



# DATENSCHUTZ-TICKER

## 1. Gesetzesänderungen

### +++ BREXIT UND DATENSCHUTZ: ANGEMESSENHEITS-BESCHLUß IN SICHT +++

Die EU-Kommission hat das Verfahren zum Erlass eines Angemessenheitsbeschlusses eingeleitet, um auch nach dem Brexit die Übermittlung personenbezogener Daten aus der EU nach Großbritannien zu ermöglichen. Seit dem vollzogenen Brexit ist das Vereinigte Königreich Drittland im Sinne der DSGVO. Aufgrund des mit der EU vereinbarten Handels- und Kooperationsabkommens vom 31. Dezember 2020 wird Großbritannien jedoch während einer Übergangsfrist von maximal sechs Monaten nicht als Drittland angesehen, so dass derzeit noch keine zusätzlichen Sicherheitsmaßnahmen für den Datenaustausch vorgenommen werden müssen. Damit dies auch ab dem 1. Juli 2021 unverändert möglich ist, hat die EU-Kommission nun festgestellt, dass im Vereinigten Königreich ein angemessenes Datenschutzniveau im Sinne der DSGVO besteht, und hat den Entwurf eines entsprechenden Angemessenheitsbeschlusses vorgelegt.

[Zum Entwurf des Angemessenheitsbeschlusses](#)

### +++ NEUER ENTWURF DER E-PRIVACY-VERORDNUNG +++

Der Rat der Europäischen Union hat sich auf einen neuen Entwurf für die Europäische Verordnung über den Schutz der Privatsphäre und Vertraulichkeit in der elektronischen Kommunikation (sog. „ePrivacy-Verordnung“) geeinigt. Die Verordnung soll die Verarbeitung von auf dem Endgerät des Nutzers (z.B. Handy oder Tablet) gespeicherten Daten sowie von Kommunikations- und Metadaten bei der Nutzung von Online-Diensten neu regeln. Der Entwurf sieht u.a. vor, dass der Zugang zu einer Webseite unter bestimmten Umständen von der Einwilligung in die Verwendung von Cookies abhängig gemacht werden kann (sog. „Cookie Wall“). Auch sollen Verbindungsdaten anlasslos protokolliert werden können (sog. „Vorratsdatenspeicherung“). Der Ratsentwurf wird im nächsten Schritt dem EU-Parlament vorgelegt.

[Zur Pressemitteilung des Rats](#)

### +++ KABINETT BESCHLIEßT TELEKOMMUNIKATION-TELE MEDIEN-DATENSCHUTZGESETZ +++

Die Bundesregierung hat den Entwurf eines Telekommunikation-Telemedien-Datenschutzgesetzes (TTDSG) beschlossen, das den Trilogverhandlungen zur ePrivacy-Verordnung (s.o.) noch vorgehen soll. Das TTDSG führt Datenschutzbestimmungen aus Telemediengesetz (TMG) und Telekommunikationsgesetz (TKG) zusammen und schützt die Privatsphäre der Nutzer bei der Verwendung von Telemediendiensten. Auf einem Endgerät (etwa mithilfe von Cookies) gespeicherte Informationen dürfen nur noch mit Einwilligung des Nutzers ausgelesen werden, sofern dies nicht für die Bereitstellung des Dienstes erforderlich ist. Daneben enthält das TTDSG Regelungen zur Verarbeitung von Verkehrs- und Standortdaten und zum Fernmeldegeheimnis, insbesondere zum sog. „digitalen Nachlass“.

[Zum Gesetzesentwurf der Bundesregierung](#)

### +++ BUNDES RAT STOPPT REFORM DER BESTANDS-DATENAUSKUNFT +++

Der Bundesrat hat seine Zustimmung zur Neuregelung der Bestandsdatenauskunft verweigert. Mit dem Gesetzesentwurf sollten Anpassungen an dem „Gesetz zur Bekämpfung von Rechtsextremismus und Hasskriminalität“ vorgenommen werden, die nach einem Urteil des Bundesverfassungsgerichts erforderlich geworden waren (siehe [BB Datenschutz-Ticker Juli 2020](#)). Der Gesetzesentwurf sollte Telemedienanbieter u. a. dazu verpflichten, Nutzerpasswörter auf Anfrage von Behörden herauszugeben.

[Zur Pressemeldung des Bundesrats](#)

## 2. Rechtsprechung

### +++ BVERFG: ERHEBLICHKEITSSCHWELLE BEI DSGVO-SCHADENSERSATZ MUSS ZUM EUGH +++

Das Bundesverfassungsgericht (BVerfG) hat festgestellt, dass die ungeklärte Rechtsfrage, ob das Erreichen einer Erheblichkeitsschwelle Voraussetzung für einen ersatzfähigen immateriellen Schaden nach Art. 82 DSGVO ist, dem Europäischen Gerichtshof (EuGH) zur Vorabentscheidung vorzulegen ist. Seit Einführung der DSGVO ist dies heftig umstritten. Verschiedene Gerichte hatten zuletzt DSGVO-Schadensersatzforderungen von Betroffenen zurückgewiesen, wenn ein Datenschutzverstoß nur geringe Auswirkungen auf das Persönlichkeitsrecht hatte (sog. „Bagatellschäden“). Wie das BVerfG nun festgestellt hat, ergibt sich diese Erheblichkeitsschwelle aber nicht aus dem Gesetzestext. Im konkreten Fall geht es um ein Urteil des Amtsgerichts Goslar, das eine Schadensersatzforderung wegen des unrechtmäßigen Versands einer einzigen Werbe-Email zurückgewiesen hatte.

[Zum Beschluss des BVerfG \(v. 14. Januar 2021, Az. 1 BvR 2853/19\)](#)

### +++ LG KARLSRUHE: ABHANDENKOMMEN VON NAMEN, GEBURTSDATUM, GESCHLECHT, E-MAIL ADRESSE UND TELEFONNUMMER IST BAGATELLEN-SCHADEN +++

Das Landgericht Karlsruhe hat – mutmaßlich vor Veröffentlichung des o.g. Beschlusses des BVerfG – entschieden, dass ein DSGVO-Schadensersatzanspruch bei bloßen Bagatellschäden nicht besteht. Das Gericht wertete die Verbreitung des Namens, Geburtsdatums, Geschlechts, der E-Mail-Adresse und Telefonnummer des Klägers aufgrund eines Datenlecks als bloßen Bagatellschaden, von dem kein spürbarer Nachteil für den Kläger ausgegangen sei. Die Möglichkeit eines Identitätsdiebstahls sah das Gericht als „abstrakt“ und „nicht sonderlich wahrscheinliches Risiko“ an. Auch der Verlust von Transaktionsdaten führe nicht zu einem ersatzfähigen immateriellen Schaden, da diese keine kompromittierenden Informationen enthielten.

[Zum Urteil des LG Karlsruhe \(v. 9. Februar 2021, Az. 4 O 67/20\)](#)

### +++ LG FRANKFURT A.M.: KLÄGER TRIFFT BEWEISLAST FÜR DATENSCHUTZVERLETZUNG BEI DSGVO-SCHADENSERSATZ +++

Das Landgericht Frankfurt am Main hat entschieden, dass der Kläger die Darlegungs- und Beweislast dafür trägt, dass ein Datenleck bei der verantwortlichen Stelle auf eine Verletzung von DSGVO-Pflichten zurückzuführen ist. In dem Fall war es bei der Beklagten zu einem Datenleck gekommen. Daraufhin hatte der Kläger Spam-Anrufe und SMS erhalten und begehrte in der Folge Schadensersatz nach Art. 82 DSGVO von der Beklagten. Das Gericht wies die Klage ab, weil der Kläger letztlich nur vermutet, nicht aber schlüssig dargelegt habe, dass das Datenleck tatsächlich auf eine Pflichtverletzung der Beklagten zurückzuführen sei. Es sei denkbar, dass das Datenleck auf einen illegalen Hackerangriff zurückzuführen sei, mit dem die Beklagte und ihre Erfüllungsgehilfen in dieser Form nicht haben rechnen müssen. Der

Kläger konnte sich auch nicht auf die Beweislastumkehr aus Art. 82 Abs. 3 DSGVO berufen, da diese sich nur auf die Frage des Verschuldens, nicht aber auf die Pflichtverletzung bezieht.

[Zum Urteil \(v. 18. Januar 2021, Az. 2-30 O 147/20\)](#)

### +++ VG MAINZ: NUTZUNG VON TRANSPORTVERSCHLÜSSELUNG FÜR E-MAILS AUCH BEI BERUFSGEHEIMNISTRÄGERN AUSREICHEND +++

Das VG Mainz hat festgestellt, dass die Nutzung einer obligatorischen Transportverschlüsselung (SSL/TLS) für den Versand einer E-Mail, die personenbezogene Daten enthält, grundsätzlich ein angemessenes Schutzniveau im Sinne von Art. 32 DSGVO herstellt. Dies gelte auch für Berufsgeheimnisträger, hier einen Rechtsanwalt. Beständen im Einzelfall besondere Anhaltspunkte für einen erhöhten Schutzbedarf, müssten aber zusätzliche Schutzmaßnahmen (etwa Ende-zu-Ende Verschlüsselung) ergriffen werden. Dies betreffe insbesondere den Versand von besonderen Kategorien personenbezogener Daten (Art. 9 DSGVO) oder Daten über strafrechtliche Verurteilungen und Straftaten (Art. 10 DSGVO).

[Zum Urteil des VG Mainz \(v. 17. Dezember 2020, Az 1 K 778/19.MZ\)](#)

### +++ OVG LÜNEBURG: VERÖFFENTLICHUNG VON FOTOS AUF FACEBOOK-FANPAGE EINER PARTEI RECHTSWIDRIG +++

Das Oberverwaltungsgericht Lüneburg hat festgestellt, dass die Veröffentlichung eines Fotos mit identifizierbaren Personen auf der Facebook-Fanpage einer Partei ohne deren Einwilligung nicht zulässig war. Zwar habe die Partei ein berechtigtes Interesse daran zu dokumentieren, dass eine größere Anzahl von Personen an ihren Themen politisch interessiert sei. Die Darstellung von identifizierbaren Personen sei aber nicht erforderlich gewesen. Es hätte vielmehr ausgereicht, ein anonymisiertes Foto (z. B. mit verpixelten Gesichtern) zu veröffentlichen. Nach Auffassung des Gerichts ist die Veröffentlichung von Fotos in sozialen Netzwerken aufgrund der großen Reichweite mit erheblichen Risiken verbunden.

[Zum Beschluss \(v. 19. Januar 2021, Az. 11La 16/20\)](#)

## 3. Behördliche Maßnahmen

### +++ „TASK FORCE“ DER DATENSCHUTZBEHÖRDEN WILL NUTZUNG VON US-CLOUD-DIENSTEN DURCH DEUTSCHE UNTERNEHMEN PRÜFEN +++

Verschiedene Datenschutzbehörden der Länder beteiligen sich laut Presseberichten an einer neu gebildeten „Task Force“, die den Transfer von personenbezogenen Nutzerdaten in Drittstaaten durch deutsche Unternehmen überprüfen soll. Ein solcher Transfer findet insbesondere bei der Nutzung von Cloud-Diensten von US-Anbietern statt. Die Task Force soll von den Datenschutzbehörden Hamburg und Berlin geleitet werden. Der Transfer von personenbezogenen Daten in die USA ist seit dem Wegfall des

sog. EU-US Privacy Shields (Europäischer Gerichtshof, Urteil vom 16. Juli 2020, Az. C-311/18 – „Schrems-II“, siehe [BB Datenschutz-Ticker von Juli 2020](#)) mit erheblichen Rechtsunsicherheiten verbunden. Auf Anfrage des Nachrichtenportals Golem.de teilte der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit Johannes Caspar mit, die Task Force verfolge das Ziel, die Anforderungen des Schrems-II Urteils „zu vollziehen“. Es sollen bundesweit stichprobenartig Unternehmen kontrolliert werden, bei denen der Verdacht bestehe, dass diese Dienstleister aus Drittstaaten verwendeten.

[Zu dem Bericht auf Golem.de](#)

[Zu dem Artikel im Handelsblatt \(Paywall\)](#)

### +++ NORWEGISCHE DATENSCHUTZBEHÖRDE KÜNDIGT MILLIONEN-BUßGELD GEGEN BETREIBER DER APP „GRINDR“ AN +++

Die norwegische Datenschutzbehörde (Datatilsynet) hat angekündigt, gegen den Betreiber der Dating-App „Grindr“ ein Bußgeld in Höhe von fast EUR 10 Mio. zu erlassen. Die Behörde bemängelt, dass Grindr Daten an Werbenetzwerke weitergebe, ohne hierfür eine wirksame Einwilligung der Nutzer eingeholt zu haben. Dies soll auch sensible Daten zur sexuellen Orientierung der Nutzer umfassen. In der Vorabinformation führt die Behörde detailliert auf, warum die in Grindr eingeholte Einwilligung nicht den Vorgaben der DSGVO entspreche.

[Zur Vorabinformation zum Bußgeld \(englisch\)](#)

### +++ BUßGELDER IN HÖHE VON EUR 250.000 BZW. EUR 260.000 WEGEN UNERLAUBTER TELEFONWERBUNG +++

Die Bundesnetzagentur (BNetzA) hat zwei hohe Bußgelder wegen unrechtmäßig durchgeführter Werbeanrufe in hunderten Fällen festgesetzt. Gegen den Energieversorger mivolta GmbH wurde ein Bußgeld in Höhe von EUR 250.000 verhängt, weil Einwilligungen in Werbeanrufe nicht ordnungsgemäß eingeholt worden seien. Bemängelt wurde u. a., dass die Einwilligungserklärungen intransparent waren und mitunter in Zusammenhang mit einem Online-Gewinnspiel eingeholt wurden. In einem weiteren Fall hat die BNetzA ein Bußgeld in Höhe von EUR 260.000 gegen das Call-Center KiKxxl GmbH verhängt. Auch hier seien „gravierende Mängel bei der Prüfung von Werbeeinwilligungen“ ermittelt worden.

[Zur Pressemitteilung der Bundesnetzagentur \(v. 11. Februar 2021 bzgl. mivolta GmbH\)](#)

[Zur Pressemitteilung der Bundesnetzagentur \(v. 17. Februar 2021 bzgl. KiKxxl GmbH\)](#)

### +++ BUßGELDVERFAHREN GEGEN VfB STUTTGART ERÖFFNET +++

Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg (LfDI) hat Bußgeldverfahren gegen den VfB Stuttgart 1893 e.V. und die VfB Stuttgart 1893 AG eröffnet. Der LfDI sieht hinreichende tatsächliche Anhaltspunkte für Datenschutz-Verstöße in Zusammenhang mit einer Mitgliederversammlung im Jahr 2017 und einzelnen Datentransfers an einen externen Dienstleister im Jahr 2018. Daneben bestünden auch Fragen zur Umsetzung der aktuellen Rechtslage unter DSGVO. Vorausgegangen war ein mehrere Monate andauerndes Prüfverfahren zur Klärung des Sachverhalts.

[Zur Pressemitteilung des LfDI](#)

## 4. Stellungnahmen

### +++ EDSA VERÖFFENTLICHT BEISPIELE ZU MELDEPFLICHTIGEN SICHERHEITSVORFÄLLEN +++

Der Europäische Datenschutzausschuss (EDSA) hat Leitlinien mit 18 Fallbeispielen aus der Praxis zum Umgang mit Verletzungen der Datensicherheit veröffentlicht. Der EDSA stellt jeweils dar, welche präventiven Maßnahmen vor dem jeweiligen Sicherheitsvorfall geschützt hätten, welche Faktoren nach Eintritt des Sicherheitsvorfalls bei der Risikoabwägung zu berücksichtigen sind, welche Maßnahmen der Verantwortliche ergreifen muss, um die Risiken für Betroffene zu reduzieren, und ob eine gesetzliche Meldepflicht besteht.

[Zu den Leitlinien des EDSA \(englisch\)](#)

### +++ BlnBDI: AKTUALISIERTE HINWEISE ZU ANBIETERN VON VIDEOKONFERENZDIENSTEN +++

Die Berliner Beauftragte für Datenschutz und Informationsfreiheit (BlnBDI) hat verschiedene Anbieter von Videokonferenzdiensten einer Kurzprüfung unterzogen und die Hinweise zu datenschutzgerechten Videokonferenzdiensten aktualisiert. Die BlnBDI untersuchte die Rechtskonformität der von Anbietern bereitgestellten Auftragsverarbeitungsverträge und (oberflächlich) die technischen Eigenschaften der Videokonferenzdienste. Ein Schwerpunkt lag dabei auf der Prüfung, ob ein Dienst Daten in Drittländer exportiert. Die Hinweise könnten eine Hilfestellung für Verantwortliche bei der Auswahl eines sicheren Videokonferenzsystems darstellen. Sie ersetzen die Prüfpflichten des Verantwortlichen allerdings nicht. Die Hinweise werden durch die BlnBDI laufend aktualisiert.

[Zu den Hinweisen zu datenschutzgerechten Videokonferenzdiensten](#)

Für Rückfragen sprechen Sie den BEITEN BURKHARDT Anwalt Ihres Vertrauens an oder wenden Sie sich direkt an das BEITEN BURKHARDT Datenschutz-Team:

## MÜNCHEN



### Dr. Axel von Walter

Rechtsanwalt | CIPP/E | CIPM  
 Fachanwalt für Urheber- und Medienrecht  
 Fachanwalt für Informationstechnologierecht  
 Axel.Walter@bblaw.com  
 Tel.: +49 89 35065-1321



### Laureen Lee

Rechtsanwältin | LL.M.  
 Laureen.Lee@bblaw.com  
 Tel.: +49 89 35065-1307



### Gudrun Hausner

Rechtsanwältin  
 Gudrun.Hausner@bblaw.com  
 Tel.: +49 89 35065-1307

## FRANKFURT AM MAIN



### Dr. Andreas Lober

Rechtsanwalt  
 Andreas.Lober@bblaw.com  
 Tel.: +49 69 756095-582



### Susanne Klein

Rechtsanwältin | LL.M.  
 Fachanwältin für Informations-  
 technologierecht  
 Susanne.Klein@bblaw.com  
 Tel.: +49 69 756095-582



### Lennart Kriebel

Rechtsanwalt  
 Lennart.Kriebel@bblaw.com  
 Tel.: +49 69 756095-477

## DÜSSELDORF



### Mathias Zimmer-Goertz

Rechtsanwalt  
 Mathias.Zimmer-Goertz@bblaw.com  
 Tel.: +49 211 518989-144



### Christian Frederik Döpke

Rechtsanwalt | LL.M. | LL.M.  
 Christian.Doepke@bblaw.com  
 Tel.: +49 211 518989-144

## Impressum

### BEITEN BURKHARDT

Rechtsanwaltsgesellschaft 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/hinweise/impressum>

### REDAKTION (VERANTWORTLICH)

Dr. Andreas Lober | Rechtsanwalt | Partner

© BEITEN BURKHARDT Rechtsanwaltsgesellschaft mbH.  
 Alle Rechte vorbehalten 2021.

### HINWEISE

Diese Veröffentlichung stellt keine Rechtsberatung dar.  
 Wenn Sie diesen Newsticker nicht mehr erhalten möchten,  
 können Sie jederzeit per E-Mail (bitte E-Mail mit Betreff  
 „Abbestellen“ an [newsletter@bblaw.com](mailto:newsletter@bblaw.com)) oder sonst  
 gegenüber BEITEN BURKHARDT widersprechen.