LOSCHELDER

Newsletter Datenschutzrecht

März 2019

Inhalt

Löschung durch Anonymisierung?

Vorsorgliche und reguläre Einwilligung

Einwilligung bei Adresshandel und Asset Deal?

Bundesverfassungsgericht zu Datenschutzthemen

Löschung durch Anonymisierung?

Verantwortliche sind gemäß Art. 17 DSGVO zur Löschung personenbezogener Daten verpflichtet. Dieser Pflicht können sie – so entschied es die österreichische Datenschutzbehörde im Dezember 2018 (Bescheid) – durch Anonymisierung genügen. Ein Personenbezug darf aber weder für den Verantwortlichen noch einen Dritten ohne unverhältnismäßigen Aufwand wieder herstellbar sein. Das Löschen von personenbezogenen Daten setzt demnach nicht immer auch die Vernichtung der Daten voraus. Trotz Löschungsbegehren kann somit die Nutzung werthaltiger Daten ohne Personenbezug weiter möglich bleiben.

Art. 17 DSGVO verpflichtet in weitem Umfang zur Löschung personenbezogener Daten, etwa wenn Einwilligungen widerrufen oder Vertragszwecke erreicht wurden. Die im Zuge der Datenverarbeitung angelegten Datensätze können indes auch ohne Bezug zu einer spezifischen natürlichen Person werthaltig sein, etwa um ein typisches Vertragsverhalten oder Nutzerinteressen statistisch auszuwerten. In vielen Fällen kann es daher für den Verantwortlichen von erheblichem Wert sein, wenn er die Datensätze weiterverwenden kann und lediglich den Bezug zu einer bestimmten Person entfernt, mithin eine Anonymisierung durchführt. Ob dies den Anforderungen an die Datenlöschung genügt, wird streitig diskutiert – denn Art. 17 DSGVO spricht nur von „löschen", umgangssprachlich verstanden als „vernichten", und jedenfalls nicht explizit vom Anonymisieren.

Die österreichische Datenschutzbehörde musste nun jüngst entscheiden, ob ein Anspruch auf Löschung von Kundendaten auch durch Anonymisierung erfüllt werden kann oder ob zwingend eine Vernichtung der Daten erforderlich ist. Bei den zu löschenden Daten handelte es sich um Daten aus einer allgemeinen Online-Berater-Anfrage zu einer KFZ-Versicherung. Die Recherchen des Verantwortlichen zu dem Betroffenen in seinen IT-Systemen ergaben zunächst zwei seit 2015/2016 stornierte Vertragsverhältnisse zu einer Rechtsschutz- und KFZ-Versicherung. Der Verantwortliche löschte die personenbezogenen Kontaktdaten des Betroffenen – trotz noch nicht final geklärter Identität – für sämtliche Marketingzwecke. Da aber nach der ersten Abfrage der Datenbestände Daten eines weiteren Vertragsverhältnisses noch fehlten, stellte der Verantwortliche erneut Recherchen an. Unter anderem durch Rücksprache mit dem Kundenberater konnte der Bezug einzelner Kun-

dendaten zu dem Betroffenen hergestellt werden. Die dem Betroffenen demnach zuzuordnenden Daten wurden – je nach System – entweder sofort gelöscht oder anonymisiert.

So wurde etwa sowohl die Kundenanfrage als auch das Angebot, das aufgrund der Onlineangaben des Kunden vom Kundenmanagementsystem erstellt worden war, gelöscht, ebenso wir alle elektronischen Kontakte (E-Mail-Adresse, Telefonnummer, etc.) des Kunden. Sowohl Name als auch Adresse sind dann durch eine anonyme, nicht zuordenbare Person (Max Mustermann) mit identischem Geschlecht und Geburtsdatum unwiderruflich manuell überschrieben worden. Die nun inhaltsleere Kundenverbindung war nur noch Max Mustermann zugeordnet. Die hierfür verwendete Technik gewährleistete, dass diese Schritte nachhaltig erfolgten. Auch in den Logdaten wurden bei alledem keine personenbezogenen Daten gespeichert, da die Identifikation ausschließlich über Kennzahlen („ID´s“) erfolgte.

Nach Ansicht der österreichischen Datenschutzbehörde ist durch die Umsetzung all dieser beschriebenen Schritte eine faktische Anonymisierung der ursprünglichen Kundenverbindung durch das Überschreiben mit einer „Dummy Kundenverbindung“ herbeigeführt worden. Es waren danach keine personenbezogenen Daten und somit keine identifizierenden Merkmale mehr vorhanden, die mit der ursprünglichen Onlineanfrage des Kunden in Verbindung gebracht werden könnten. Dies genügte den Löschanforderungen des Art. 17 DSGVO.

Damit ist aufsichtsbehördlich eine Auslegung bestätigt worden, die die Betroffenenrechte und die wirtschaftlichen Interessen der Verarbeiter in einen angemessenen Ausgleich bringt: Denn Daten können auch ohne Personenbezug werthaltig sein, beispielsweise für Statistikzwecke.

Vorsorgliche und reguläre Einwilligung

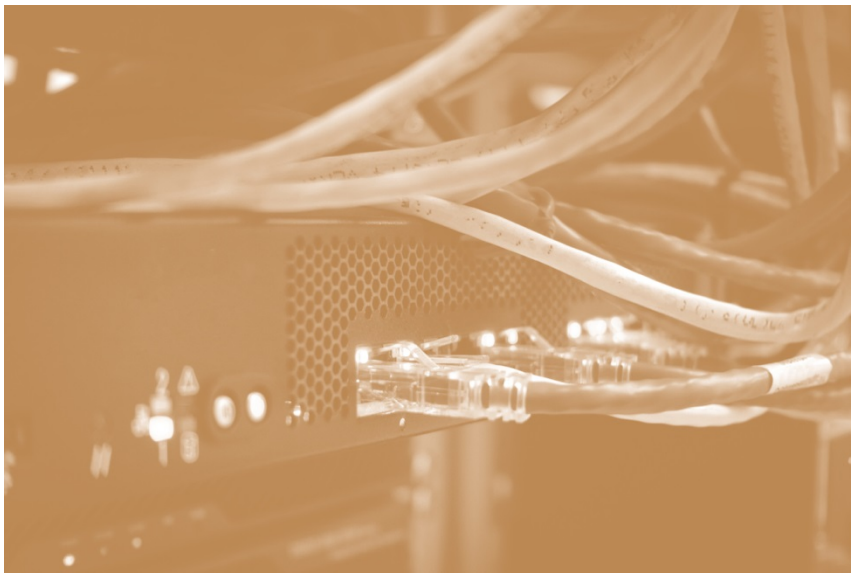
In den letzten Wochen sind zwei interessante Hilfestellungen rund um das Thema Einwilligung veröffentlicht worden. Zum einen hat sich auch der HBDI pro „vorsorgliche" Einwilligung positioniert. Zum anderen hat die Datenschutzkonferenz ein Kurzpapier Nr. 20 zu den Anforderungen an DSGVO-konforme Einwilligungen herausgegeben.

Der HBDI hält eine „vorsorgliche" Einwilligung für zulässig. Vorsorglich bedeutet, eine Einwilligung für den Fall einzuholen, dass einer der gesetzlichen Erlaubnistatbestände nicht greift: Eine Datenverarbeitung kann dann beispielsweise zuvörderst auf eine Vertragserfüllung gem. Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO gestützt werden und zusätzlich – sicherheitshalber – auf eine Einwilligung nach Art. 6 Abs. 1 UAbs. 1 lit. a DSGVO. Ob dies zulässig ist, ist im Hinblick auf das Fairnessgebot hoch umstritten, Art. 5 DSGVO:

Bei Betroffenen wird der Eindruck erweckt, sie könnten mit einem Widerruf der Einwilligung die Verarbeitung verhindern. Dagegen bleibt die Verarbeitung auf Grundlage des gesetzlichen Erlaubnistatbestandes weiter möglich. Aus dem Grund hat sich etwa der LfDI BW bereits vor einiger Zeit deutlich gegen die Zulässigkeit vorsorglicher Einwilligungen ausgesprochen (Ratgeber zum Beschäftigtendatenschutz, S. 19; kritisch auch in der jüngst veröffentlichten Neuauflage des Ratgebers, S. 20 f.). Teilweise wird die vorsorgliche Einwilligung als zulässig erachtet, aber erhöhte Informationspflichten angenommen. Es müsste auf das Vorliegen eines ge-

setzlichen Erlaubnistatbestandes und auf den rein vorsorglichen Charakter hingewiesen werden. Mit der aktuellen Positionierung für die Zulässigkeit der vorsorglichen Einwilligung durch die Hessische Aufsichtsbehörde bleibt die Debatte offen und der Weg über eine vorsorgliche Einwilligung wird noch besser vertretbar. Für die Datenverarbeiter ist dies vorteilhaft, weil das Vorliegen eines gesetzlichen Erlaubnistatbestandes nicht immer eindeutig ist. Die vorsorgliche Einwilligung kann – wenn sie wirksam ist (allgemeine Anforderungen) – ein Sicherheitsnetz darstellen. Gleichwohl ist nicht stets der Weg über die aufwändige Einwilligung sinnvoll, sondern regelmäßig nur für die Grenzfälle gesetzlicher Erlaubnistatbestände.

Zu den Anforderungen an wirksame Einwilligungen im Allgemeinen hat sich jüngst auch die Datenschutzkonferenz positioniert: Das oben erwähnte Kurzpapier Nr. 20 der Datenschutzkonferenz kann denjenigen, die sich über die allgemeinen rechtlichen Anforderungen der Einwilligung einen Überblick verschaffen wollen, als Hilfestellung dienen. Es ergänzt bzw. fasst die Leitlinien zur Einwilligung des europäischen Datenschutzausschusses (WP 259 rev. 01 „Leitlinien in Bezug auf die Einwilligung gemäß V. 2016/679“) zusammen. Interessant sind die konkretisierenden Ausführungen zur Fortgeltung von Einwilligungen, die vor dem Inkrafttreten erteilt wurden. Insoweit hält die DSK an der Positionierung der BayLDA bereits aus dem vergangenen Jahr fest: „Alt-Einwilligungen“ gelten fort, wenn sie der Art nach bereits den wesentlichen Bedingungen der DSGVO entsprechen (vgl. Erwägungsgrund 171 DSGVO).



Einwilligung bei Adresshandel und Asset Deal?

Jede Übertragung von personenbezogenen Daten von einem Unternehmen zu einem anderen stellt eine erlaubnispflichtige Verarbeitung dar. Daher sind die Pflichten der DSGVO sowohl beim Adresshandel als auch im Rahmen von Asset Deals zu beachten: Für jede Datenübertragung muss ein Erlaubnistatbestand vorliegen. Da das neue Datenschutzrecht keine spezifischen Vorgaben zum Adresshandel mehr beinhaltet, wie dies beim alten BDSG der Fall war, kommt es dabei regelmäßig zu Wertungsfragen und Auslegungsschwierigkeiten, die sich dank neuer Positionierungen von Aufsichtsbehörden zunehmend rechtssicher beantworten lassen.

Als Erlaubnisgründe für den Adresshandel kommen das berechtigte Interesse nach Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO und die Einwilligung nach Art. 6 Abs. 1 UAbs. 1 lit. a DSGVO in Betracht. Wenn es nach dem 34. Tätigkeitsbericht des LfDI BW geht, überwiegen beim Adresshandel mit Kundendaten regelmäßig die Interessen des Betroffenen, so dass eine Übertragung ohne Einwilligung verboten bleibt. Ob sich diese Meinung letztlich durchsetzt, erscheint überaus fraglich – auch beim Adresshandel gibt es überzeugende Ansatzpunkte, je nach Umfang, Ziel und Herkunft der Daten überwiegende berechtigte Interessen i.S.d. Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO zu bejahen.

Noch differenzierter ist die Rechtfertigungslage beim Asset Deal, der sich nicht allein auf die Übertragung von Kundendatenbanken bezieht. Bei der Unternehmensübertragung im Wege eines Asset Deals werden die Vermögenswerte des Unternehmens und damit auch Datenbanken etc. mit personenbezogenen Daten, in dessen „Besitz“ das Unternehmen ist, einzeln an ein anderes Unternehmen übertragen. Kunden-, Patienten- oder Mandantendaten können im Einzelfall einen erheblichen, wenn nicht gar weit überwiegenden Teil am Wert eines Unternehmens ausmachen. Im Unterschied zum Share Deal, bei dem leidglich Unternehmensanteile verkauft werden, so dass der Verantwortliche i.S.d. Art. 4 Nr. 7 DSGVO nicht wechselt, kommt es beim Asset Deal zu einer erlaubnispflichtigen Datenübertragung im Sinne der DSGVO von einem Verantwortlichen zu einem anderen.

Erlaubt ist eine solche Datenübertragung danach regelmäßig in Fällen der Vertragsübernahme: Übernimmt der Unternehmenskäufer die Kundenverträge des Verkäufers, dient die zukünftige Verarbei-

tung der personenbezogenen Daten der Vertragserfüllung im Sinne von Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO. Wenn indes keine Übernahme der einzelnen Verträge stattfindet, kommen als Erlaubnistatbestände insbesondere die Einwilligung nach Art. 6 Abs. 1 UAbs. 1 lit. a DSGVO oder das überwiegende berechtigte Interessen nach Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO in Betracht:

Das praktische Problem mit Einwilligungen besteht nun darin, dass die Einholung von Einwilligungen vorab regelmäßig äußerst umständlich ist, weil sie von *allen* Betroffenen eingeholt werden müssen und die Rücklaufquoten erfahrungsgemäß niedrig sind. Die Übertragung geschlossener Datenbanken ist so regelmäßig nicht möglich; auch fordert die Einholung von Einwilligungen eine Ansprache der Betroffenen womöglich zu einem Zeitpunkt, zu dem der Deal noch nicht bekannt werden soll (etwa, wenn bereits für die Bewertung bekannt werden muss, wie viele und welche Datensätze überhaupt auf den Verkäufer übertragen werden können). Über eine Zweckänderung der Datenvereinbarung sind die Betroffenen vor Übermittlung der Daten jedoch zu informieren, Art. 13 Abs. 3, 14 Abs. 4 DSGVO.

Ausgehend davon, dass im Zuge des Asset Deals keine sensiblen Daten gem. Art. 9 DSGVO, beispielsweise Gesundheitsdaten, übertragen werden (dann wird stets eine Einwilligung benötigt), bleibt dem Verkäufer und Käufer alternativ der Erlaubnistatbestand des berechtigten Interesses gem. Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO. In diesem Fall ist eine dokumentierte Einzelabwägung vorzunehmen:

Es muss ein berechtigtes Interesse des Verkäufers und / oder des Käufers vorliegen, die Verarbeitung muss zur Wahrung dieser berechtigten Interessen erforderlich sein und die Interessen des Betroffenen dürfen nicht überwiegen. In vielen Fällen wird es im berechtigten Interesse von Verkäufer und Käufer liegen, Kundendaten im Zuge eines Asset Deals zu übertragen, wenn nur so eine erfolgreiche Transaktion möglich ist. Dies gilt jedenfalls dann, wenn das Unternehmen nach Verkauf fortgeführt wird und der Fokus des Deals auf dem Unternehmensgegenstand liegt und es kein Fall eines „verschleierten" Adresshandel ist. In diesen Fällen liegt es regelmäßig auch im Interesse des Kunden, dass seine Vertragsbeziehungen fortgeführt werden. Unternehmen sollten einen Verkauf zudem dazu nutzen, die eigene Kundendatenbank auszumisten und um „Karteileichen" zu bereinigen. Das sorgt zunächst dafür, dass die Werthaltigkeit der Kundendatenbank sicher ermittelt wer-

den kann und löst ferner datenschutzrechtliche Probleme, da Datensätze, bei denen eine Interessenabwägung höchstwahrscheinlich zu Lasten von Verkäufer und Käufer ausgeht, bereits zuvor gelöscht werden.

Bundesverfassungsgericht zu Datenschutzthemen

Das BVerfG hatte kürzlich (Ende 2018 und Anfang 2019) gleich zweimal Gelegenheit, sich mit der Reichweite des Schutzes des Grundrechts auf informationelle Selbstbestimmung in datenschutzrechtlichem Zusammenhang auseinanderzusetzen. Im Wesentlichen bestätigte das Gericht seine bisherige Rechtsprechung. Im Falle der Verfassungsbeschwerde entschied es Ende 2018, dass die automatisierte KFZ-Kennzeichenkontrolle in Bayern gegen das Recht auf informationelle Selbstbestimmung verstößt und erklärte die Regelung als teilweise verfassungswidrig. Im zweiten Falle lehnte es den Antrag, § 9a des Gesetzes zur Vorbereitung des Zensus 2021 (ZensVorbG 2021) außer Vollzug zu setzen, ab.

Für Unternehmen sind diese Entscheidungen deswegen äußerst interessant und relevant, weil sich hieraus allgemeine Aussagen und Wertungen für die Zulässigkeit eigener Geschäftsmodelle ziehen lassen, bspw. im Rahmen einer eigenen Kennzeichenerfassung oder eines Kunden- oder Mitarbeiterprofilings.

Das 1983 im sogenannten „Volkszählungsurteil“ des Bundesverfassungsgerichts als Grundrecht anerkannte Recht auf informationelle

Selbstbestimmung schützt die freie Entfaltung der Persönlichkeit unter den modernen Bedingungen der Datenverarbeitung. Dies setzt den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Grundsätzlich ist jeder selbst befugt, über die Preisgabe sowie die Verwendung seiner persönlichen Daten zu entscheiden. Bereits aus dieser Kurzdefinition lässt sich die besondere Relevanz des Grundrechts für den Datenschutz erkennen.

Der Beschluss des Bundesverfassungsgerichts vom 6.2.2019 zum Zensus 2011 stellt klar, dass schon eine umfangreiche Speicherung von nicht anonymisierten Daten (Klardaten) einen Nachteil für die Freiheit und Privatheit des Einzelnen darstellt. Zu einer irreparablen Beeinträchtigung, die höher zu gewichten ist und im Einzelfall schwerer zu rechtfertigen ist, verdichtet sich der Eingriff erst mit der tatsächlichen Abrufung der Daten, nicht bereits mit der bloßen Speicherung. Das Erfassen der Daten ist daher streng zu trennen von ihrer Verarbeitung. Beide Maßnahmen greifen in das Recht auf informationelle Selbstbestimmung ein und bedürfen daher einer entsprechenden Rechtsgrundlage, aber mit unterschiedlichem Gewicht.

Zudem betonte das Bundesverfassungsgericht erneut, dass das Grundrecht seinen Schutz auch schon im Vorfeld von datenschutzrechtlich relevanten Maßnahmen (seitens des Staates) entfaltet. Dass bzw. ob Daten, die erhoben werden, öffentlich zugänglich sind, vermag hieran nichts zu ändern. Der Umgang mit personenbezogenen Daten muss daher entsprechend transparent sein, um dem individuellen Rechtsschutz zu genügen und entsprechende Kontrolle zu gewährleisten. Damit Eingriffe gerechtfertigt sein können, müssen insbesondere tragfähige Regelungen zur Nutzung und Löschung der Daten bestehen. Die Besonderheit der elektronischen Datenverarbeitung liege gerade darin, dass Unmengen von Daten zusammengeführt, ausgewertet und verbunden werden könnten, was wiederum neue Rückschlüsse auf die private Lebensgestaltung der Betroffenen zulasse. Inwiefern etwa die automatisierte Erfassung von Kfz-Kennzeichen damit vereinbar ist, muss differenziert und vor allem mit Blick auf die Verhältnismäßigkeit und den Bestimmtheitsgrundsatz beantwortet werden. So wäre vor allem eine anlasslose, flächendeckende und langfristige Speicherung nur unter engen Voraussetzungen zulässig. Diese grundsätzlichen Gedanken gelten auch für die Datenverarbeitung privater Unternehmen, so-

dass eine privat betriebe Kennzeichenerfassung auch nur dann zulässig sein kann, wenn sie eng zweckgebunden und an den Grundsätzen der Erforderlichkeit ausgerichtet ist.

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