LOSCHELDER

Newsletter Datenschutzrecht
Mai 2019

Inhalt

Übermittlung von Kontaktdaten B2B

Auch der Austausch von personenbezogenen Kontaktdaten zwischen Ansprechpartnern in Unternehmen – etwa der Austausch von Visitenkarten oder die Benennung als Ansprechpartner durch einen Kollegen – ist bekanntlich datenschutzrechtlich relevant und bedarf einer Erlaubnis für die Datenverarbeitung. Wann eine solche gegeben ist, konkretisiert das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) auf Anfrage der IHK Nürnberg in einer aktuellen Stellungnahme.

Bei den Kontaktdaten von Ansprechpartnern im B2B-Bereich, wie z.B. Geschäfts-E-Mail-Adresse mit Namensbestandteil, handelt es sich um personenbezogene Daten. Ihre Verarbeitung – etwa über den Austausch von Visitenkarten oder die Benennung als Ansprechpartner in einem Angebot – bedarf einer Rechtsgrundlage. Diese kann in wenigen Fällen in Art. 6 Abs. 1 lit. b) DSGVO liegen, wenn die Verarbeitung zur Vertragsanbahnung oder Erfüllung eines Vertrages erforderlich ist. Dies ist allerdings, wie auch das BayLDA bestätigt, nur der Fall, wenn der Vertrag mit der Person geschlossen ist bzw. geschlossen wird, deren Daten verarbeitet werden. Dieser Erlaubnistatbestand kommt demnach nur in Betracht, wenn das Unternehmen und der Ansprechpartner personenidentisch sind (z. B. Einzelkaufmann, Einzelselbständiger). Für Arbeitnehmer greift dieser Erlaubnistatbestand nicht.

Dennoch ist die Verarbeitung dieser personenbezogenen Daten auch nach der aktuellen Stellungnahme des BayLDA regelmäßig erlaubt, aus berechtigten Interessen des Arbeitgebers (Art. 6 Abs. 1 lit. f) DSGVO). Berufsbezogene Kontaktdaten sind bereits im Ausgangspunkt regelmäßig wenig schutzwürdig, da sie oft öffentlich bekannt und für die Verbreitung unter den potentiellen Kontaktpersonen auch in anderen Unternehmen bestimmt sind. Etwa die Übergabe von Visitenkarten erfolgt üblicherweise gerade zum Zweck der späteren Kontaktaufnahme, je nach Kontext z.B. für Informations- oder Werbezusendungen, zur Kontaktaufnahme für Vertragsverhandlungen, für gemeinsame Projekte oder zur Vorbereitung eines Besuches. Ebenso ist die Benennung als Ansprechpartner eines Unternehmens durch den Arbeitgeber und die darauf folgende Datenverarbeitung auch durch Dritte regelmäßig durch überwiegende berechtigte Interessen von Arbeitgeber und Drittem gedeckt, wenn diese im Rahmen üblicher beruflicher Tätigkeiten erfolgt. Offen steht dem betroffenen Arbeitnehmer selbstverständ-

lich sein jederzeitiges Widerspruchsrecht nach Art. 21 DSGVO – außerhalb von Werbezwecken mit besonderem Grund. Danach dürfte jedenfalls dann die Datenverarbeitung nach Widerspruch der betroffenen Person zu beenden sein, wenn der Arbeitnehmer das Unternehmen verlassen hat.

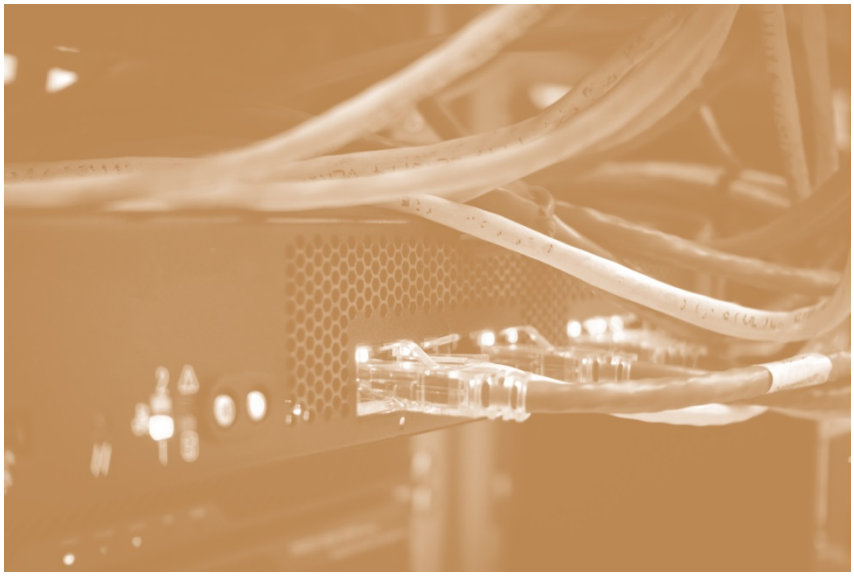
Schließlich ist auch der Erlaubnistatbestand der Einwilligung gem. Art. 6 Abs.1 lit. a) DSGVO in Betracht zu ziehen. Diese muss allerdings freiwillig erteilt werden und ist jederzeit widerrufbar. In Fällen, in denen eine Person aufgrund ihrer arbeitsrechtlichen Pflichten als Ansprechpartner zur Verfügung stehen muss, dürfte es an der Freiwilligkeit einer Einwilligung fehlen. Praktisch relevant ist dieser Erlaubnistatbestand daher zuvörderst bei der Datenverarbeitung zu Werbezwecken.

Orientierungshilfe der DSK zur Zugangssicherung

Anbieter von Online-Diensten, die personenbezogene Daten von Nutzerinnen und Nutzern verarbeiten, müssen die Sicherheit der Verarbeitung auch durch Zugangssicherungen gewährleisten (Art. 32 DSGVO). Praktische Hilfen, wie dies umzusetzen ist, haben jüngst nach dem BSI auch die Datenschutzaufsichtsbehörden veröffentlicht.

Hilfreiche Empfehlungen für die Einrichtung der notwendigen Zugangssicherungen enthielt bisher vor allem das Kompendium des Bundesamtes für Sicherheit in der Informationstechnik (BSI) im IT-Grundschutz- zum Identitäts- und Berechtigungsmanagement

(Stand: 28.09.18). Nun fassten Ende März auch die deutschen Aufsichtsbehörden in ihrer Orientierungshilfe „Anforderungen an Anbieter von Online Diensten zur Zugangssicherung“ die Maßnahmen zusammen, die nach ihrer Einschätzung dem Stand der Technik entsprechen und einen effektiven Schutz gewährleisten können. Überraschungen enthält das kurze Papier nicht; es kann als eine Art Checkliste für die Überprüfung der eigenen Zugangssicherungen herangezogen werden.



Clouds „Made in Germany“

Cloud-Dienste ermöglichen Flexibilität und die Einsparung lokaler Serverkapazitäten; bekannt waren in der Vergangenheit insbesondere die Cloud-Dienste US-amerikanischer Unternehmen wie Dropbox, Google Drive und Apples iCloud. Diese sind aber nicht zuletzt nach Aufhebung des Safe-Harbor-Abkommens durch den EuGH Ende 2015 und das Inkrafttreten der Datenschutzgrundverordnung verstärkt in die Kritik geraten und durch EU-zentrierte Angebote ergänzt worden. Welche Clouds insbesondere unter den Aspekten des Datenschutzes und der Datensicherheit akzeptabel sind, hat nun auch die Stiftung Warentest untersucht.

Die Stiftung Warentest prüfte insgesamt 11 Cloud-Dienste und äußerte Bedenken gegen die vorgenannten großen US-Anbieter von Cloud-Diensten. Laut der Stiftung Warentest gibt es Alternativen; ein deutscher Anbieter etwa wurde Testsieger.

Zertifizierungen, Datenschutzsiegel und -prüfzeichen

Verantwortliche und Auftragsverarbeiter sollen mit Zertifizierungen, Datenschutzsiegeln und -prüfzeichen nachweisen können, dass sie die Datenschutzgrundverordnung einhalten (Art. 42 DSGVO); die Mitgliedstaaten, Aufsichtsbehörden und Kommission sollen die Einführung derartiger Verfahren unterstützen. Eine Übersicht über das Verfahren ist von den Aufsichtsbehörden veröffentlicht worden.

Etwa für Auftragsverarbeiter oder online aktive Unternehmen, die mit sensiblen Daten arbeiten, können Zertifizierungen als Werbemittel dienen. Darüber hinaus kann eine erfolgreiche Zertifizierung auch rechtliche Wirkung entfalten: Zum einen können Zertifizierungen als ein Gesichtspunkt bei der Beurteilung, ob die notwendigen technisch organisatorischen Maßnahmen ergriffen wurden, dienen (Art. 24 Abs. 3 DSGVO). Des Weiteren sieht Art. 25 Abs. 3 DSGVO Zertifizierungen als einen Faktor bei der Beurteilung der Einhaltung der Pflichten zum „Privacy By Design“ (Art. 25 Abs. 1 DSGVO) und „Privacy By Default“ (Art. 25 Abs. 2 DSGVO).

Zuständig für die Akkreditierung der Zertifizierungsstellen sind die Aufsichtsbehörden. Die akkreditierten Zertifizierungsverfahren und Datenschutzsiegel und -prüfzeichen werden nach Genehmigung der Aufsichtsbehörde in ein Register aufgenommen und veröffentlicht (Art. 42 Abs. 8 DSGVO). Die Zertifizierungsstellen sind die privaten Vereine oder Unternehmen, die das akkreditierte Zertifizierungsverfahren durchführen und die Datenschutzsiegel und -

prüfzeichen erteilen (Art. 42 Abs. 7 DSGVO). Die Zertifikate dienen als Nachweis darüber, dass die Vorgaben der DSGVO eingehalten wurden (Art. 42 Abs. 1 DSGVO).

Einen Überblick über den Akkreditierungsprozess bietet eine Übersicht der DSK, in der der Akkreditierungsprozess für den Bereich Datenschutz (Art. 42 und 43 DSGVO) dargestellt wird. Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden Württemberg folgte mit einer Kurzerklärung.

Branchenspezifische Verhaltensregeln für den Datenschutz

Wirtschafts- oder Branchenverbände können sich selbst und den ihnen angehörigen Unternehmen branchenspezifische datenschutzrechtliche Verhaltensregeln auferlegen. Einen Überblick über die in NRW bisher genehmigten Verhaltensregelungen hat jüngst die Landesbeauftragte für Datenschutz und Informationsfreiheit NRW erstellt und veröffentlicht.

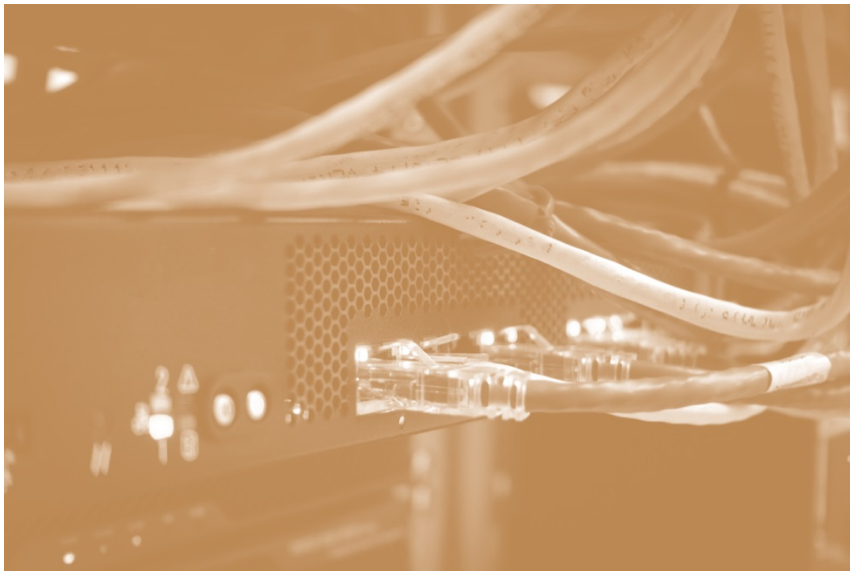
Die datenschutzrechtlichen Pflichten der Unternehmen werden durch Verhaltensregelungen mit Blick auf die Spezifika der Branche und dort typische Prozessabläufe konkretisiert, ein Branchenstandard wird etabliert. Dies führt auch zu einer erhöhten Rechtssicherheit für die gesamte Branche, zumal die Verhaltensregelungen von der zuständigen Aufsichtsbehörde genehmigt werden müssen. Dennoch führt dieses durch die DSGVO neu geschaffene Instru-

ment bisher ein Schattendasein. Die Landesbeauftragte für Datenschutz und Informationsfreiheit NRW hat jüngst ein Verzeichnis über die von ihr genehmigten Verhaltensregeln erstellt und veröffentlicht (hier). Darin veröffentlicht sind bisher nur die Verhaltensregeln für die Prüf- und Löschfristen von Wirtschaftsauskunfteien.

Bisher haben neben dem Wirtschaftsauskunfteien e.V. nur wenige Verbände von dieser Möglichkeit Gebrauch gemacht. So sind auf europäischer Ebene etwa der Verhaltenskodex der Federation of European Direct and Interactive Marketing („FEDMA“) und auf nationaler Ebene die Verhaltensregeln für den Umgang mit personenbezogenen Daten durch die deutsche Versicherungsgesellschaft des Gesamtverbandes der deutschen Versicherungswirtschaft und der GeoBusiness Code of Conduct des Vereins der Selbstregulierung Informationswirtschaft e.V. (SRIW) und der Kommission für Geoinformationswirtschaft (GIW-Kommission) zu nennen. Im Hinblick auf eine hierdurch voranschreitende Erleichterung, praktische Vereinheitlichung der Auslegung der DSGVO und insbesondere eine erheblich verbesserte Rechtssicherheit wäre die Ausarbeitung von Verhaltensregeln jedenfalls wünschenswert – auch wenn es nach Art. 40 DSGVO geht, soll dies ausdrücklich gefördert werden. Dennoch ist nicht zu verkennen, dass die Ausarbeitung von Verhaltensregelungen mit einem erheblichen Arbeitsaufwand verbunden ist.

Zum Hintergrund: Verbände oder andere Vereinigungen, die Kategorien von Verantwortlichen oder Auftragsverarbeitern vertreten, können gemeinsame Verhaltensregelungen erarbeiten. Nach Art. 40 Abs. 5 DSGVO legen sie diese ausgearbeiteten Verhaltensregeln dann der zuständigen Aufsichtsbehörde zur Genehmigung vor. Die Aufsichtsbehörde gibt eine Stellungnahme darüber ab, ob der Entwurf mit der DSGVO vereinbar ist und genehmigt ihn, wenn sie der Auffassung ist, dass er ausreichende geeignete Garantien für den Datenschutz enthält. Verhaltensregeln stellen Handlungsleitlinien dar, durch die die Anwendung der DSGVO für die jeweilige Branche präzisiert, vereinfacht und vereinheitlicht werden soll. Sie können branchentypische Prozesse bei der Verarbeitung personenbezogener Daten weitaus präziser erfassen, als die symmetrisch alle Branchen erfassende DSGVO. Damit können sie Unternehmen eine Orientierungshilfe bieten und – gerade angesichts der Prüfung durch die Aufsichtsbehörde – die Rechtssicherheit erheblich erhöhen. Unternehmen, die sich den Verhaltensregeln unterwerfen, be-

weisen durch die freiwillige Selbstregulierung einen verantwortungsvollen Umgang mit dem Datenschutz, zumal die Einhaltung der Verhaltensregeln von Kontrollstellen zu überwachen ist. Art. 40 Abs. 4 DSGVO sieht vor, dass die Verbände und Vereinigungen ein effektives Verfahren etablieren, das der Überwachungsstelle ermöglicht, angemessene Maßnahmen bei Zuwiderhandlung zu treffen. Grundlage hierfür ist dann etwa die Verbandssatzung oder eine von den Unternehmen unterzeichnete Unterwerfungserklärung. Ziel dieser Regelung ist, dass Verhaltensregeln nicht nur zu „gut gemeinten Empfehlungen“ ohne Konsequenzen verkümmern.



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

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

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

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

Impressum

LOSCHELDER RECHTSANWÄLTE
Partnerschaftsgesellschaft mbB
Konrad-Adenauer-Ufer 11
50668 Köln

Tel. +49 (0)221 65065-0, Fax +49 (0)221 65065-110
info@loschelder.de
www.loschelder.de