundlagen, mögliche externe Empfänger sowie die bestehenden Lösch- und Aufbewahrungsfristen mitgeteilt werden. Weiter ist der Betroffene eingehend über seine Rechte zu belehren. Erfolgt die Datenerhebung beim Betroffenen selbst, ist ihm mitzuteilen, ob er zur Auskunft verpflichtet ist. Erfolgt die Datenerhebung aus anderen Quellen, sind dem Betroffenen diese Quellen mitzuteilen.

All dies gilt auch für die Datenverarbeitung in Beschäftigungsverhältnissen mit Arbeitnehmern, Auszubildenden oder Praktikanten. Selbstverständlich wäre es nicht praktikabel, Beschäftigte bei jedem Datenverarbeitungsvorgang gesondert und immer wieder aufs Neue zu informieren.

Stattdessen sollte jedes Unternehmen ein Mitteilungsschreiben als einheitliches Formular erstellen, welches die vorgeschriebenen Informationen für sämtliche Datenverarbeitungsprozesse enthält, die es im Zusammenhang mit Beschäftigungsverhältnissen regelmäßig praktiziert. Dieses Mitteilungsschreiben sollte allen Beschäftigten übergeben oder per E-Mail übermittelt werden. Wenn zukünftig Mitarbeiter eingestellt werden, sollte das Mitteilungsschreiben als datenschutzrechtlicher „Beipackzettel“ mit dem Arbeitsvertrag übergeben und unterzeichnet werden.

Bislang ist weitgehend ungeklärt und in der rechtswissenschaftlichen Literatur umstritten, wie konkret die Mitteilungen erfolgen müssen. Es spricht viel dafür, dass sich die Mitteilung nicht in formelhaften Wendungen erschöpfen darf, sondern den Beschäftigten ein anschauliches Bild davon vermitteln muss, mit welchen Datenverarbeitungsprozessen sie im Arbeitsverhältnis konkret zu rechnen haben. Unternehmen sollten durch eine konkrete und eindeutige Information auf Nummer sicher gehen. Insbesondere muss der Beschäftigte über die Dauer sämtlicher Löschfristen informiert werden. Hierzu sollte der datenschutzrechtliche „Beipackzettel“ genau mit den im Unternehmen geltenden Löschfristen abgestimmt werden, die im datenschutzrechtlichen Löschkonzept definiert wurden.

Wir unterstützen Sie bei der Formulierung des datenschutzrechtlichen „Beipackzettels“ und stellen Ihnen Mustervorlagen auf Wunsch gerne zur Verfügung.

Datenschutz im Bewerbermanagement

Das Bewerberportal eines Unternehmens ist sein datenschutzrechtliches Aushängeschild: Durch einen flüchtigen Blick auf die Unternehmenswebseite kann sich jeder Außenstehende hier sofort ein Bild von den datenschutzrechtlichen Bemühungen eines Unternehmens verschaffen. Auf den Umgang der Unternehmen mit Bewerbungsunterlagen legen Datenschutzbehörden zudem besonderes Augenmerk. Dies überrascht nicht, geben Bewerbungsunterlagen doch einen sensiblen Einblick in das Persönlichkeitsprofil und den Werdegang einer Person. Arbeitgeber sollten der datenschutzkonformen Ausgestaltung ihres Bewerberportals deshalb Priorität einräumen.

Die Datenschutzbehörden beabsichtigen, den Umgang mit Bewerbungsunterlagen gesondert zu prüfen und haben zu diesem Zweck bereits detaillierte Prüfungsfragebögen veröffentlicht. Unternehmen müssen ihre Karriere-Webseiten und Bewerberportale anpassen, wozu wir dringend raten. Bedenken Sie, dass Datenschutzbehörden mit einem flüchtigen Blick auf die Karriere-Webseite Ihres Unternehmens sofort ersehen können, ob sich Ihr Unternehmen mit der Implementierung von Datenschutzprozessen auseinandergesetzt hat oder ob es die neuen Anforderungen ignoriert. Jeder Datenschutzerklärung sieht man ohne weiteres an, ob sie sich noch an der alten Rechtslage oder den Anforderungen der DSGVO orientiert.

Damit im Bereich des Bewerbermanagements keine datenschutzrechtlichen Verstöße festgestellt werden, sollten Arbeitgeber folgende Maßnahmen umsetzen:

1. Arbeitgeber müssen Bewerbern nach Art. 13 DSGVO unbedingt einen datenschutzrechtlichen Hinweis geben, der über den Umgang mit Bewerberdaten, insbesondere den eingereichten Bewerbungsunterlagen, aufklärt. Dieser Hinweis sollte sichtbar auf der Karriere-Webseite eines jeden Unternehmens veröffentlicht werden und zwar so, dass er sowohl für Initiativbewerber als auch bei Bewerbungen auf bestimmte Stellen keinesfalls übersehen werden kann.

   Auf Anfrage stellen wir Ihnen Formulare zur Verfügung, die auf den Bewerbungsprozess in Ihrem Unternehmen zugeschnitten sind.

2. Bewirbt sich ein Bewerber auf eine bestimmte Stelle, darf die Bewerbung nach Auffassung der Datenschutzbehörden im Grundsatz nur für die Entscheidung zur Besetzung

genau dieser Stelle herangezogen werden. Im Unternehmen darf also nicht unter Weiterleitung der Bewerbungsunterlagen „herumgefragt“ werden, ob andere Führungskräfte Bedarf nach „solch einem Bewerber“ haben.

Anders ist dies, wenn der Arbeitnehmer in eine solche Verwendung seiner Bewerbungsunterlagen ausdrücklich einwilligt. Dann ist deren Weiterleitung auch zulässig, um andere Einsatzmöglichkeiten im Unternehmen zu prüfen. Wenn Sie auf Ihrer Unternehmenswebseite ein Bewerbungsportal zur Verfügung stellen, sollten Sie für diese Einwilligung eine Ankreuz-Option veröffentlichen. In den Voreinstellungen darf das Kästchen noch nicht angekreuzt sein („Opt-in“ statt „Opt-out“). E-Mail-Bewerber können Sie in Stellenausschreibungen ausdrücklich dazu auffordern, im Bewerbungsanschreiben eine Einwilligung dazu abzugeben, dass die Bewerbungsunterlagen auch zur Besetzung weiterer Stellen herangezogen werden.

Demgegenüber dürfen Sie Initiativbewerbungen grundsätzlich zur Besetzung sämtlicher in Betracht kommender Stellen heranziehen und ihren Inhalt sämtlichen Führungskräften bekannt geben, die in Betracht kommende Einstellungsentscheidungen treffen. Dies entspricht regelmäßig dem Willen des Initiativbewerbers.

3. Zum Umgang mit Bewerbungsunterlagen und Bewerberdaten müssen Prozesse definiert und in schriftlicher Form bekannt gegeben werden. Zum einen muss festgelegt werden, welche Personen in Bewerbungsunterlagen zu welchem Anlass Einsicht nehmen dürfen. Zum anderen muss untersagt werden, dass Beteiligte zahlreiche Sicherheitskopien von Bewerbungsunterlagen erstellen, so dass diese nicht mehr überblickt werden können. Eine beliebige Weiterleitung von Bewerbungsunterlagen an alle Neugierigen und die Anfertigung beliebiger Sicherungskopien ist unter der neuen Rechtslage nicht mehr zulässig und muss ausdrücklich untersagt werden.

Zum anderen müssen Löschfristen für die Bewerbungsunterlagen festgelegt werden. Sobald unter keinem Gesichtspunkt mehr ein berechtigtes Interesse an der Verwahrung der Bewerbungsunterlagen besteht, muss die letzte im Unternehmen vorhandene elektronische Kopie gelöscht werden. Dies folgt aus Art. 17 DSGVO.

- Bewerbungsunterlagen dürfen selbstverständlich während der Dauer des Bewerbungsverfahrens zum Zwecke seiner Durchführung gespeichert werden und müssen nicht gelöscht werden, solange keine endgültige Absage erfolgt ist.

- Nach der Absage des Bewerbers dürfen die Bewerbungsunterlagen weitere drei bis sechs Monate gespeichert werden, um sie als Beweismittel für einen möglichen Entschädigungsprozess wegen behaupteter Bewerber-Diskriminierung (vgl. § 15

Abs. 2 u. Abs. 4 AGG) vorzuhalten. Zu diesem Zeitpunkt benötigt streng genommen nur noch die Rechtsabteilung Zugriff auf die Bewerbungsunterlagen. Hierzu kann eine zentrale Datenbank mit automatisierten Löschfristen eingerichtet werden, wobei die Löschfristen bei Abschluss des Bewerbungsverfahrens „scharf" zu schalten wären. Es spricht viel dafür, dass alle Beteiligten bei Abschluss des Bewerbungsverfahrens sämtliche sonstige elektronische Kopien der Bewerbungsunterlagen löschen und Papierausdrucke vernichten sollten.

- Bei Initiativbewerbern und Bewerbern, die einer Verwendung ihrer Bewerbungsunterlagen auch für andere Stellenbesetzungen eingewilligt haben, können die Bewerbungsunterlagen zu diesem Zweck für einen Zeitraum von ca. einem Jahr den in Betracht kommenden Entscheidern im Unternehmen zur Verfügung gestellt werden. Typischerweise werden die Bewerbungsunterlagen hierzu in einer Datenbank im Unternehmensintranet für definierte Berechtigte für den Zugriff freigegeben. Bewerbungsunterlagen, die älter als ein Jahr sind, entfalten für Stellenbesetzungen keine signifikante Aussagekraft mehr und dürfen zu diesem Zweck nicht mehr aufbewahrt werden. In der Bewerberdatenbank sollte deshalb eine Lösch- oder Sperrroutine implementiert werden, die nach einem Jahr automatisch ausgelöst wird.
- Datenschutzbehörden legen Wert darauf, dass sämtliche Papierausdrucke von Bewerbungsunterlagen entweder zurückgegeben oder im Aktenvernichter zerschreddert, nicht aber im normalen Müll entsorgt werden.

Die Datenschutzbehörden erwarten, dass solche Prozesse in schriftlichen Dienstanweisungen bekanntgegeben und in regelmäßigen Schulungen besprochen werden. Dass einzelne Mitarbeiter gelegentlich gegen diese Vorgaben verstoßen, lässt sich natürlich nicht vermeiden.

4. Wenn Sie Bewerberfragebögen verwenden, müssen die dort gestellten Fragen zulässig sein. Fragen nach Familienverhältnissen, Geburtsort, Nationalität oder Alter gelten z.B. im Grundsatz als unzulässig. Sie sollten nicht in standardisierten Bögen enthalten sein, welche womöglich auf der Unternehmenswebseite veröffentlicht werden und der Datenschutzbehörde sofort ins Auge springen.

Anpassung von Datenverarbeitungsvorgängen – Was ist im HR-Bereich zu tun?

Unternehmen müssen seit dem 25.05.2018 über ein DSGVO-konformes Datenmanagement verfügen. Mit Blick auf die Beschäftigtendaten bleibt diese Aufgabe oft an den Personalabteilungen hängen. Unsere Checkliste zeigt Ihnen, was bei der Anpassung von Personaldatenverarbeitungsprozessen zu tun ist. Die größte Herausforderung besteht in der Implementierung von Löschkonzepten.

Ein großer Teil der von Unternehmen verarbeiteten personenbezogenen Daten sind Beschäftigtendaten. Ihren Umgang mit Beschäftigtendaten sollten Unternehmen anlässlich der Geltungserlangung der DSGVO unbedingt hinterfragen. Wenn der Datenschutzbeauftragte nicht aktiv wird, sollten die Personalabteilungen handeln. Orientieren Sie sich hierzu an unserer Check-Liste:

1. Sämtliche Datenverarbeitungsvorgänge im Unternehmen müssen nach Art. 30 DSGVO in einem Verzeichnis von Verarbeitungstätigkeiten erfasst werden. Bei einer Prüfung werden die Datenschutzbehörden zuallererst diese Verzeichnisse anfordern und darin nach sensiblen Vorgängen suchen. Für den datenschutzrechtlichen Compliance-Prozess ergibt sich aus dem Verzeichnis der Verarbeitungsvorgänge die maßgebliche To-Do-Liste: Jeder der dort aufgeführten Datenverarbeitungsvorgänge muss auf seine datenschutzrechtliche Rechtfertigung hin überprüft und gegebenenfalls angepasst werden.

2. Im Ausgangspunkt stellt sich für jeden Datenverarbeitungsvorgang die Frage, ob er im Ganzen oder womöglich nur teilweise gerechtfertigt ist. Allgemein gesprochen ist zu prüfen, ob der Vorgang zum Zwecke der Durchführung des Beschäftigungsverhältnisses oder zur Verfolgung anderweitig legitimer Interessen erforderlich und verhältnismäßig ist (Art. 6 Abs. 1 lit. c u. f. DSGVO i.V.m. § 26 Abs. 1 Satz 1 u. 2 BDSG n.F.). Was dies im Einzelnen bedeutet, ist weitgehend ungeklärt. Unter dem bislang geltenden Bundesdatenschutzgesetz wurden zur datenschutzrechtlichen Rechtfertigung von Personalverarbeitungsvorgängen kaum gerichtliche Entscheidungen veröffentlicht, da das Datenschutzrecht bislang an einem Durchsetzungsdefizit litt. Dies wird sich nunmehr unter der Geltung der DSGVO ändern. Bis die ersten gerichtlichen Entscheidungen veröffentlicht werden, müssen sich Arbeitgeber in vielen Punkten jedoch erst einmal auf ihr Bauchgefühl verlassen.

Wir raten nicht zu überzogener Angst vor datenschutzrechtlichen Sanktionen. Unternehmen, die Ihre Datenverarbeitungsvorgänge systematisch hinterfragen, tun derzeit bereits mehr, als ein großer Teil ihrer Mitbewerber. Solche Unternehmen werden in den Augen der Datenschutzbehörden nicht als die „schwarzen Schafe“ erscheinen. Bevor bei bestehenden sinnvollen Datenverarbeitungsvorgängen schmerzhafte Einschränkungen vorgenommen werden, sollte besser abgewartet werden, bis sich die Rechtslage nach und nach klärt. Schon jetzt erkennen Datenschutzbehörden übrigens an, dass es grundsätzlich der unternehmerischen Freiheit des Arbeitgebers unterliegt, darüber zu entscheiden, welche Datenverarbeitungsprozesse erforderlich sind und welche nicht.


>>
>>
>>delete

Im Arbeitsverhältnis übliche Datenverarbeitungsvorgänge wie die Lohnbuchhaltung, die Arbeitszeiterfassung sowie das Führen einer Personalakte mit dem üblichen Inhalt (Arbeitsverträge, Bewerbungsunterlagen, Zeugnisse, Abmahnungen, Zielvereinbarungen) dürfen selbstverständlich fortgesetzt werden.

Kritischer sollte die Gestaltung interner Mitarbeiterportale, Leistungsdokumentationen oder besonderer Überwachungsmaßnahmen hinterfragt werden. Die Ergebnisse von Mitarbeiterbefragungen und Untersuchungen sollten i.d.R. anonymisiert dokumentiert und ausgewertet werden. Bei besonders sensiblen Vorgängen sollten Unternehmen eine Datenschutz-Folgeabschätzung nach Art. 35 DSGVO durchführen und schriftlich dokumentieren.

Ganz unzulässig wäre es, eine verdachtsunabhängige heimliche Dauerüberwachung von Mitarbeitern einzurichten, Geheimdossiers zu Details ihrer privaten Lebensführung auf Vorrat anzulegen oder Mitarbeiterdaten ohne Anonymisierung und Zustimmung an Datenhändler zu verkaufen. Derartige Maßnahmen kamen bei der überwiegenden Zahl der Arbeitgeber aber auch in der Vergangenheit nicht vor. Werden Unternehmen bei solchen Maßnahmen durch Datenschutzbehörden „ertappt“, muss künftig mit schmerzhaften Bußgeldsanktionen gerechnet werden.

3. Für die Einsichtnahme in bestimmte Mitarbeiterdaten, z.B. die Personalakte, die Arbeitszeiterfassung, angelegte BEM-Akten, die Lohnbuchhaltungsunterlagen oder bestimmten Angaben in elektronischen Mitarbeiterportalen müssen Berechtigungskonzepte definiert werden. Solche Berechtigungskonzepte haben auch in der Vergangenheit existiert, zumindest als gelebte Praxis. Bei der überwiegenden Zahl von Unternehmen dürfte kaum Anpassungsbedarf bestehen. Generell gilt: Es ist sinnvoll, eine gelebte Praxis als offizielle Richtlinie oder in Form einer Betriebsvereinbarung zu verschriftlichen, um gegenüber den Datenschutzbehörden belegen zu können, dass ein strukturierter Prozess etabliert wurde.

4. Neu ist hingegen, dass die Unternehmen für sämtliche Datentypen Löschfristen definieren müssen. Hierbei sind Unternehmen im Vorteil, die ihre Personalakten nicht in Papierform, sondern elektronisch führen. In der elektronischen Personalakte können automatisierte Löschroutinen implementiert werden, die nicht von Hand überwacht werden müssen. Spätestens, sobald sich die IT-Dienstleister auf die Vorgaben der DSGVO eingestellt haben und die ersten „Update-Wellen“ überstanden sind, spricht viel dafür, von der Papierakte zur elektronischen Personalakte zu wechseln.

   Bei der Festlegung von Löschfristen beraten wir nach folgender Maxime: Das Wichtigste ist, dass überhaupt sachlich begründbare Löschfristen existieren. Auf keinen Fall sollten Löschfristen zu kurz bemessen werden. Werden Daten unwiederbringlich gelöscht, können sie auch in unerwarteten Notfällen nicht mehr zurückgeholt werden und das Unternehmen ist hilflos und blind. Aus unserer Sicht sollten die Löschfristen daher großzügig bemessen werden. Z.B. verjähren Ansprüche auf Betriebsrenten erst 30 Jahre nach dem Tod des Arbeitnehmers und können bis dahin noch durch Witwen und Waisen gerichtlich

geltend gemacht werden (§ 18a BetrAVG). Um solchen Ansprüchen entgegentreten zu können, empfehlen wir, Arbeitsvertragsunterlagen und sämtliche Dokumentationen zu Betriebsrentenbeiträgen typisiert erst 100 Jahre nach Einstellung des Arbeitnehmers zu löschen. Es wird sich mittelfristig zeigen, welche Position Datenschutzbehörden und Gerichte zu diesem großzügigen Verständnis beziehen. Für bereits unwiederbringlich gelöschte Daten ist es dann aber zu spät.

Auf Wunsch stellen wir Ihnen gerne eine Übersicht über die von uns für zulässig und zweckmäßig gehaltenen Löschfristen zur Verfügung.

Damit Löschfristen nicht leerlaufen, sollte den Mitarbeitern übrigens untersagt werden, sich weitere elektronische Kopien sensibler Beschäftigtendaten auch auf ihrem Dienstrechner anzufertigen. Dieses Verbot sollte in schriftlichen Dienstanweisungen veröffentlicht werden.

5. Wenn Unternehmen Personaldatenverarbeitungen, insbesondere die Lohnbuchhaltung, durch einen Drittdienstleister vornehmen lassen, handelt es sich um eine Auftragsverarbeitung (früher: „AuftragsDATENverarbeitung“). Hierbei muss das Unternehmen mit dem Drittdienstleister einen schriftlichen Vertrag zur Auftragsverarbeitung schließen, der die Vorgaben nach Art. 28 Abs. 3 DSGVO erfüllt. Altverträge mit Auftragsdatenverarbeitern nach § 11 BDSG a.F. müssen an die neue Rechtslage angepasst werden.

   Erfolgt die Personaldatenverarbeitung konzernübergreifend in einer Personalabteilung des Mutterunternehmens auch für verschiedene Tochterunternehmen, treten Mutter- und Tochterunternehmen als gemeinsame Verantwortliche nach Art. 26 DSGVO auf. Hierbei müssen die wechselseitigen Rechte und Pflichten in einer besonderen, schriftlichen Vereinbarung festgelegt werden.

   Kommt es zu einer Überprüfung durch die Datenschutzbehörde, sollte Ihr Unternehmen die vorgeschriebenen schriftlichen Verträge vorlegen können. Bei der Vertragsgestaltung können Sie auf unsere lösungsorientierte Unterstützung vertrauen. Insbesondere, wenn Sie Daten ins außereuropäische Ausland übermitteln, sollten Sie sich rechtlich beraten lassen.

6. Beschäftigte genießen hinsichtlich erhobener personenbezogener Daten nach Art. 15 ff. DSGVO eine Reihe von Rechten, nämlich auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragung und Widerspruch. Für den Fall, dass derartige Rechte geltend gemacht werden, müssen Zuständigkeiten und Prozesse definiert werden. Zuständigkeiten und Prozesse müssen ebenfalls feststehen, wenn personenbezogene Daten derart verletzt werden, dass gemäß Art. 33 DSGVO eine Meldung bei der Datenschutzbehörde zu erfolgen hat.

Neue Anforderungen an die datenschutzrechtliche Einwilligung

Wir raten allen Arbeitgebern, bei ihren Mitarbeitern vorsorgliche Einwilligungen für die bestehenden Datenverarbeitungsvorgänge einzuholen. Bei der Gestaltung der Einwilligungserklärungen ist Vorsicht geboten. Diese dürfen künftig nicht mehr als Vertragsbestandteil in den Arbeitsvertrag integriert werden. Stattdessen müssen für die Einwilligungserklärungen gesonderte Formulare entwickelt werden. Prüfen Sie daher Ihre Vertragsunterlagen!

Kurz nach Inkrafttreten der DSGVO ist noch nicht geklärt, welche Datenverarbeitungsvorgänge zulässig sind und welche nicht. Die meisten Datenschutzbehörden dürften zunächst eine eher restriktive Linie vertreten, die durch Gerichte erst nach und nach korrigiert und gelockert wird. In der Zwischenzeit kann es zu kontroversen Verhandlungen zwischen Unternehmen und Datenschutzbehörden kommen. Erfahrungsgemäß sind viele Datenschützer Idealisten, die dazu neigen, über ihr Ziel hinauszuschießen.

In den Verhandlungen mit den Datenschutzbehörden kann ein Unternehmen seine Verhandlungsposition deutlich verbessern, wenn es seine Mitarbeiter in sämtliche bestehenden Datenverarbeitungsprozesse vorsorglich einwilligen lässt. Datenverarbeitungsprozesse, in die ein Mitarbeiter eingewilligt hat, sind nach Art. 6 Abs. 1 lit. a DSGVO grundsätzlich gerechtfertigt. Will die Datenschutzbehörde die Legitimationswirkung einer Einwilligung in Frage stellen, muss sie deutlich gewichtigere Einwände vorbringen.

Will ein Arbeitgeber die Privatnutzung des Dienstrechners, insbesondere des E-Mail-Postfachs zulassen, sollte er im Gegenzug unbedingt eine spezielle datenschutzrechtliche Einwilligung einholen, welche Zugriffe des Arbeitgebers auf die auf dem Dienstrechner gespeicherten Daten legitimiert. Andernfalls wären solche Zugriffe mit hohen rechtlichen Risiken bis hin zur Strafbarkeit verbunden.

Bei der Gestaltung von Einwilligungserklärungen muss der Arbeitgeber unbedingt die neu anzuwendenden Formvorschriften beachten:

- Die datenschutzrechtliche Einwilligungserklärung darf nicht Bestandteil des Arbeitsvertrages sein. Zumindest theoretisch muss der Arbeitnehmer die Möglichkeit haben, den Arbeitsvertrag zu unterzeichnen, die Abgabe der datenschutzrechtlichen Einwilligung aber zu verweigern. Dies folgt aus Art. 7 Abs. 2 u. 4 i.V.m. Erwägungsgrund 43 DSGVO und § 26 Abs. 2 Satz 2 u. 3 BDSG n.F.

- Die datenschutzrechtliche Einwilligungserklärung unterliegt künftig noch strengeren Transparenzanforderungen. Der Arbeitgeber muss nachvollziehbar und anschaulich erläutern, auf welche Datenverarbeitungsprozesse sich die Einwilligung bezieht und zu welchen Zwecken diese erfolgen. Auch die durch die Einwilligung begünstigten Rechtsträger müssen benannt werden. Dies folgt aus Art. 7 Abs. 2 u. 4 i.V.m. Erwägungsgrund 42 DSGVO und § 26 Abs. 2 BDSG n.F.

- Bei einer vorsorglichen Einwilligung muss unbedingt der vorsorgliche Charakter im Einwilligungsschreiben deutlich gemacht werden. Es muss nachvollziehbar klargestellt werden, dass die Datenverarbeitung auch bei Verweigerung der Einwilligung erfolgen wird und die Einwilligung nur eine zusätzliche Vorsichtsmaßnahme ist. Andernfalls werten Datenschutzbehörden die Einwilligung als irreführend.

Prüfen Sie, ob die von Ihnen bislang verwendeten Formulare diesen Anforderungen genügen.

Wir stellen Ihnen gerne Formulare zur Verfügung, die auf die künftige Rechtslage und die Besonderheiten Ihres Unternehmens zugeschnitten sind.

Schließen Sie Betriebsvereinbarungen zum Beschäftigtendatenschutz!

Nach Art. 88 DSGVO und § 26 Abs. 4 BDSG n.F. können Betriebsvereinbarungen als besondere datenschutzrechtliche Ermächtigungsgrundlagen fungieren, die dazu geeignet sind, Personaldatenverarbeitungsprozesse zu legitimieren. Außerdem dokumentieren schon Verhandlungen um den Abschluss von Betriebsvereinbarungen die datenschutzrechtlichen Bemühungen eines Unternehmens eindrücklich. Wir empfehlen kurzfristig, dem Betriebsrat den Abschluss einer allgemeinen Betriebsvereinbarung zum Beschäftigtendatenschutz anzubieten.

Das Datenschutzrecht ist ein weiches Rechtsgebiet. Zwar gibt es eine Reihe von Formalvorgaben und offensichtlicher No-Gos. Oft handelt es sich aber um eine schwer zu beantwortende Wertungsfrage, ob, wieweit und auf welche Weise Unternehmen ihre Prozesse nach den Grundsätzen der Datenvermeidung und Datensparsamkeit optimieren müssen und sollten. Ausgehend von diesem Problem sehen sich Datenschutzbehörden in einer Doppelrolle, nämlich einerseits als Sanktionierungsstelle und andererseits als Beratungsstelle.

- Werden Unternehmen bei offener Ignoranz gegenüber datenschutzrechtlichen Problemstellungen „ertappt“, verhängen Datenschutzbehörden künftig in ihrer Rolle als Sanktionierungsstelle empfindliche Bußgelder.

- Ziel aller Unternehmen sollte daher sein, ernsthafte Bemühungen um die datenschutzrechtliche Optimierung ihrer Prozesse zu demonstrieren; gelingt dies glaubhaft, werden Datenschutzbehörden regelmäßig von der Rolle als Sanktionierungsstelle in ihre Rolle als Beratungsstelle wechseln und kooperativ auf das Unternehmen zugehen.

Indem das Unternehmen ernsthafte Verhandlungen mit seinen Betriebsräten aufnimmt, um die Datenverarbeitungsprozesse in Beschäftigungsverhältnissen in Betriebsvereinbarungen zu regeln, kann es den Datenschutzbehörden seine Bemühungen um eine ausgewogene Lösung glaubhaft demonstrieren. Wenn der Verhandlungsprozess mit dem Betriebsrat bei bestimmten Problemfeldern ins Stocken gerät

und es vorerst nicht zu einem Abschluss kommt, lässt sich gegenüber Datenschutzbehörden (immerhin) präzise und konstruktiv darstellen, wo Beratungs- und Schlichtungsbedarf besteht und in welchen Konflikten etwaige Umsetzungsverzögerungen (unverschuldet) ihre Ursache haben.

Gelingt sogar der Abschluss einer Betriebsvereinbarung, kann diese gemäß Art. 88 DSGVO als Ermächtigungsgrundlage für die darin beschriebenen Datenverarbeitungsprozesse fungieren. In der Betriebsvereinbarung beschriebene Datenverarbeitungsvorgänge werden i.d.R. als datenschutzrechtlich legitimiert anzusehen sein und müssen von den Datenschutzbehörden akzeptiert werden.

Bei technischen Überwachungsmaßnahmen müssen nach § 87 Abs. 1 Nr. 6 BetrVG ohnehin Betriebsvereinbarungen geschlossen werden. Hier sollte in den Betriebsvereinbarungen klargestellt werden, dass sie zugleich datenschutzrechtliche Ermächtigungsgrundlage sind. Als Ermächtigungsgrundlage bieten sich Betriebsvereinbarungen darüber hinaus z.B. an für

- Veröffentlichung privater Angaben in Mitarbeiterlisten zu Zwecken des sozialen Austauschs,
- Taschenkontrollen,
- Einholung von Schufa-Auskünften über Mitarbeiter,
- Durchsuchungen von Schreibtischschubladen und Spints und
- den Einsatz von Scheinkunden zur Qualitätskontrolle.

Wir empfehlen, der Betriebsratsseite kurzfristig den Abschluss einer allgemeinen (Rahmen-) Betriebsvereinbarung zum Beschäftigtendatenschutz anzubieten, die „als erster Schritt“ grundsätzliche, aber dafür umfassende Regelungen enthält. Anschließend können besondere datenschutzrechtliche Problemstellungen in weiteren Verhandlungen nach und nach aufbereitet werden.

Einen auf Ihr Haus angepassten Text für eine allgemeine Betriebsvereinbarung zum Beschäftigtendatenschutz, die Handlungswillen demonstriert, ohne die Handlungsfähigkeit des Unternehmens zu bedrohen, können wir Ihnen zur Verfügung stellen.

Beschäftigtendatenschutzrecht

Bei Fragen zum Beschäftigtendatenschutzrecht stehen Ihnen gerne zur Verfügung:

Dr. Detlef Grimm
+49 (0) 221 650 65-129
detlef.grimm@loschelder.de

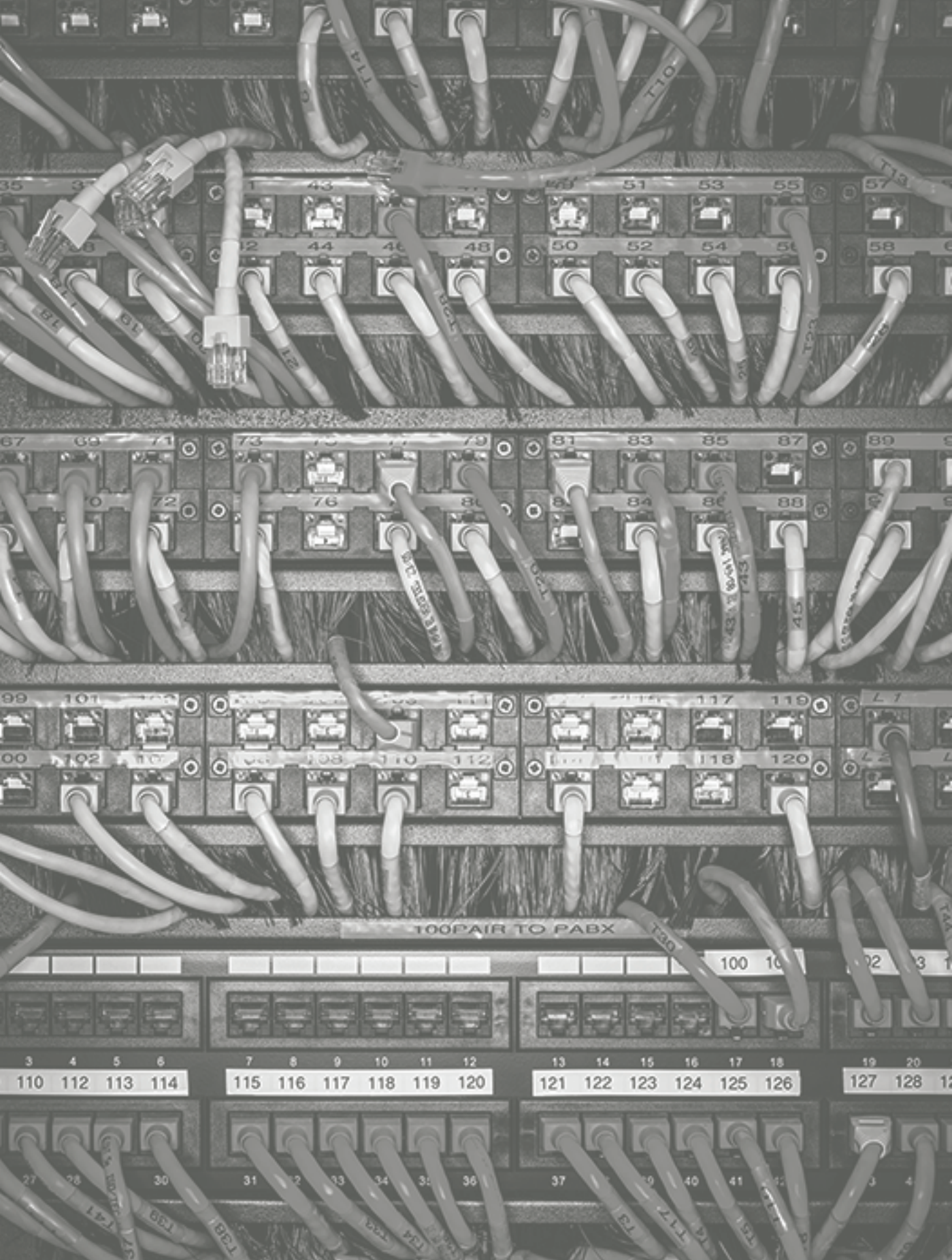
Dr. Martin Brock
+49 (0) 221 650 65-233
martin.brock@loschelder.de

Dr. Sebastian Pelzer
+49 (0) 221 650 65-263
sebastian.pelzer@loschelder.de

Arne Gehrke, LL.M.
+49 (0) 221 650 65-263
arne.gehrke@loschelder.de

Dr. Stefan Freh
+49 (0) 221 650 65-129
stefan.freh@loschelder.de

Dr. Jonas Kühne
+49 (0) 221 650 65-129
jonas.kuehne@loschelder.de


100PAIR TO PABX
110 112 113 114
115 116 117 118 119 120
121 122 123 124 125 126
127 128

AGB-Recht

Datenschutzklauseln in Allgemeinen Geschäftsbedingungen im unternehmerischen Rechtsverkehr

Sowohl beim Einkauf als auch beim Verkauf von Waren erheben und speichern Unternehmen oft personenbezogene Daten (insbesondere Namen und Kontaktdaten) der jeweiligen zuständigen Mitarbeiter aus den Einkaufs- und Verkaufsabteilungen ihrer Zulieferer bzw. Kunden. Unabhängig davon, ob diese Daten nur für die jeweilige konkrete Bestellung bzw. das konkrete Angebot oder auch für künftige Bestellungen und Angebote genutzt werden, handelt es sich dabei um die Verarbeitung personenbezogener Daten natürlicher Personen im Sinne von Art. 4 Datenschutzgrundverordnung (DSGVO).

Nach Inkrafttreten der DSGVO am 25. Mai 2018 sind Unternehmen bei der Verarbeitung personenbezogener Daten verpflichtet, eine Vielzahl von neuen datenschutzrechtlichen Vorgaben einzuhalten. Diese Anforderungen können Unternehmen zwar nicht durch entsprechende Klauseln in ihren AGB erfüllen. Allerdings können sie sich möglicherweise durch Regelungen in AGB die Erfüllung von Informationspflichten gegenüber den betroffenen Personen nach Art. 13, 14 DSGVO erleichtern sowie klar nach außen dokumentieren, dass sie das Datenschutzrecht beachten.

Soweit Unternehmen personenbezogene Daten im Rahmen des Einkaufs oder Verkaufs von Waren verarbeiten, kann es daher sinnvoll sein, entsprechende Klauseln in die AGB aufzunehmen. Dabei sollte auf die nachfolgenden drei Punkte geachtet werden:

Dokumentation nach außen

Mit Hilfe entsprechender AGB-Klauseln kann nach außen dokumentiert werden, dass die Verarbeitung personenbezogener Daten ausschließlich unter Einhaltung der datenschutzrechtlichen Vorgaben erfolgt. Solche Klauseln zeigen den Kunden und Zulieferern, dass das jeweilige Unternehmen sich datenschutzrechtskonform verhält, was für viele Unternehmen heute wichtig bei der Auswahl ihrer Vertragspartner ist. Zum anderen dokumentieren derartige Klauseln auch gegenüber der zuständigen Aufsichtsbehörde, dass das Unternehmen die datenschutzrechtlichen Vorgaben einhält. Dies kann u.U. im Fall eines Verfahrens bußgeldmindernd wirken.

Bei der Formulierung solcher Klauseln ist nach Inkrafttreten der DSGVO allerdings darauf zu achten, nicht nur allgemeine Standardklauseln einzufügen. Wichtig ist, dass neben der allgemeinen Angabe, dass die Verarbeitung personenbezogener Daten unter Einhaltung der datenschutzrechtlichen Vorgaben erfolgt, ganz konkret beschrieben wird, wie das jeweilige Unternehmen die erhobenen personenbezogenen Daten verarbeitet.

Information der betroffenen Personen

Erhebt ein Unternehmen personenbezogene Daten, ist es verpflichtet, die betroffenen Personen zu informieren, bei Erhebung über einen

Dritten nach Maßgabe des Art. 14 DSGVO und bei Erhebung bei dem Betroffenen selbst nach Maßgabe des Art. 13 DSGVO. Das bedeutet, dass Unternehmen, die beim Einkauf oder Verkauf von Waren die personenbezogenen Daten der zuständigen Mitarbeiter ihrer Kunden und Zulieferer erheben, speichern und evtl. für künftige Bestellungen und Angebote nutzen und/oder an Dritte weitergeben, gemäß Art. 13, 14 DSGVO verpflichtet sind, die individuellen Personen, deren Daten erhoben wurden, persönlich über eine Vielzahl von Aspekten der konkreten Datenverarbeitung zu informieren.

Im normalen Geschäftsablauf kann es unpraktikabel sein, wenn die betroffenen Personen aus den Einkaufs- und Verkaufsabteilungen, deren Daten verarbeitet werden, zunächst persönlich informiert werden müssen. Die Verpflichtung, die betroffenen Personen persönlich zu informieren, gilt allerdings dann nicht, wenn das Unternehmen davon ausgehen kann, dass die Information anderweitig erfolgt, da die betroffene Person dann bereits informiert ist (Art. 13 Abs. 4, 14 Abs. 5 lit. a DSGVO). Daher können Unternehmen, die beim Einkauf und Verkauf personenbezogene Daten der jeweiligen Mitarbeiter erheben, eine Klausel in ihre Einkaufs- und Verkaufsbedingungen aufnehmen, wonach diese bei der Übermittlung personenbezogener Daten verpflichtet sind, ihre eigenen Mitarbeiter nach Maßgabe von Art. 13, 14 DSGVO zu informieren. Nutzt ein Unternehmen derartige Klauseln in allgemeinen Verkaufs- und Einkaufsbedingungen kann es wohl, solange ihm keine gegenteiligen Informationen vorliegen, davon ausgehen, dass seine Zulieferer und Kunden ihre Mitarbeiter entsprechend informieren.

Unabhängig von solchen Klauseln muss das Unternehmen allerdings die für die Erfüllung der Informationspflicht notwendigen Angaben gleichwohl selbst dem Zulieferer bzw. Kunden zur Verfügung stellen. Entsprechende Informationsblätter müssen also – jedenfalls dann, wenn der Zulieferer / Kunde diese anfragt – trotz der vorab dargestellten AGB-Klauseln erstellt werden.

Kenntnis von den AGB

Die unmittelbare Information gegenüber den betroffenen Personen nach Art. 13, 14 DSGVO können AGB allerdings nur dann entbehrlich machen, wenn der Vertragspartner bei Abschluss des Vertrages ausreichende Möglichkeit der Kenntnisnahme von den AGB hatte.

AGB-rechtlich müssen die AGB nur im internationalen Rechtsverkehr stets beigefügt werden. Bei rein deutschen Verträgen im B2B-Verkehr reicht sowohl der Verweis auf im Internet veröffentlichte AGB als auch der Hinweis, dass die AGB bei Bedarf übersandt werden können.

Datenschutzrechtlich ist noch nicht abschließend geklärt, ob es dafür erforderlich ist, dass die AGB stets in Papierform übergeben bzw. übersandt werden müssen. Solange dies noch nicht durch Gerichte entschieden ist, gehen wir davon aus, dass die Information der betroffenen Personen bei Nutzung entsprechender Klauseln in AGB unter den vorab dargestellten Voraussetzungen dann entbehrlich sein kann, wenn diese in Papierform (oder als pdf-Datei) überlassen werden. Der Verweis auf im Internet veröffentlichte AGB dürfte auch noch ausreichen. Dagegen

gehen wir davon aus, dass allein der Hinweis, dass die AGB bei Bedarf übersandt werden können, nicht ausreichend ist. Möchte man sicher gehen, sollten die AGB jeder Bestellung, jedem Angebot und jeder Auftragsbestätigung beigefügt werden.

Bei Fragen zu Datenschutzklauseln in AGB stehen Ihnen gerne zur Verfügung:

Dr. Kristina Schreiber
+49 (0) 221 650 65-337
kristina.schreiber@loschelder.de

Dr. Sandra Orlikowski-Wolf
+49 (0) 221 650 65-206
sandra.orlikowski-wolf@
loschelder.de


+ 1,18 % 13450,23
26.3.
1.4.
7.4.
+ 0,55 % 5656,95
20.3.
26.3.
1.4.
7.4.
- 0,17 % 1,5676
Kurs
Kurs Vortag
Hoch

Aktienrecht

Informationspflichten bei Einberufung und Durchführung von Hauptversammlungen nach der DSGVO

Nach der DSGVO, die am 25. Mai 2018 in Kraft getreten ist, bestehen umfangreiche Informationspflichten, wann immer personenbezogene Daten erhoben werden (Art. 13 DSGVO). Die betroffene Person muss unter anderem darüber informiert werden, wer, zu welchem Zweck, wie lange und auf welcher Rechtsgrundgrundlage personenbezogene Daten erhebt und ob und an wen die erhobenen Daten möglicherweise weitergegeben werden. Diese Vorschrift ist der Grund, warum derzeit viele Unternehmen wie etwa Banken und Versicherungen ihre Kunden anschreiben und über die Datenerhebung informieren. Die neu geschaffene Informationspflicht hat aber auch Auswirkungen auf Aktiengesellschaften und ihre Aktionäre bzw. deren Vertreter.

Insbesondere im Zusammenhang mit der Einberufung und Durchführung der Hauptversammlung werden personenbezogene Daten erhoben. Viele Aktiengesellschaften legen ihren Einberufungsunterlagen zur Hauptversammlung Informationen zum Datenschutz für ihre Aktionäre bei oder halten diese Informationen jedenfalls im Internet auf der Unternehmens-Webseite zum Abruf bereit.

So sind die Aktionäre und ihre Vertreter beispielsweise darüber zu informieren, dass in der Hauptversammlung ein Teilnehmerverzeichnis aufgestellt werden muss. Darin müssen die erschienenen oder vertretenen Aktionäre und die Vertreter von Aktionären mit Vor- und Nachnamen und Wohnort und der jeweils vertretenen Stückzahl von Aktien aufgenommen werden (§ 129 Abs. 1 Satz 2 AktG). Das Teilnehmerverzeichnis steht nicht nur jedem Teilnehmer während der Hauptversammlung zur Einsicht offen, sondern jedem Aktionär (d.h. auch Aktionären, die nicht an der Hauptversammlung teilgenommen haben) für die Dauer von zwei Jahren nach

der Hauptversammlung. Nimmt der Notar, der das Protokoll in der Hauptversammlung führt, das Teilnehmerverzeichnis als Anlage zum Hauptversammlungsprotokoll, ist es sogar dauerhaft von jedermann im Handelsregister einsehbar. Oftmals wird das Teilnehmerverzeichnis nicht von der Aktiengesellschaft selbst geführt, sondern von einem Dienstleister, an den die Aktiengesellschaft deshalb personenbezogene Daten ihrer Aktionäre bzw. deren Vertreter weitergibt. Auch darüber muss die Aktiengesellschaft informieren.

Hat die Aktiengesellschaft Namensaktien ausgegeben, so sollte sie die Einberufung der Hauptversammlung dazu nutzen, bei dieser Gelegenheit auch auf das Aktienregister hinweisen. Darin sind der Vor- und Nachname, das Geburtsdatum und die Adresse des Aktionärs mit der vom Aktionär gehaltenen Stückzahl oder der Aktiennummer vermerkt (§ 67 AktG) und somit personenbezogene Daten erhoben und gespeichert. Auch hier darf gegebenenfalls der Hinweis nicht fehlen, dass die Daten an externe Dienstleister weitergegeben werden, die das Aktienregister für die Gesellschaft führen. Zudem sind die Kontaktdaten des Datenschutzbeauftragen und der zuständigen Datenschutzaufsichtsbehörde anzugeben.

Bei Fragen zu den Auswirkungen der DSGVO auf Aktiengesellschaften stehen Ihnen zur Verfügung:

Dr. Martin Empt, LL.M.
+49 (0) 221 650 65-339
martin.empt@loschelder.de

Dr. Marcel Kleemann
+49 (0) 221 650 65-266
marcel.kleemann@loschelder.de

Wettbewerbsrecht

Abmahnwelle wegen DSGVO-Verstößen: Sturmflut – oder doch nur Sturm im Wasserglas?

In der Vergangenheit haben insbesondere minimale Verstöße gegen die Impressumspflicht auf Webseiten, fehlerhafte Belehrungen über gesetzliche Widerrufsrechte oder die Verwendung unzulässiger AGB sog. Abmahnwellen ausgelöst, die bei den betroffenen Unternehmen zu Ärger und vermeidbaren Kosten führen. Auch anlässlich des Inkrafttretens der Datenschutz-Grundverordnung wurde befürchtet, dass „Abmahnanwälte" die Neuerungen im Datenschutzrecht ausnutzen, um massenhaft kostenpflichtige Abmahnungen an Unternehmen zu verschicken, die den Anforderungen des neuen Rechts noch nicht (vollständig) gerecht werden.

Rechtlicher Rahmen: Abmahnung wegen Wettbewerbsverstoß

Abmahnanwälte können mit Abmahnungen wegen geringfügiger Verstöße gegen gesetzliche Bestimmungen schnell und leicht Geld verdienen: Insbesondere auf Webseiten lassen sich Rechtsverletzungen mühelos – teils mithilfe spezieller Software – auffinden. Die rechtliche Bewertung bereitet in der Regel keine Schwierigkeiten und auch ein Abmahnschreiben ist insbesondere dann schnell verschickt, wenn der beauftragte Anwalt auf Textbausteine zurückgreifen kann.

Eine berechtigte Abmahnung setzt aber voraus, dass dem Abmahnenden ein Unterlassungsanspruch gegen den Abgemahnten zusteht. Hierfür bedarf es regelmäßig eines „Umwegs" über das Wettbewerbsrecht: Insbesondere Mitbewerbern und bestimmten Verbänden stehen Unterlassungsansprüche gegen unlautere geschäftliche Handlungen zu. Verstöße gegen gesetzliche Bestimmungen sind im Sinne des Wettbewerbsrechts unlauter und damit abmahnfähig, wenn es sich bei der betroffenen Vorschrift um eine sog. Marktverhaltensreglung handelt. Erforderlich ist, dass die gesetzliche Bestimmung (auch) das Verhalten der Unternehmen im Wettbewerb steuern soll. Konkurrenten sollen Gesetzesverstöße nämlich nicht um ihrer selbst willen sanktionieren, sondern nur, um zu verhindern, dass Unternehmen durch gesetzeswidriges Verhalten einen Vorsprung im Wettbewerb gegenüber ihren rechtstreuen Wettbewerbern erlangen.

Ist die Abmahnung wegen eines Wettbewerbsverstoßes berechtigt, kann der Abmahnende von dem Abgemahnten die Kosten, die durch die Einschaltung eines Rechtsanwalts entstanden sind, ersetzt verlangen. Diese belaufen sich mindestens auf einige hundert Euro, können je nach Bedeutung des Verstoßes aber auch schnell deutlich höher liegen. Gibt der Abgemahnte

die in der Abmahnung geforderte Unterlassungserklärung nicht ab, droht ein gerichtliches Verfahren – häufig im einstweiligen Rechtsschutz – durch das weitere Kosten entstehen können.

Sind Bestimmungen der DSGVO „Marktverhaltensregelungen"?

Wer die mediale Berichterstattung anlässlich des Inkrafttretens der Datenschutz-Grundverordnung verfolgt hat, konnte schnell den Eindruck gewinnen, dass es nur eine Frage der Zeit ist, bis die nächste Abmahnwelle wegen Verstößen gegen das neue Datenschutzrecht losbricht. Meldungen machten die Runde, dass findige Softwareentwickler bereits Programme anbieten, mit denen sich im Internet gezielt nach Datenschutzverstößen suchen lässt. Und in der Tat dauerte es nur wenige Stunden, ehe einzelne Anwälte bereits am Tag des Inkrafttretens der DSGVO die ersten Abmahnungen wegen Verstößen gegen das neue Datenschutzrecht verschickten. Soweit ersichtlich ist es jedoch bei Einzelfällen geblieben, eine große Zahl von Abmahnungen wurde nicht versandt.

Doch ist die Rechtslage wirklich so eindeutig? Tatsächlich ist die Frage, ob und welche datenschutzrechtlichen Vorschriften als Marktverhaltensregelung einzustufen sind, noch nicht geklärt. Zwar herrschte zum alten Datenschutzrecht die Ansicht vor, dass Vorschriften des BDSG, welche die Verwendung von Daten zu Werbezwecken betreffen (§§ 28, 29 BDSG) als Marktverhaltensregeln einzustufen sind. Unklar ist aber, ob diese Wertung auf die Vorschriften der neuen DSGVO zu übertragen ist, die seit dem 25.05.2018 gelten. Insoweit wird vertreten, dass Art. 77–84 DSGVO spezielle und abschließende Vorschriften zur Durchsetzung von Ansprüchen betroffener Personen enthält. Allerdings lässt sich der abschließende Charakter der Regelungen der DSGVO zumindest nicht zweifelsfrei entnehmen. Vielmehr entspricht es dem Regelungsziel der Gewährleistung eines hohen Datenschutzniveaus, auch weitere, ggf. nur in einzelnen Mitgliedstaaten vorhandene Durchsetzungsmechanismen zu akzeptieren. Dies gilt insbesondere vor dem Hintergrund, dass die Verordnung ausdrücklich das unterschiedlich hohe Datenschutzniveau in den Mitgliedsländern als Hemmnis für den Wettbewerb ansieht. Dies spricht dafür, dass die Regelungen der DSGVO (insbesondere die Regelungen mit eindeutigem Bezug zur Werbung wie z.B. Art. 21 Abs. 2, 3 DSGVO) die erforderliche zumindest sekundäre wettbewerbsbezogene Schutzfunktion aufweisen.

In diesem Fall könnten Verstöße gegen das neue Datenschutzrecht nicht nur von den zuständigen Behörden, sondern auch und insbesondere von Mitbewerbern sanktioniert werden.

Praxishinweis: Was ist zu tun?

Gerichtliche Entscheidungen zu der Frage, ob Verstöße gegen die DSGVO auch von Mitbewerbern über das Wettbewerbsrecht sanktioniert werden können, sind bis Redaktionsschluss – soweit ersichtlich – noch nicht veröffentlicht. Bis zu einer endgültigen Klärung der Rechtslage durch den Bundesgerichtshof bzw. den Europäischen Gerichtshof werden ohnehin mehrere Jahre vergehen. Bis dahin steht zu befürchten, dass nicht nur Behörden, sondern auch Mitbewerber Verstöße gegen das Datenschutzrecht verfolgen.

Die Sorgen um eine Abmahnwelle wegen DSGVO-Verstößen hat in der Zwischenzeit auch die Politik auf den Plan gerufen: Die Unionsfraktion im Bundestag möchte kurzfristig eine Gesetzes-

änderung auf den Weg bringen, nach der die Erstattung von Abmahngebühren wegen DSGVO-Verstößen vorerst nicht mehr gefordert werden darf. Dies macht den massenhaften Versand von Abmahnungen wegen geringfügiger Verstöße für Abmahnanwälte unattraktiv.

Von einer zeitnahen Umsetzung der neuen Anforderungen des Datenschutzrechts würde aber auch die Gesetzesänderung nicht entbinden. Zum einen soll das Moratorium, das noch vor der Sommerpause in Kraft treten könnte, nur für einen Übergangszeitraum von zwölf Monaten gelten. Zum anderen könnten Konkurrenten weiterhin – unter Verzicht auf die Erstattung von Abmahnkosten – Datenschutzverstöße verfolgen. Spätestens durch ein gerichtliches Verfahren würden Kosten entstehen, die im Falle eines Datenschutzverstoßes von dem Abgemahnten zu tragen wären, sollte ein Gericht die Bestimmungen der DSGVO als Marktverhaltensregelungen ansehen. Daher sollte ein entsprechendes Schreiben auch dann nicht ignoriert werden, wenn der Bundestag ein Moratorium beschließt.

Bei Fragen zu Abmahnungen wegen Datenschutzverstößen stehen Ihnen gerne zur Verfügung:

Dr. Stefan Maaßen, LL.M.
+49 (0) 221 650 65-231
stefan.maassen@loschelder.de

Dr. Patrick Pommerening
+49 (0) 221 650 65-134
patrick.pommerening@loschelder.de

Die Publikation „Recht Aktuell“ ist eine unregelmäßig erscheinende Veröffentlichung von Loschelder und beinhaltet keinen konkreten Rechtsrat zu einem speziellen Sachverhalt. Die veröffentlichten Artikel sind allgemeine Zusammenfassungen zu aktuellen rechtlichen Fragen, gesetzgeberischen Entwicklungen und Veränderungen aufgrund neuer Entscheidungen. Wir empfehlen deshalb dringend, bei konkreten Fragen einen Rechtsanwalt unserer Sozietät zu konsultieren. Dieser wird Ihre speziellen Fragen unter Berücksichtigung des Sachverhaltes und Ihrer Bedürfnisse gerne beantworten. Diese Veröffentlichung kann auf unserer Homepage unter www.loschelder.de abgerufen werden. Dort finden Sie auch weitere Veröffentlichungen unserer Sozietät.

Impressum

Herausgeber:
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

Konzept, Gestaltung:
wiehl, Co.

Fotografie:
iStock/gettyimages, Asbach

Loschelder

Konrad-Adenauer-Ufer 11
50668 Köln

+49 (0) 221 650 65-0
www.loschelder.de