



1. Gesetzesänderungen

+++ REGISTERMODERNISIERUNGSGESETZ VERKÜNDET: STEUER-ID WIRD ZENTRALES PERSONENKENNZEICHEN FÜR VERWALTUNGSDATEN +++

Das nun verkündete Gesetz zur Einführung und Verwendung einer Identifikationsnummer in der öffentlichen Verwaltung (Registermodernisierungsgesetz) führt auf Grundlage der Steuer-ID eine individuelle, übergreifende Identifikationsnummer für Bürgerinnen und Bürger (sog. „Bürger-ID“) ein. Der Bürger-ID werden künftig sämtliche Verwaltungsdaten der Bürger (z. B. Verwaltungsleistungen, Angaben und Nachweise gegenüber bestimmten Behörden) zugeordnet, um einen vereinfachten Datenaustausch zwischen den Behörden zu ermöglichen. Öffentliche Stellen können dann mithilfe der individuellen Bürger-ID auf die dort gespeicherten Daten zugreifen. Die Einführung der Bürger-ID als zentrales Personenkennzeichen wurde zuvor von Datenschutzbehörden und Datenschützern heftig kritisiert.

[Zur Pressemitteilung des Bundesministeriums des Inneren, für Bau und Heimat \(BMI\)](#)

+++ REFORM DER BESTANDSDATENAUSKUNFT BESCHLOSSEN +++

Nachdem der Bundesrat seine Zustimmung zur Neuregelung der Bestandsdatenauskunft zunächst verweigert hatte (siehe BB Datenschutz-Ticker Februar 2021), konnte das Gesetz nun mit geänderten Regelungen zur Passwortherausgabe verabschiedet werden.

Das Gesetz ermöglicht Sicherheitsbehörden unter bestimmten Umständen, von Telekommunikations-unternehmen Bestands- oder Nutzungsdaten ihrer Kunden zu erlangen. Auch eine Passwortherausgabe kommt bei besonders schweren Straftaten in Betracht. Zugleich wurden Änderungen an dem Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität vorgenommen, welches daraufhin am 3. April 2021 in Kraft trat.

[Weitere Informationen zur Neuregelung der Bestandsdatenauskunft](#)

[Informationen zum Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität](#)

2. Rechtsprechung

+++ OLG STUTTGART: KEINE BEWEISLASTUMKEHR/ BEWEISERLEICHTERUNG FÜR SCHADENSERSATZANSPRÜCHE NACH ART. 82 DSGVO, VORLAGE DER ORIGINALVOLLMACHT BEI AUSKUNFTSERSUCHEN +++

Das Oberlandesgericht Stuttgart hat entschieden, dass die allgemeinen zivilprozessualen Beweisregeln auch für Schadensersatzansprüche nach Art. 82 DSGVO gelten. Demnach muss der Kläger in einem Gerichtsverfahren den haftungsbegründenden Verstoß einer DSGVO-Pflicht darlegen und beweisen. Dagegen führten auch die Rechenschaftspflichten der beklagten Verantwortlichen (Art. 5 Abs. 2 DSGVO) nicht zu einer prozessualen Beweislastumkehr oder Beweiserleichterung zu Gunsten des Klägers. In dem verhandelten Fall konnte der Kläger nicht beweisen, dass die Beklagte ihre Pflichten aus Art. 32 DSGVO durch Nichteinhaltung von Sicherheitsstandards verletzt hat.

In demselben Urteil hat das OLG Stuttgart auch klargestellt, dass ein Auskunftsersuchen nach Art. 15 DSGVO, das durch einen Bevollmächtigten (z. B. einen Rechtsanwalt) geltend gemacht wird, vom Verantwortlichen zurückgewiesen werden darf, bis der Bevollmächtigte eine von dem Betroffenen ausgestellte Vollmacht im Original vorlegt. Das Gericht erklärte die entsprechende Norm des Bürgerlichen Gesetzbuchs (§ 174 BGB) auf DSGVO-Auskunftsersuchen für anwendbar.

[Zu dem Urteil des OLG Stuttgart \(v. 31. März 2021, Az. 9 U 34/21\)](#)

+++ LArbG BW: VERARBEITUNG VON BESCHÄFTIGTENDATEN DURCH US-KONZERNMUTTER KANN DSGVO-SCHADENS- ERSATZPFLICHT DES ARBEITGEBERS AUSLÖSEN +++

Das Landesarbeitsgericht Baden-Württemberg hat festgestellt, dass die „Gefahr eines Missbrauchs von Daten durch Ermittlungsbehörden in den USA oder andere Konzerngesellschaften“ bzw. der „Verlust, die

personenbezogenen Daten kontrollieren zu können“ geeignet ist, einen immateriellen Schaden nach Art. 82 DSGVO bei den betroffenen Arbeitnehmern zu begründen. Der Kläger war bei dem beklagten Unternehmen, einer deutschen Konzerntochter, angestellt. Das beklagte Unternehmen übermittelte im Rahmen des konzernweit genutzten Systems „Workday“ Beschäftigtendaten an eine Sharepoint-Seite der in den USA ansässigen Konzernmutter. Das Gericht erkannte hierin einen „Kontrollverlust“ in Bezug auf die übermittelten Daten, der grundsätzlich zu einem ersatzfähigen Schaden führen könne. Das Gericht wies die Klage dennoch ab, da der Schaden im konkreten Fall nicht (kausal) auf einen DSGVO-Verstoß zurückzuführen sei.

[Zum Urteil des LArbG \(v. 25. Februar 2021, Az. 17 Sa 37/20\)](#)

3. Behördliche Maßnahmen

+++ BAYLDA: UNGEPRÜFTER EINSATZ VON NEWSLETTER TOOL MAILCHIMP RECHTSWIDRIG +++

Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) hält den Einsatz des Newsletter-Versand-Tools Mailchimp für unzulässig, wenn vorab nicht geprüft worden ist, ob die Übermittlung von E-Mail-Adressen in die USA durch „zusätzliche Maßnahmen“ abzusichern ist. Der EuGH hatte in der sog. „Schrems-II“-Entscheidung (EuGH, Urt. v. 16.7.2020, C-311/18, siehe [BB Datenschutz-Ticker Juli 2020](#)) festgestellt, dass Verantwortliche ggf. zusätzliche Maßnahmen zum Schutz von personenbezogenen Daten ergreifen müssen, bevor die Daten in die USA übermittelt werden. Das BayLDA stellt fest, dass Mailchimp als Anbieter von elektronischen Kommunikationsdiensten dem aus europäischer Sicht besonders kritischen US-Gesetz „FISA702“ unterfallen könne, das US-Geheimdiensten den Zugriff auf die übermittelten Daten erlaube.

[Zur Entscheidung des BayLDA im Rahmen eines Beschwerdeverfahrens](#)

+++ SPANISCHE DATENSCHUTZBEHÖRDE: EUR 8,15 MIO. BUßGELD GEGEN MOBILFUNKGESELLSCHAFT +++

Die spanische Datenschutzbehörde Agencia Española Protección Datos (AEPD) hat wegen verschiedener Datenschutzverstöße Bußgelder in Höhe von insgesamt EUR 8,15 Mio. gegen die Vodafone España S.A.U. verhängt. Hiervon wurden allein EUR 2 Mio. wegen der Einschaltung eines Auftragsverarbeiters verhängt, der die zu verarbeitenden Kundendaten seinerseits ohne hinreichende Absicherung an einen Unter-Auftragsverarbeiter, der in einem Drittstaat (Peru) ansässig war, übermittelte. Die weiteren Vorwürfe der Behörde drehten sich u. a. um die Versendung von Werbe-E-Mails, für die der Konzern keine Einwilligung der Kunden eingeholt habe.

[Zu dem Bußgeldbescheid der AEPD \(spanisch\)](#)

+++ ITALIENISCHE DATENSCHUTZBEHÖRDE: EUR 4,5 MIO. BUßGELD GEGEN TELEKOMMUNIKATIONSUNTERNEHMEN +++

Die italienische Datenschutzbehörde Garante per la Protezione dei Dati Personali (GPDP) hat ein Bußgeld in Höhe von rund EUR 4,5 Mio. gegen das Telekommunikationsunternehmen Fastweb S.p.A. verhängt. Die Behörde erhielt hunderte Beschwerden über unzulässige Werbeanrufe des Unternehmens. In einer umfassenden Untersuchung deckte die Behörde systematische Verstöße bei Fastweb und deren Callcentern auf. Die Unternehmen hätten u. a. von Dritten stammende Kundenlisten und Kontaktdaten für Werbeanrufe missbraucht, keine hinreichenden Maßnahmen zum Schutz der Daten getroffen und Betroffenenrechte nur mangelhaft erfüllt. Insgesamt sollen Kontaktdaten von über 7,5 Mio. Betroffenen ohne deren Einwilligung verarbeitet worden sein.

[Zur Pressemitteilung der GPDP \(italienisch\)](#)

+++ NIEDERLÄNDISCHE DATENSCHUTZBEHÖRDE: BUßGELD FÜR ZU SPÄT GEMELDETES DATENLECK +++

Die niederländische Datenschutzbehörde Autoriteit Persoonsgegevens (AP) hat ein Bußgeld in Höhe von EUR 475.000 gegen Booking.com festgesetzt. Die Buchungsplattform für Reiseunterkünfte erlangte Anfang 2019 Kenntnis von einem Datenschutzvorfall, bei dem sich Angreifer Zugang zu Daten (u. a. Namen, Adressen, Telefonnummern und Buchungsdetails) von 4109 Kunden verschafft hatten. Booking.com meldete der Behörde diesen Vorfall erst nach 25 Tagen. Die DSGVO sieht für derartige Datenschutzvorfälle eine Meldefrist von höchstens 72 Stunden vor.

[Zur Pressemitteilung der AP \(englisch\)](#)

4. Stellungnahmen

+++ BlnDSB: ZUR ZULÄSSIGKEIT VON 360-GRAD MITARBEITER FEEDBACK AM ARBEITSPLATZ +++

Die Berliner Beauftragte für Datenschutz und Informationsfreiheit (BlnDSB) hat in ihrem Tätigkeitsbericht für das Jahr 2020 konkrete Anforderungen an die Ausgestaltung von sog. „360-Grad-Feedback“ Verfahren am Arbeitsplatz gestellt. Bei diesen Verfahren wird die Arbeitsleistung der Beschäftigten von den eigenen Kolleginnen und Kollegen (z. B. durch Benotung) beurteilt. Der Einsatz derartiger Konzepte dürfe nicht zu einem permanenten Überwachungsdruck bei den Betroffenen führen. Ablauf und Inhalt der Bewertungsverfahren müssten transparent offengelegt werden. Im konkret überprüften

Verfahren musste das Unternehmen die Anzahl der bewertenden Mitarbeiter auf drei beschränken. Den betroffenen Beschäftigten wurde zudem ein Vetorecht gegen einzelne Bewertungen eingeräumt.

[Zum Jahresbericht 2020 der BlnDSB](#)

+++ DULDUNG VON WEIT VERBREITETEN VIDEOKONFERENZSYSTEMEN DURCH SCHULEN LÄUFT AUS +++

Der Hessische Beauftragte für Datenschutz und Informationsfreiheit (HBDI) hat erklärt, dass der Einsatz von nicht datenschutzkonformen Videokonferenzsystemen durch Schulen nur noch bis zum 31. Juli 2021 geduldet wird. Der HBDI hatte sich vor dem Hintergrund des Pandemiegeschehens im April 2020 für eine temporäre Duldung weit verbreiteter Videokonferenzlösungen ausgesprochen. Eine (weitere) Verlängerung dieser Duldung sei nun ausgeschlossen, da bis zum Beginn des neuen Schuljahres datenschutzkonforme Alternativen bereitstünden. Insbesondere der Einsatz US-amerikanischer Videokonferenzsysteme, etwa Microsoft Teams, sei dann „weder erforderlich noch datenschutzrechtlich zulässig“.

[Zu der Stellungnahme des HBDI](#)

[Zu den Hinweisen der BlnBDI zu datenschutzgerechten Videokonferenzsystemen](#)

+++ BITKOM: LEITFADEN ZU DATENSCHUTZVERLETZUNGEN UND MELDUNGEN IM KONTEXT DES „HAFNIUM HACKS“ +++

Der Branchenverband Bitkom hat einen Leitfaden für Verantwortliche, die von dem sog. „Hafnium Hack“ betroffen sind, veröffentlicht. Dieser nutzte Sicherheitslücken in den Microsoft Exchange Servern aus (siehe BB [Datenschutz-Ticker März 2021](#)). Der Leitfaden enthält Informationen zu ggf. bestehenden Meldepflichten und den Auswirkungen des Hacks, etwa in Zusammenhang mit Auftragsverarbeitungen.

[Zu dem Leitfaden von Bitkom](#)

[Ihre Ansprechpartner](#)

Redaktion (verantwortlich)

[Dr. Andreas Lober](#)

Zur Newsletter Anmeldung
E-Mail weiterleiten



Hinweise

Diese Veröffentlichung stellt keine Rechtsberatung dar.

Wenn Sie künftig keine Informationen erhalten möchten, können Sie sich jederzeit [abmelden](#).

© BEITEN BURKHARDT

Rechtsanwalts-gesellschaft mbH

Alle Rechte vorbehalten 2021

Impressum

BEITEN BURKHARDT Rechtsanwalts-gesellschaft mbH

(Herausgeber)

Ganghoferstraße 33, D-80339 München

AG München HR B 155350/USt.-Idnr: DE-811218811

Weitere Informationen (Impressumsangaben) unter:

<https://www.beiten-burkhardt.com/de/impressum>