



**LOSCHELDER**

**Newsletter Datenschutzrecht  
Juli 2019**

## **Inhalt**

**Das digitale Beratungsangebot von Loschelder jetzt auch online präsentiert**

**Das „Zweite Datenschutz-Anpassungs- und Umsetzungsgesetz“**

**Datenschutz beim Asset Deal**

**Geltendmachung von Betroffenenrechten: Identitätsprüfung**

## Das digitale Beratungsangebot von Loschelder jetzt auch online präsentiert

*Kaum ein anderes Thema offenbart derart viele Chancen und Herausforderungen für die Wirtschaft wie die digitale Transformation. Wir begleiten unsere Mandanten schon seit Beginn der Digitalisierung bei der rechtssicheren Umsetzung neuer technischer Möglichkeiten. Neu ist nun die Präsentation unseres digitalen Beratungsangebots auf unserer [Website](#).*

Dort können Sie nachlesen, wie wir auch Ihr Unternehmen mit unserer umfangreichen Erfahrung mit Digitalisierungsprozessen in unterschiedlichsten Branchen und Unternehmen jeglicher Größenordnung unterstützen können – gleich, ob Sie den digitalen Wandel neu in Angriff nehmen oder bereits digitalisiert sind und sich mit spezifischen Herausforderungen konfrontiert sehen.

Wir würden uns freuen, wenn unsere erweiterte Website Ihr Interesse findet! Bei Fragen hierzu stehen Ihnen alle Kolleginnen und Kollegen bei Loschelder zur Verfügung, Ihren passenden Ansprechpartner finden Sie auch zu den spezifischen Digitalisierungsthemen verlinkt.



## Das „Zweite Datenschutz-Anpassungs- und Umsetzungsgesetz“

*In der Nacht vom 27. auf den 28. Juni 2019, also in der letzten Woche vor der Sommerpause, hat der Bundestag in einer nächtlichen Sitzung mit*

*Minimalbesetzung das „Zweite Datenschutz-Anpassungs- und Umsetzungsgesetz“ verabschiedet; mit über einem Jahr Verzögerung (auch dieses Gesetz hätte nach den EU-Anforderungen bereits am 25. Mai 2018 in Kraft treten müssen) und hoch umstrittenen Inhalten. Das sogenannte „Zweite Datenschutz-Anpassungs- und Umsetzungsgesetz“ betrifft 154 Einzelgesetze und passt diese an die DSGVO an. Daneben enthält es aber auch allgemeingültige Neuregelungen, insbesondere zur Bestellpflicht eines Datenschutzbeauftragten.*

Das Zweite Datenschutz-Anpassungs- und Umsetzungsgesetz (kurz: 2. DSAnpUG-EU) wird auch als „Omnibusgesetz“ bezeichnet, da es die Anpassung von über 150 Einzelgesetzen an die Datenschutzgrundverordnung umfasst – „Fahrgäste“ dieses Omnibusses sind etwa das Informationsfreiheitsgesetz, der Postdatenschutz oder die Sozialgesetzbücher. Die Regelungen, die mit den über 150 zu ändernden Gesetzen fast alle Ressorts betreffen, beinhalten sowohl redaktionelle Änderungen als auch inhaltliche Nejustierungen, die für die jeweiligen Spezialbereiche von großer Bedeutung sind.

Von allgemeiner Bedeutung für alle Unternehmen sind zwei Änderungen am Bundesdatenschutzgesetz, die sich in dem umfassenden 2. DSAnpUG-EU beinahe verstecken:

- „In § 26 Absatz 2 Satz 3 BDSG „werden die Wörter „bedarf der Schriftform“ durch die Wörter „hat schriftlich oder elektronisch zu erfolgen“ ersetzt“.
- „In § 38 Absatz 1 Satz 1 wird das Wort „zehn“ durch die Angabe „20“ ersetzt.“

(Beschlussempfehlung, Drucksache 19/11181, S. 7)

Was bedeuten diese unscheinbar erscheinenden Änderungen? In der Praxis eine ganze Menge:

- Auch im Beschäftigungsverhältnis können **Einwilligungen** künftig – entsprechend der weiteren DSGVO-Anforderungen – elektronisch abgegeben und eingeholt werden. Die Schriftform-Begrenzung wird aufgegeben.
- Kleine Unternehmen werden von der Pflicht, einen **Datenschutzbeauftragten** zu bestellen, entlastet: Erst ab 20 Mitarbeitern – und nicht, wie bisher, ab 10 Mitarbeitern – die sich ständig mit der automatisierten Verarbeitung personenbezo-

gener Daten beschäftigen, muss ein Datenschutzbeauftragter bestellt werden.

Letztere Änderung führt zu einer Entlastung kleiner Unternehmen; zu beachten bleibt allerdings, dass die Anforderungen der DSGVO auch von diesen kleinen Unternehmen einzuhalten sind – es entfällt aber die formale Bestellpflicht.



### **Datenschutz beim Asset Deal**

*Wann welche personenbezogenen Daten beim Asset Deal an Interessenten und Vertragspartei datenschutzrechtskonform übermittelt werden dürfen, wird seit jeher kontrovers diskutiert. Die Datenschutzkonferenz hat Ende Mai einen insofern sehr hilfreichen Katalog veröffentlicht, wann aus ihrer Sicht die Übermittlung personenbezogener Daten zulässig ist.*

Jede Übertragung von personenbezogenen Daten von einem Unternehmen zu einem anderen stellt eine erlaubnispflichtige Verarbeitung dar. Hierzu kommt es auch beim Asset Deal, bei dem – anders, als im Fall eines Share Deals – Vermögenswerte eines Unternehmens inklusive personenbezogener Daten von einer juristischen Person auf eine andere übertragen werden. Wann und wie dies erlaubt ist, wird kontrovers diskutiert. Wir haben dies zuletzt in unserem [März-Newsletter](#) aufbereitet.

Für die Praxis überaus hilfreich ist angesichts dessen der von der Datenschutzkonferenz unter dem 24. Mai 2019 nun veröffentlichte

Beschluss „[Asset Deal – Katalog von Fallgruppen](#)“, der auflistet, wann welche Datenübermittlung nach Ansicht der Aufsichtsbehörden datenschutzrechtlich aufgrund überwiegender berechtigter Interessen Art. 6 Abs. 1 Satz 1 lit. f i.V.m. Abs. 4 DSGVO regelmäßig zulässig ist bzw. welche zusätzlichen Anforderungen zu beachten sind. Behandelt werden die Fallgruppen

- Kundendaten bei laufenden Verträgen (die ohnehin zivilrechtlich zustimmen müssen),
- Bestandskunden ohne laufende Verträge (liegt der letzte Kontakt maximal 3 Jahre zurück, ist eine Übermittlung an und aktive Nutzung durch das erwerbende Unternehmen regelmäßig zulässig),
- Daten bei fortgeschrittener Vertragsanbahnung (mit Widerspruchslösung und ausreichend bemessener Widerspruchsfrist),
- Kundendaten im Fall offener Forderungen (bei denen die Übertragung regelmäßig im Annex zur Forderungsabtretung berechtigt ist) sowie
- Kundendaten besonderer Kategorien, etwa Gesundheitsdaten, die nur mit Einwilligung übergeleitet werden können.

Es gilt danach: Wo praktikabel, bietet sich die Anwendung der ausdeklinierten Fallgruppen an. Indes ist auch hierbei stets der Einzelfall im Auge zu behalten: Besonderheiten können durchaus eine umfangreichere Datenübermittlung tragen, indes auch zu stärkeren Restriktionen führen.



## **Geltendmachung von Betroffenenrechten: Identitätsprüfung**

*Die DSGVO enthält bekanntlich umfangreiche Betroffenenrechte. Diese sollten indes nicht vorschnell erfüllt werden: Die datenverarbeitende Stelle muss sicherstellen, dass sie stets „den richtigen“ Betroffenen vor sich hat. Dies gilt etwa für Auskunftersuchen, deren Inhalt nicht an Dritte gelangen soll. Was nach einer Selbstverständlichkeit klingt, kann sich in der Praxis durchaus als Herausforderung entpuppen: die Identifikation der antragstellenden Person als auskunftsberechtigt. Wann welche Maßnahmen zur Identitätsprüfung notwendig und zulässig sind, hat kürzlich der BayLfD konkretisiert.*

Erhält ein Unternehmen einen Antrag auf Geltendmachung von Betroffenenrechten, ist es unumgänglich, den Antragsteller als Berechtigten zu identifizieren (Art. 12 DSGVO). Nachweislich geklärt werden muss, ob der Antragsteller der Inhaber des Betroffenenrechts, also derjenige, dessen personenbezogenen Daten verarbeitet werden.

Zur Ausräumung von Zweifeln an der Identität des Antragstellers gibt es verschiedene Möglichkeiten, die bei Bedarf miteinander kombiniert werden können. Der BayLfD hat hierzu jüngst eine illustrative [Kurzinformation](#) veröffentlicht, die auch von privaten Unternehmen herangezogen werden kann (der BayLfD ist Datenschutzaufsichtsbehörde alleine für die bayerischen öffentlichen Stellen):

Bislang unbekannte Daten können mit bereits in der Datenbank vorhandenen Daten abgeglichen werden; es können zusätzliche Informationen abgefragt werden, wie z.B. Geburtsdatum, Adresse, Transaktionsnummer oder ein zuvor vereinbartes Passwort; eine Identifizierung kann per Bestätigungslink (double-opt-in) durchgeführt werden; die Geltendmachung der Betroffenenrechte ist über ein privates Kundenkonto möglich; eine Identifikation kann auch per Post-/Video-Ident-Identifikation erfolgen. Auch die Abfrage einer Ausweiskopie ist denkbar, allerdings sollte dies nur nach besonderer Prüfung erfolgen (häufig werden hierdurch zusätzliche Daten verarbeitet, die zur Zweckerreichung der Identifikation nicht erforderlich sind und deren Verarbeitung damit unzulässig ist).

Die Daten, die zur Identifikation der antragstellenden Person verarbeitet werden, sind übrigens an diesen Zweck gebunden und nach Zweckerreichung (Identitätsnachweis) zu löschen, sofern keine spezifische Erlaubnis für die Speicherung mehr vorliegt (die zunächst in dem berechtigten Interesse liegen dürfte, nachweisen zu können, dass die Betroffenenrechte ordnungsgemäß erfüllt wurden).



**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