LOSCHELDER

# Newsletter Datenschutzrecht
# November 2021

Sehr geehrte Damen und Herren,

auch in diesem Monat gibt es wieder spannende Themen mit Datenschutzfokus: Der Europäische Datenschutzausschuss äußert sich zum Drittstaatentransfer, das BAG legt dem EuGH wesentliche Fragen zu den Erlaubnisgrundlagen bei der Verarbeitung sensibler Daten vor und das LG Mainz spricht einem Betroffenen immateriellen Schadensersatz wegen einer zu frühen SCHUFA-Meldung zu.

In Sachen Cookies wird es auch wieder spannend: Ab dem 1. Dezember gelten neue Regelungen. Einen Überblick haben wir für die LTO erstellt, er ist hier abrufbar: Neues Datenschutzrecht: Cookie-Banner vor dem Aus? (lto.de). Mit der Frage, wer die Einhaltung der neuen Regelungen kontrolliert, beschäftigt sich unser vierter Beitrag.

Und für alle Leserinnen und Leser, die sich mit der Gestaltung von Websites und anderen Online-Angeboten beschäftigen und weitere Informationen zu den neuen Regeln suchen, ein Hinweis auf unser Webinar zu den neuen Rechtsvorgaben:

### *Verschwinden jetzt die Cookie-Banner? Neue Rechtsvorgaben für Websites & Co.*

Zum 1. Dezember tritt das Telekommunikation-Telemedien-Datenschutzgesetz - kurz TTDSG - in Kraft. Damit kommen wieder neue Regelungen für den rechtskonformen Websitebetrieb: Wann dürfen Cookies & Tags ohne Einwilligung gesetzt werden? Und ersetzen bald Einwilligungsverwaltungssysteme die Cookie-Banner auf jeder Website? Wir geben einen Überblick über das neue Recht und die Risiken im Fall von Verstößen.

**Mittwoch, den 08.12.2021: 12.00 bis 12.30 Uhr**
Dr. Kristina Schreiber / Dr. Malte Göbel

Gerne können Sie sich zu dem kostenfreien Webinar anmelden unter webinare@loschelder.de

.

**Inhalt**

## Neues zum Drittstaatentransfer

*Wann dürfen US-Dienstleister datenschutzkonform genutzt werden? Was gilt es zu beachten, um das Datenschutzrisiko beim Transfer von Daten in Länder außerhalb des EWR zu minimieren? Seit der EuGH-Entscheidung in Sachen Schrems II sind diese Fragen ein (leidiger) Dauerbrenner. Vor wenigen Tagen hat der Europäische Datenschutzausschuss neue Leitlinien hierzu erlassen. Wir haben das Wichtigste daraus für Sie zusammengefasst.*

Die Leitlinien 05/2021 des Europäischen Datenschutzausschusses (EDSA), die am 18.11.2021 angenommen wurden, befassen sich mit dem „Zusammenspiel zwischen der Anwendung von Artikel 3 und den Bestimmungen über internationale Übermittlungen gemäß Kapitel V der DSGVO". Ein sperriger Titel für eine höchst praxisrelevante Thematik:

Wann ist überhaupt von einem „Drittstaatentransfer" von Daten auszugehen? Ist dies nur dann der Fall, wenn personenbezogene Daten physisch auf Servern in Ländern außerhalb des Europäischen Wirtschaftsraums (EWR) gespeichert werden? Oder reichen bereits Support-Zugriffe etwa aus den USA heraus, wie dies jedenfalls auf 3. Ebene bei Microsoft, AWS und vielen mehr der Regelfall ist? Ist womöglich bereits dann von einem Drittstaatentransfer im Sinne der DSGVO auszugehen, wenn Daten auf Servern im EWR gespeichert sind, diese Daten aber z.B. von US-Unternehmen oder ihren EU-Töchtern kontrolliert werden (dann gibt es u.U. Zugriffsrechte der US-Behörden unter dem CLOUD ACT)?

Diese in der Praxis hoch relevanten und umstrittenen Fragen diskutiert der EDSA in seinen Leitlinien. Diese sind nicht verbindlich – weder für nationale Datenschutzaufsichtsbehörden noch für Unternehmen. Sie geben aber wertvolle Anhaltspunkte, wie hoch das Risiko eines aufsichtsbehördlichen Einschreitens ist und mindern so die bestehenden Rechtsunsicherheiten.

**Kriterien für das Vorliegen eines Drittstaatentransfers**

Der EDSA definiert drei Kriterien, bei deren kumulativem Vorliegen von einem Drittstaatentransfer von Daten auszugehen ist. In diesem Fall müssen die Vorgaben der Art. 44 ff. DSGVO eingehalten werden:

1. Ein Unternehmen verarbeitet personenbezogene Daten im Anwendungsbereich der DSGVO.

2. Dieses Unternehmen macht die personenbezogenen Daten einem anderen Unternehmen zugänglich, durch Übermittlung oder auf andere Weise.

3. Das andere Unternehmen befindet sich in einem Drittland oder ist eine internationale Organisation.

Diese Kriterien sind denkbar weit: Anders als der Begriff „Drittstaatentransfer" vermuten lässt, müssen Daten nicht notwendigerweise in ein Drittland geschickt werden. Es reicht vielmehr, wenn die Daten auf Servern im EWR gespeichert bleiben und ein Unternehmen aus dem Drittland diese dort „ansehen" kann. Diese Position wird nicht nur vom EDSA, sondern, soweit ersichtlich, auch von der überwiegenden Literatur so vertreten.

Für die Praxis bedeutet das, dass alle der folgenden Optionen einen „Drittstaatentransfer" im Sinne der DSGVO darstellen und damit für jede der folgenden Situationen angemessene Garantien für die Absicherung der Datenverarbeitung im Drittland vorgesehen werden müssen:

- **Versand** in Drittländer
- **Supportzugriffe** aus Drittländern
- **Behördenzugriffe** aus Drittländern

All das gilt auch dann, wenn nur der Auftragnehmer in der EU ansässig ist und hier – z.B. als IT-Dienstleister oder Tochterunternehmen eines US-Konzerns – personenbezogene Daten im Auftrag verarbeitet. Für den „Rückversand" der personenbezogenen Daten vom **Auftragnehmer** an den Verantwortlichen gelten die Anforderungen der Art. 44 ff. DSGVO.

Ein abzusichernder Drittstaatentransfer liegt natürlich nur dann vor, wenn Daten übertragen werden, nicht, wenn dies nur theoretisch denkbar ist. Bei Supportzugriffen sollte aber regelmäßig schon vorab und nicht erst im Supportfall eine Absicherung für den Drittstaatentransfer geschaffen werden: Wenn Hilfe benötigt wird, bleibt regelmäßig keine Zeit mehr, um die entsprechenden Absicherungen zu schaffen. Bei Behördenzugriffen aus Drittländern kann dies anders sein, je nach nationalem Recht und – jedenfalls bei Akzeptanz eines risikobasierten Ansatzes, wie dieser aus den neuen Standardvertragsklauseln ersichtlich ist – der Antwort auf die Frage, ob auch praktisch mit solchen Zugriffen zu rechnen ist.

Ein Drittstaatentransfer liegt nicht vor, wenn EU-Bürger ihre Daten direkt an ein Unternehmen übermitteln, das nicht dem Anwendungsbereich der DSGVO unterliegt, beispielsweise bei einer **direkten Bestellung** von Kleidung bei einem Unternehmen in Singapur, welches zwar eine Website in englischer Sprache unterhält, aber weder eine Niederlassung in der EU hat noch seine Kollektion gezielt EU-Bürgern anbietet.

Nicht erfasst sind nach einem Beispiel des EDSA auch **Remote-Work-Zugriffe**: Wenn der Arbeitnehmer eines deutschen Unternehmens auf einer Dienstreise aus Indien heraus auf den Unternehmensserver zugreift und personenbezogene Daten verarbeitet, ist dies kein Datentransfer nach Indien und die Vorgaben der Art. 44 ff. DSGVO müssen nicht eingehalten werden.

**Folgen des Vorliegens eines Drittstaatentransfers**

Werden Daten in Drittstaaten übertragen, muss der Datentransfer durch angemessene Garantien abgesichert werden. Angemessene Garantien können etwa ein Angemessenheitsbeschluss der EU-Kommission sein (z.B. für UK oder Kanada), die Vereinbarung der (neuen) Standardvertragsklauseln mit Prüfung der Rechtslage im Zielstaat und etwaigen zusätzlichen Maßnahmen. Bei unternehmensinternen Transfers können auch Binding Corporate Rules die Datenflüsse absichern.

Grundvoraussetzung für eine DSGVO-konforme Datenverarbeitung ist indes stets, die Verarbeitungsprozesse im Unternehmen zu kennen. Dies gilt auch und gerade für Drittstaatentransfers. Dokumentiert werden können die Transfers etwa im Kontext der Verarbeitungsverzeichnisse. Die Datenschutzaufsichtsbehörden erwarten dies spätestens seit dem EuGH-Schrems II-Urteil im Sommer 2020. In der Bundesrepublik wird seit Juni 2021 eine von mehreren Landesdatenschutzbehörden abgestimmte Schwerpunktprüfung der Drittstaatentransfers ausgewählter Unternehmen durchgeführt. Wir berichteten hierzu in unserem Newsletter vom Juni 2021.

## Höchstrichterliche Rechtsprechung zur Verarbeitung von Gesundheitsdaten

*Auch über drei Jahre nach Inkrafttreten der DSGVO ist die Zahl der Rechtsprechung zu vielen Detailfragen des Datenschutzrechts überschaubar. Wer in seiner täglichen Arbeit mit Fragen des Datenschutzrechts befasst ist, muss sich regelmäßig auf Stellungnahmen von Behörden oder aus der Literatur verlassen – dies bringt Rechtsunsicherheit mit sich. Etwas mehr Klarheit könnte hier eine aktuelle Vorlage des BAG an den EuGH bringen, in der sich das BAG mit der Auslegung der Erlaubnisnormen zur Verarbeitung von Gesundheitsdaten beschäftigt. Die von dem Gericht eingenommenen Positionen und mögliche Auswirkungen auf die Praxis fassen wir nachfolgend für Sie zusammen und zeigen auf, wo das Verfahren gerade auch außerhalb des Beschäftigtendatenschutzes Relevanz hat: Bei der Verarbeitung von Gesundheitsdaten durch Ärzte, DiGAS oder andere digitale Gesundheitsanwendungen.*

In dem vor dem BAG verhandelten Fall (Beschluss vom 26.08.2021, Az. 8 AZR 253/20) ging es – kurz zusammengefasst – um einen Mitarbeiter des Medizinischen Dienstes einer Krankenkasse, der aufgrund einer psychischen Erkrankung langfristig arbeitsunfähig war. Die Erkrankung dauerte mehrere Monate an, sodass die Krankenkasse des Erkrankten zur Zahlung von Krankengeld verpflichtet war. Diese gab daraufhin bei ihrem Medizinischen Dienst, bei dem der Erkrankte beschäftigt war, ein Gutachten in

Auftrag, in dem festgestellt werden sollte, ob die behauptete Krankheit tatsächlich vorlag oder vorgetäuscht war. Nach Erstellung des Gutachtens verlangte der Betroffene eine Entschädigung i.H.v. 20.000 EURO von seinem Arbeitgeber, also dem Medizinischen Dienst der Krankenkasse, weil er der Auffassung war, dass für die Verarbeitung seiner personenbezogenen (Gesundheits-)Daten keine Rechtsgrundlage bestanden habe.

Das BAG hat den Fall zunächst nicht entschieden, sondern dem EuGH Fragen zur Auslegung der DSGVO vorgelegt. Die Positionen, die das BAG dabei einnimmt, gehen in ihrer Bedeutung weit über den konkreten Fall hinaus und könnten Klarheit auch für andere Fragen bei der Verarbeitung von besonderen Kategorien personenbezogener Daten, insbesondere im Gesundheitssektor durch Gesundheitsprodukte und -dienstleistungen, bringen.

**Auslegung von Art. 9 Abs. 2 DSGVO**

In der ersten Frage des BAG geht es um das Verhältnis von zwei Erlaubnisgrundlagen zur Verarbeitung von Gesundheitsdaten (Art. 9 Abs. 2 lit. b und lit. h DSGVO). Die erste (lit. b) gibt Arbeitgebern das Recht, Gesundheitsdaten von Arbeitnehmern zu verarbeiten, wenn sie rechtlich zu der Verarbeitung verpflichtet sind. Die Norm erfasst die wenigen Fälle, in denen ein Arbeitgeber (den dieser Bereich üblicherweise nichts angeht) Informationen über die Gesundheit eines Arbeitnehmers erfahren darf/muss. Ein triviales Beispiel dafür ist etwa die Krankmeldung eines Arbeitnehmers oder die Verarbeitung von Informationen zur Tauglichkeit bei Berufen mit besonderen Anforderungen.

Keinesfalls muss ein Arbeitgeber allerdings Informationen über die genaue Krankheit eines Arbeitnehmers, die zur Arbeitsunfähigkeit führt, erhalten – hier bleibt es bei der Information, dass eine Krankheit besteht, die die Arbeitsunfähigkeit begründet. Daher erfährt er regelmäßig nichts über den genauen Inhalt eines Gutachtens über den Gesundheitszustand eines Arbeitnehmers, sondern allenfalls dessen Ergebnis (krank oder nicht krank, arbeitsunfähig oder arbeitsfähig).

Informationen zur konkreten Krankheit des Arbeitnehmers dürfen dagegen auf der Grundlage von Art. 9 Abs. 2 lit. h) DSGVO verarbeitet werden, etwa von Ärzten. Nach dieser Erlaubnisgrundlage dürfen Gesundheitsdaten zur Beurteilung der

Arbeitsfähigkeit eines Beschäftigten verarbeitet werden, durch unabhängige Dritte, die als Angehörige von Gesundheitsberufen besonderen Verschwiegenheitspflichten unterliegen. Dies umfasst etwa auch die Erstellung von Gutachten über den Gesundheitszustand von Versicherten durch den Medizinischen Dienst einer Krankenkasse. Normalerweise sind solche Begutachtungen zulässig. Problematisch wird es allerdings, wenn der Versicherte – wie im vorliegenden Fall – gleichzeitig Arbeitnehmer des Medizinischen Dienstes der Krankenkasse ist. Das BAG fragt hierzu den EuGH, ob in diesem Fall nicht die an sich zulässige Erstellung des Gutachtens unzulässig sei, da der Arbeitgeber nach Art. 9 Abs. 2 lit. b) DSGVO nicht berechtigt wäre, ein Gutachten zu erstellen. Das BAG fragt also, ob Art. 9 Abs. 2 lit. b) DSGVO für einen Arbeitgeber Sperrwirkung entfaltet, sodass dieser weitere Rechtsgrundlagen des Art. 9 Abs. 2 DSGVO nicht mehr nutzen darf.

Diese Position des BAG lässt sich auf andere Fälle übertragen und könnte so weitreichende Folgen haben: Werden z.B. Ärzte in der Verarbeitung der Gesundheitsdaten ihrer Mitarbeiter beschränkt, wenn sich diese in der eigenen Praxis behandeln lassen? Wie sieht das bei DiGAs (ausgewählte Gesundheitsanwendungen für Patienten) und anderen digitalen Gesundheitsanwendungen aus: Müssen Anbieter ihre eigenen Mitarbeiter von der Verwendung dieser Tools ausschließen? Wie sieht es mit anderen Kombinationen von Erlaubnistatbeständen des Art. 9 Abs. 2 DSGVO aus?

**Zusätzliche Maßnahmen zur Datensicherheit**

Oder reichen interne „Chinese Walls“, die sicherstellen, dass die jeweiligen Kenntnisse nicht für das Arbeitsverhältnis selbst verwendet werden? Auf diese Thematik zielt die zweite Frage des BAG: Falls die Erstellung des Gutachtens zulässig war, hätten dann nicht zusätzliche Maßnahmen zur Geheimhaltung des Gutachtens vor Personen, mit denen der Betroffene Kontakt hatte, ergriffen werden müssen? Das BAG führt hierzu aus, dass es nicht ausreichen könne, dass an dem Gesundheitsgutachten nur beruflich zur Verschwiegenheit Verpflichtete mitwirken (so die Vorgabe aus Art. 9 Abs. 3 DSGVO) und HR-Mitarbeiter keinen Zugang zu den Informationen erhalten dürfen (so die Regelung zu Sozialdaten aus § 35 Abs. 1 S. 3 SGB I). Vielmehr, so das BAG, hätte der Arbeitgeber zum Schutz des Betroffenen sicherstellen müssen, dass keine Person, die mit dem Betroffenen zu tun hatte, an der Erstellung des

Gutachtens mitwirken konnte oder berechtigt oder unberechtigt Zugriff auf das Gutachten hätte haben können.

Beantwortet der EuGH diese Frage so, dass besondere Vorkehrungen zum Schutz der Gesundheitsdaten des Betroffenen erforderlich gewesen wären, stellen sich wie oben Folgefragen bei der Nutzung von Gesundheitsprodukten oder -dienstleistungen. Müssen Arbeitgeber hier in Zukunft sicherstellen, dass Arbeitnehmerdaten nicht durch Kollegen wahrgenommen werden können? Aus der Beantwortung des EuGH zu dieser Frage ergeben sich womöglich auch weitergehende hilfreiche Hinweise darauf, wie besonders sensitive Daten technisch und organisatorisch geschützt werden müssen – eine in der Praxis höchst relevante Frage.

**Rechtsgrundlage nach Art. 9 und Art. 6 DSGVO erforderlich?**

Die größte Relevanz für die Praxis birgt die dritte, wiederum hypothetisch gestellte Frage des BAG. Diese betrifft das Verhältnis von Art. 6 und Art. 9 DSGVO. Grundsätzlich gilt hier: in Art. 9 Abs. 2 DSGVO werden die Rechtsgrundlagen für die Verarbeitung besonderer Kategorien personenbezogener Daten (Gesundheitsdaten, Daten über religiöse und politische Auffassungen, über die sexuelle Orientierung etc.) aufgelistet. Art. 6 Abs. 1 DSGVO enthält dagegen Rechtsgrundlagen für die Verarbeitung aller anderen, weniger sensiblen Daten. Die Normen stehen nach bisher überwiegender Ansicht unabhängig nebeneinander, wer von einer Rechtsgrundlage aus Art. 9 Abs. 2 DSGVO Gebrauch macht, braucht Art. 6 Abs. 1 DSGVO nicht zu beachten und umgekehrt.

Das BAG hat dem EuGH nunmehr die Frage vorgelegt, ob die Verarbeitung von Daten auf der Grundlage von Art. 9 Abs. 2 DSGVO zusätzlich voraussetzt, dass auch eine Rechtsgrundlage nach Art. 6 Abs. 1 DSGVO vorliegt. Dazu führt das BAG aus, dass – allerdings bei einer ziemlich konservativen Auslegung der Rechtsgrundlagen des Art. 6 Abs. 1 DSGVO – im zu entscheidenden Fall die Voraussetzungen des Art. 6 Abs. 1 DSGVO nicht erfüllt gewesen seien.

Sollte sich das BAG in dieser Frage mit seinem Verständnis durchsetzen, hätte das weitreichenden Einfluss auf die Auslegung und Handhabung der DSGVO in der Praxis. Liegt eine Rechtsgrundlage nach Art. 9 Abs. 2 DSGVO vor, war bisher

regelmäßig keine weitere Rechtsgrundlage nach Art. 6 Abs. 1 DSGVO für die Verarbeitung von Daten erforderlich. Bei einer entsprechenden Veränderung müssten etliche Verarbeitungsprozesse neu geprüft und bewertet werden: Liegt auch eine Erlaubnisgrundlage nach Art. 6 DSGVO vor? Müssen zusätzliche Dokumentationen erstellt werden? Sind die Informationen der Betroffenen (resp. die Datenschutzerklärungen) anzupassen? Fehlt eine Rechtsgrundlage nach einer der Normen, müssten die Datenverarbeitungen beendet werden.

**Fazit**

Das BAG hat dem EuGH relativ weitreichende Fragen zur Auslegung von Art. 9 Abs. 2 DSGVO vorgelegt. Der EuGH hat damit nun Gelegenheit, zu einigen grundsätzlichen Fragen in Bezug auf die Auslegung der DSGVO Stellung zu nehmen und damit ein Mehr an Rechtsklarheit und Rechtssicherheit zu schaffen.

Auch wenn das Verfahren primär den Beschäftigtendatenschutz betrifft, so wird sich die Entscheidung voraussichtlich weit darüber hinaus auswirken und auch Verarbeitungsprozesse beeinflussen, die außerhalb des Beschäftigtenverhältnisses sensitive Daten betreffen. Wir informieren Sie selbstverständlich, sobald Antworten aus Luxemburg eintreffen.

## Schadensersatz wegen SCHUFA-Eintrag

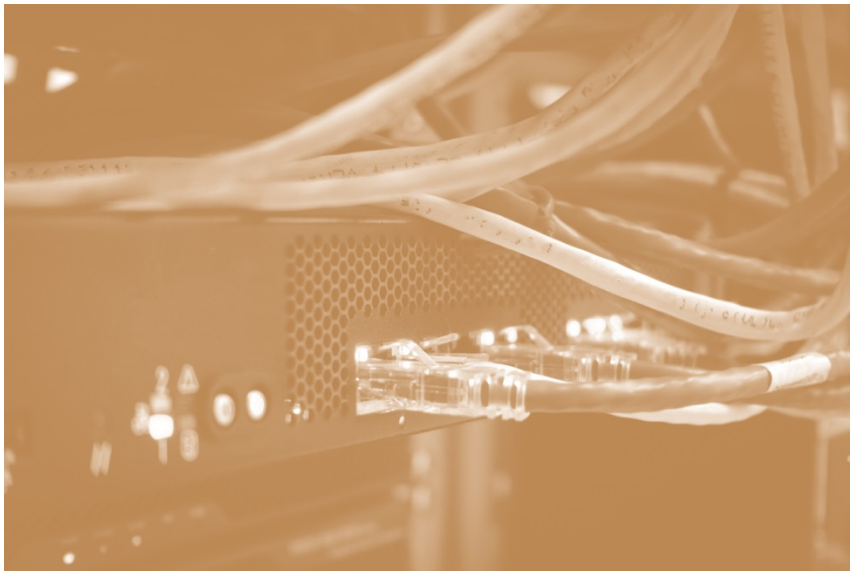
*Unternehmen, die an die SCHUFA Meldungen abgeben, müssen auf die Richtigkeit der Meldung sorgsam achten. Dabei kommt es nicht nur auf den Wahrheitsgehalt an, sondern auch auf die Einhaltung der „Meldevoraussetzungen" in § 31 BDSG. Wer zu früh meldet, kann sich schadensersatzpflichtig machen – im konkreten Fall wurden dem Betroffenen 5.000 Euro zugesprochen, da die Meldung ohne vorherige Androhung erfolgte. Das Urteil ist ein weiterer Mosaikstein: Zivilrechtliche Schadensersatzklagen wegen Datenschutzverletzungen nehmen zu, und zwar sowohl hinsichtlich der Anzahl als auch hinsichtlich der Höhe der geltend gemachten (und hier zugesprochenen) immateriellen Schadenspositionen.*

In einem kürzlich erlassenen Urteil des LG Mainz vom 12.11.2021, Az. 3 O 12/20, wurden dem Kläger für eine „zu frühe" Negativ-Meldung ohne vorherige Androhung 5.000 Euro Schadensersatz zugesprochen. Das beklagte Unternehmen hatte eine Forderung als gegen den Kläger tituliert an die SCHUFA gemeldet und damit ein relevantes Ausfallrisiko für die betreffenden Personen kommuniziert. Eine solche Datenübermittlung des Unternehmens an die SCHUFA kann, so das Gericht, dem Grunde nach aus berechtigten Interessen gem. Art. 6 Abs. 1 UAbs. 1 lit. f) DSGVO erlaubt sein. Im konkreten Fall fehlte es aber an einer solchen Verarbeitungserlaubnis. Die Datenübermittlung war damit rechtswidrig, weil der Kläger nicht hinreichend gewarnt worden ist, dass seine Daten und die ausgebliebene Zahlung an die SCHUFA gemeldet werden. Weitere strittige Fragen im Fall, so etwa, ob das Unternehmen eine hinreichende Karenzfrist zwischen der Titulierung seiner Forderung und der Meldung an die SCHUFA eingehalten hat, konnten daher dahinstehen.

Das Gericht zog für die Ermittlung der Voraussetzungen einer Meldung an die SCHUFA § 31 BDSG heran. Es ließ dabei dahinstehen, ob diese Norm überhaupt anwendbar ist oder aber dem EU-Recht weichen muss (es ist umstritten, ob die DSGVO den Mitgliedsstaaten eine solche Regelung, wie sie § 31 BDSG enthält, erlaubt). Denn auch bei einer Interessenabwägung unter Art. 6 Abs. 1 UAbs. 1 lit. f) DSGVO wäre das Gericht zum selben Ergebnis gekommen.

Die SCHUFA als solche steht auch noch unter einem anderen Blickwinkel im datenschutzrechtlichen Fokus: Das VG Wiesbaden verpflichtete Ende September (Urteil vom 27.09.2021, Az. 6 K 549/21) den Hessischen Beauftragten für Datenschutz und Informationsfreiheit zu einem Einschreiten gegenüber der SCHUFA. Die hessische Datenschutzaufsichtsbehörde hatte dies abgelehnt, nachdem sich ein Betroffener an sie gewandt hatte, um die Löschung eines Negativ-Eintrags zu erwirken. Das VG Wiesbaden hielt fest, dass ein Betroffener im Wege der Verpflichtungsklage erzwingen kann, dass die Aufsichtsbehörde tätig wird. Und auch in der Sache kam das VG Wiesbaden zu einer Pflicht des Einschreitens der Aufsichtsbehörde, da vorliegend erhebliche Gründe für eine Löschpflicht der SCHUFA bestanden. Auch in diesem Verfahren ging es um womöglich rechtswidrige Meldungen von Zahlungsaufforderungen, die von Inkasso-Dienstleistern ohne Auftrag der ursprünglichen Forderungsinhaber getätigt worden waren. Vorliegend war die Fallgestaltung auch deshalb so eindeutig, weil die als ausgefallen gemeldete Forderung gerichtlich im Streit stand und das Gerichtsverfahren durch einen Vergleich abgeschlossen wurde.

Für die Praxis auch jenseits der Wirtschaftsauskunfteien sind beide Entscheidungen von Relevanz: Zum einen verdeutlichen sie, dass die Bedeutung von Schadensersatzforderungen aufgrund von DSGVO-Verstößen zunehmend wächst. Die vom LG Mainz zugesprochenen 5.000 Euro Schadensersatz begleichen keinen dem Kläger tatsächlich entstandenen Nachteil, sondern sind ein Schmerzensgeld für die Unannehmlichkeiten, die er erlitten hat. Das Urteil des VG Wiesbaden zeigt schließlich, dass Datenschutzaufsichtsbehörden von Betroffenen auch zu einem Einschreiten gezwungen werden können. Es gelten hier die allgemeinen verwaltungsrechtlichen Grundsätze, auch wenn diese bei den Tätigkeiten der Aufsichtsbehörde bisweilen eher vernachlässigt werden.



## Wer kontrolliert die Cookie-Regeln?

*Wenn Unternehmen auf ihren Webseiten, Plattformen oder anderen Online-Angeboten Cookies oder andere PlugIns nutzen, um ihre Nutzer zu erreichen, gilt das ePrivacy-Recht. Verstöße gegen das ePrivacy-Recht sind weniger streng geahndet als Datenschutzverstöße, es gibt keine vergleichbaren Bußgelder. Das ändert sich ab dem 1. Dezember. Aber welche Behörde setzt die Cookie-Regeln dann gegenüber den Unternehmen durch und verhängt Bußgelder?*

Zur Erinnerung: Das ePrivacy-Recht gilt ganz unabhängig davon, ob personenbezogene Daten verarbeitet werden. Verstöße gegen das ePrivacy-Recht sind bislang insbesondere durch Wettbewerber im Wege von Abmahnungen geltend gemacht worden. Bußgeldrisiken, wie wir sie aus dem Datenschutzrecht kennen, gab es nicht. Dies ändert sich mit Inkrafttreten des Telekommunikation-Telemedien-Datenschutzgesetzes (TTDSG) zum 1. Dezember. Ab dann können auch Verstöße gegen „Cookie-Regeln“ deutlich einfacher mit erhöhten Bußgeldern von bis zu 300.000 Euro belegt werden.

Aber: Welche Behörde ist hierfür zuständig? Und was gilt, wenn eine Webseite in vielen Ländern aktiv ist – greift dann die deutsche Behörde oder aber jene in Italien, den USA oder Australien ein?

**Cookie-Regeln**

Art. 5 Abs. 3 ePrivacy-Richtlinie bildet die rechtliche Grundlage für alle Endgerätezugriffe durch Online-Angebote, also z.B. Cookies, Nutzung des lokalen Speichers, finger printing und andere Tags und PlugIns. Alle solche Zugriffe auf die Endgeräte der Nutzer erfordern eine Einwilligung. Das Einwilligungserfordernis gilt unabhängig davon, ob personenbezogene Daten verarbeitet werden oder nicht. Eine Ausnahme vom Einwilligungserfordernis gilt nur dann, wenn die entsprechenden Tools unbedingt erforderlich sind, um den vom Nutzer angefragten Dienst auch bereitzustellen.

Bislang war Art. 5 Abs. 3 ePrivacy-Richtlinie in Deutschland nur suboptimal umgesetzt. Der unbefangene Leser konnte in der bisherigen Umsetzungsnorm § 15 Abs. 3 TMG kein Einwilligungserfordernis finden (dort war die Rede von „Widerspruch“). Dies war Anlass der Planet49-Entscheidung des EuGH (wir berichteten im Newsletter aus Oktober 2019 ausführlich) und der nachfolgenden BGH-Entscheidung im Mai 2020 (hierzu ausführlich in unserem Newsletter aus Juni 2020).

Ab dem 1. Dezember ist dies Geschichte und es gilt § 25 TTDSG: Dieser regelt dann klar – und beinahe wortgleich mit Art. 5 Abs. 3 ePrivacy-Richtlinie –, dass eine Einwilligung in der Regel erforderlich ist. Hält sich ein Unternehmen nicht an diese Vorgabe, ist dies eine Ordnungswidrigkeit, die mit einem Bußgeld von bis zu 300.000 Euro geahndet werden kann (§ 28 TTDSG).

**Komplexe Rechtslage in Deutschland**

Wer aber kontrolliert die Einhaltung der Cookie-Regeln des TTDSG und verhängt ein Bußgeld? Das TTDSG klärt dies nicht. Die Aufsichtszuständigkeiten für Einhaltung der Cookie-Regelungen im deutschen Recht bleiben damit komplex.

Die ePrivacy-RL gibt in ihren Art. 15 und Art. 17 nur vor, dass die Mitgliedsstaaten Vorschriften schaffen müssen, die die Aufsicht über die Einhaltung der Vorgaben der Richtlinie sowie rechtliche Konsequenzen bei Verstößen bestimmen. Regelungen, wann welche nationale Aufsichtsbehörde zuständig ist, enthält die ePrivacy-Richtlinie nicht, sodass jeder Mitgliedstaat eigene Bestimmungen über die Zuständigkeit treffen muss.

Im deutschen Recht fehlt es an einer ausdrücklichen Zuweisung der Aufsichtszuständigkeiten. Das TTDSG selbst regelt nur die Aufsicht über Telekommunikationsunternehmen, die sich BfDI und Bundesnetzagentur teilen (§§ 29, 30 TTDSG). Im Übrigen heißt es lapidar: „bei Telemedien bleiben die Aufsicht durch die nach Landesrecht zuständigen Behörden und § 40 Bundesdatenschutzgesetz unberührt“ (§ 1 Abs. 1 Nr. 8 TTDSG).

**Sind also die Datenschutzaufsichtsbehörden berufen, die Cookie-Regeln durchzusetzen?**

So klar ist das nicht: Die Zuständigkeit der Bundes- und Landesdatenschutzaufsichtsbehörden für die Einhaltung der DSGVO nach Art. 58 DSGVO kann nicht auf die Aufsicht über die Einhaltung der ePrivacy-RL übertragen werden – es handelt sich immerhin um zwei unterschiedliche Rechtsakte. Zudem muss auch zwischen der allgemeinen datenschutzrechtlichen Aufsicht über die Einhaltung der nationalen Umsetzungsvorschriften der ePrivacy-RL und der Zuständigkeit für die Verhängung von Bußgeldern und Sanktionen unterschieden werden sowie zwischen Telemedien und Telekommunikationsdiensten. Dabei gilt sowohl Bundes- wie auch Landesrecht und insofern sind 17 unterschiedliche Rechtsregime zu beachten. Das Fehlen eindeutiger gesetzlicher Vorschriften in Deutschland ist damit ein sehr praxisrelevantes Problem.

Zusammenfassen lässt sich die Gemengelage unter Berücksichtigung des ab dem 1. Dezember geltenden TTDSG wie folgt:

| **Neue Rechtslage (TTDSG)** | **Allgemeine Zuständigkeit** | **Zuständigkeit für Bußgelder** |
|---|---|---|
| **DSGVO** | Datenschutzaufsichtsbehörden (Art. 58 Abs. 1, 2 DSGVO) | Datenschutzaufsichtsbehörden (Art. 58 Abs. 2 lit. i), Art. 83 DSGVO) |
| **Cookie-Regeln (§ 25 TTDSG)** | Für Telemedien: ? | Für Telemedien: ? |
| **Telekommunikationsdienste** | BfDI (§ 29 Abs. 2 TTDSG) | BfDI (§ 28 Abs. 1 Nr. 13, Abs. 3 Nr. 2 TTDSG) |

**Allgemeine Aufsicht**

Die Einhaltung „allgemeiner Datenschutzbestimmungen“ durch Telemedienanbieter wird nach § 113 Satz 1 Medienstaatsvertrag (MStV) von den Datenschutzaufsichtsbehörden kontrolliert. Dabei bleibt es nach § 1 Abs. 1 Nr. 8 TTDSG, der zudem auf § 40 BDSG verweist.

Aber sind die Cookie-Regeln „allgemeine Datenschutzbestimmungen“? So klar ist dies nicht: Die Cookie-Regeln gelten unabhängig davon, ob personenbezogene Daten verarbeitet werden oder nicht. Der „Datenschutz“ aber gilt nur für personenbezogene Daten. Ob tatsächlich die Datenschutzaufsichtsbehörden auch dann zuständig sein sollen, wenn über Cookies und vergleichbare Technologien keine personenbezogenen Daten verarbeitet werden, kann berechtigterweise in Frage gestellt werden. Die Cookie-Regeln dienen schon ausweislich des Wortlauts des § 25 TTDSG dem „Schutz der Privatsphäre“. Dies ist nicht mit dem Datenschutz gleichzusetzen.

Für eine Einordnung als „Datenschutzbestimmungen“ spricht allerdings, dass es ansonsten zu einer Zersplitterung der Zuständigkeiten kommen könnte: Werden über Cookies & Co. personenbezogene Daten verarbeitet, wären die Datenschutzaufsichtsbehörden zuständig, ansonsten nicht. Dies ist kaum praktikabel.

Eindeutig geklärt ist diese Zuständigkeit indes nicht. Sie wird zu überprüfen sein – in der Praxis wohl spätestens dann, wenn eine Datenschutzaufsichtsbehörde ihre Zuständigkeiten unter Bezugnahme auf die Cookie-Regelungen ausübt, womöglich sogar in einem Anwendungsfall, der nicht mit der Verarbeitung personenbezogener Daten einhergeht.

Außen vor gelassen ist dabei die weitere Thematik, dass es nicht einfach ist, die landesrechtlich nach § 113 S. 1 MStV zuständige Behörde zu identifizieren: Greift nun § 40 BDSG über den Verweis in § 1 Abs. 1 Nr. 8 BDSG? Oder bedarf es weiterhin, wie auch bisher unter § 113 S. 1 MStV, einer Zuständigkeit nach den Landesgesetzen? Diese ist oft nicht gegeben. Eine Ausnahme bildet etwa Nordrhein-Westfalen: § 1 Abs. 2 S. 1 Telemedienzuständigkeitsgesetz NRW (TMZ-Gesetz NRW) bestimmt ausdrücklich, dass der

Landesbeauftragte für Datenschutz die nach § 113 S. 1 MStV zuständige Behörde ist.

Wenn Telekommunikationsdienste auf die Endgeräte ihrer Nutzer zugreifen, klärt das TTDSG die Zuständigkeit: Diese liegt gem. § 29 beim BfDI.

**Bußgelder**

So weit, so (un-)eindeutig. Noch komplexer wird es bei der Bestimmung der Zuständigkeiten für die Sanktionierung von Verstößen mit Bußgeldern. Die Erläuterung bedarf eines Blicks auf die Bußgeldtatbestände des TTDSG sowie in das Ordnungswidrigkeitengesetz (OWiG).

Nach § 28 TTDSG können Verstöße gegen die Cookie-Regeln bei Vorsatz oder Fahrlässigkeit mit Bußgeldern belegt werden (bis zu 300.000 Euro). Der Gesetzgeber kann die für die Verhängung dieser Sanktionen zuständige Verwaltungsbehörde nach § 36 Abs. 1 Nr. 1 OWiG ausdrücklich in einem Gesetz bestimmen. Im TTDSG selbst ist dies indes nur für Verstöße durch Telekommunikationsunternehmen erfolgt – dann ist der BfDI nach §§ 28 Abs. 3, 29 TTDSG zuständig.

Wer für die Verhängung von Bußgeldern wegen Cookie-Regelverstößen durch Telemedienanbieter (also etwa den Websitebetreiber) zuständig ist, bestimmt das TTDSG nicht.

Wenn es an einer ausdrücklichen Bestimmung der zuständigen Verwaltungsbehörde fehlt, ist auf § 36 Abs. 1 Nr. 2 lit. a OWiG zurückzugreifen, wonach bei Fehlen einer ausdrücklichen Bestimmung die oberste Landesbehörde zuständig ist. Dabei muss die Zuweisung der Zuständigkeit aber nicht in dem Gesetz erfolgen, in dem der Bußgeldtatbestand geregelt ist. Insbesondere können die Länder, soweit sie Bundesgesetze ausführen, in ihren Landesgesetzen regeln, wer die zuständige Vollzugsbehörde sein soll. Das stellt dann eine Zuständigkeitsbestimmung im Sinne des § 36 Abs. 1 Nr. 1 OWiG dar.

Für § 16 Abs. 2 TMG nahmen einige Länder diese Möglichkeit wahr und wiesen die Zuständigkeit ausdrücklich den Landesdatenschutzaufsichtsbehörden zu (so etwa für NRW in § 1 Abs. 3 Satz 3 Nr. 2 TMZ-Gesetz NRW).

Ob – fehlt es an einer solchen Zuweisung – auch die allgemeine Aufsichtszuständigkeit die Verhängung von Bußgeldern umfasst, ist dagegen höchst umstritten. Der Streit gilt jetzt auch für Länder wie NRW, da eine Zuweisung für § 28 TTDSG noch nicht erfolgt ist. Für einen Gleichlauf der Zuständigkeiten spricht, dass so die Zuständigkeit für die Aufsicht und Sanktionierung über die datenschutzrechtlichen Vorschriften bei den Landesdatenschutz-aufsichtsbehörden gebündelt wäre. Dagegen sprechen verfassungsrechtliche Bedenken: Der Bestimmtheitsgrundsatz nach Art. 20 Abs. 3 GG kann so verstanden werden, dass die Zuständigkeit für die Verhängung von Bußgeldern ausdrücklich bestimmt sein muss und nicht in eine andere Zuständigkeitsnorm über die allgemeine Aufsicht „hineingelesen" werden darf.

Andernfalls verbleibt es bei der allgemeinen Regelung des OWiG: Zuständig wären dann die obersten Landesbehörden, d.h. die Landesinnenministerien (§ 36 Abs. 1 Nr. 2 lit. a OWiG).

Es bleibt zu hoffen, dass der Gesetzgeber in diesem Zuständigkeits-Wirr-Warr noch Abhilfe schafft. Die erste Chance einer klaren Regelung im TTDSG hat er verpasst. Spätestens mit der ePrivacy-Verordnung auf EU-Ebene kommt die nächste Chance (dazu noch sogleich).

**Auch auf internationaler Ebene bleiben Unklarheiten: EDSA-Beschluss**

Nicht nur auf nationaler, sondern auch auf EU-Ebene führt die Beurteilung der Zuständigkeiten über die Aufsicht der ePrivacy-RL zu Kopfzerbrechen. Wie der Europäische Datenschutzausschuss (EDSA), der Zusammenschluss der europäischen Datenschutzaufsichtsbehörden, jüngst in einem internen Beschluss feststellte (veröffentlicht auf dem Blog des Kollegen RA Carlo Piltz, delegedata.de), unterscheiden sich die Regeln der Mitgliedsstaaten über die territorialen Zuständigkeiten der Aufsichtsbehörden erheblich.

Der EDSA hat nun einheitliche Kriterien zur Beurteilung der territorialen Zuständigkeit festgelegt. Zuständig sein soll die nationale Behörde, wenn

- der für die Verarbeitung Verantwortliche oder Dienstleister in ihrem Hoheitsgebiet niedergelassen ist

- und die Verarbeitung im Rahmen der Tätigkeiten einer Niederlassung im Hoheitsgebiet erfolgt, auch wenn die ausschließliche Verantwortung für Erhebung und Verarbeitung für das gesamte Gebiet der EU bei einer Niederlassung in einem anderen Mitgliedstaat liegt.

Hat der Verantwortliche keine Niederlassung in einem Mitgliedstaat der EU, kann sich die Zuständigkeit der nationalen Aufsichtsbehörden aus dem nationalen Recht ergeben, wenn dieses an ein anderes Kriterium als die Niederlassung anknüpft.

**Klärung durch die ePrivacy-Verordnung?**

Klärung könnte die seit langem erwartete ePrivacy-Verordnung bringen. Diese wird – wie die DSGVO – unmittelbar geltende Regelungen zum ePrivacy-Recht und auch der Aufsicht enthalten und so die rechtlichen Vorgaben in der Union vereinheitlichen (wir berichteten über den Verlauf des Gesetzgebungsprozesses und den jüngsten Entwurf in unserem Newsletter aus dem Februar 2021). Nach diesem jüngsten Entwurf sollen die Mitgliedsstaaten nach Art. 18 unabhängige Aufsichtsbehörden nach den Maßstäben der Art. 51-54 DSGVO schaffen. Dies können die Datenschutzaufsichtsbehörden nach der DSGVO oder auch neu geschaffene Stellen sein, die dann mit den Datenschutzaufsichtsbehörden zusammenarbeiten müssen.

Ob dies nun aller Fragen Lösung sein wird, ist noch offen: So kritisierte etwa der EDSA in einem Beschluss aus März 2021, dass die Aufsichtszuständigkeit nicht – wie in früheren Entwürfen beabsichtigt – den nach der DSGVO zuständigen Behörden zugewiesen wurde und dass auch Vorschriften zur Zusammenarbeit und Kohärenz zwischen den Aufsichtsbehörden gestrichen wurden. Ob die Auffassung des EDSA nun im Laufe des weiteren Gesetzgebungsverfahrens berücksichtigt wird und wie die endgültigen Bestimmungen der Aufsichtszuständigkeiten über die ePrivacy-Verordnung ausgestaltet werden, bleibt abzuwarten. Wir werden berichten.

## Zu guter Letzt

*Facebook wird eine Umgehung der Regelungen der DSGVO vorgeworfen mit der möglichen Konsequenz eines Bußgeldes in Millionenhöhe. WhatsApp wurde bereits im September dieses Jahres mit einem Rekordbußgeld über 225 Mio. Euro belegt und hat nunmehr auf die Vorwürfe reagiert und seine Datenschutzerklärung angepasst. Ebenfalls einem Bußgeld in Höhe von mehreren Millionen Euro sehen sich Sky Italia und ein spanisches Finanzinstitut, die Grupo CaixaBank, gegenüber. Und in einer kleinen norwegischen Gemeinde führte ein Ransomware-Angriff zu schwerwiegenden Folgenden. Wir haben Ihnen auch in diesem Monat einen Überblick über spannende Fälle erstellt:*

- **Bis zu 36 Mio. Euro für Facebook?**

Wieder lässt der österreichische Datenschutzaktivist Max Schrems von sich hören: Aufgrund seiner Beschwerde gegen die Verarbeitung personenbezogener Daten durch Facebook, insbesondere im Zusammenhang mit den Nutzungsbedingungen, schlug die irische Datenschutzbehörde vor, Facebook mit einer Geldstrafe von 28-36 Mio. Euro zu belegen. Der Entwurf wurde europaweit an andere Datenschutzbehörden übermittelt und wird nun überprüft. Vor einer endgültigen Entscheidung muss die federführende irische Datenschutzbehörde deren Ansichten berücksichtigen. Der Entscheidungsentwurf beschreibt die Verstöße als schwerwiegend und kritisiert Facebook für mangelnde Transparenz. Schrems kritisierte die Feststellungen und sagte, sie liefen darauf hinaus, dass

der Datenschutzbeauftragte Facebook grünes Licht für die Umgehung der EU-Datenschutzgrundverordnung gebe, indem Facebook die Vereinbarung über die Datennutzung in einen „Vertrag“ umetikettiere und die Zustimmungsklauseln zu Bereichen wie Werbung und Online-Tracking in seine Geschäftsbedingungen verschiebe. Dies widerspreche den Absichten der DSGVO, die es ausdrücklich verbiete, Einwilligungserklärungen in AGB zu verbergen.

Die Anrufung der europäischen Aufsichtsbehörden kann weitreichende Folgen haben: Bereits 2018 hatte die irische Datenschutzbehörde einen Vorschlag, WhatsApp mit einem Bußgeld über 30-50 Millionen Euro zu belegen, an weitere europäische Aufsichtsbehörden übermittelt (wir berichteten im September 2021). Am Ende des Verfahrens erging ein Verbindlicher Beschluss an die irische Behörde, die Bußgeldhöhe neu zu bewerten. Das Bußgeld gegen WhatsApp wurde daraufhin auf 225 Mio. Euro mehr als vervierfacht.

- **WhatsApp passt Datenschutzerklärung an**

Auf diese Entscheidung und die WhatsApp darin unterbreiteten Vorwürfe hat das Unternehmen mittlerweile reagiert und nunmehr seine Datenschutzerklärung umgestellt. Zwar geht WhatsApp gegen das Bußgeld gerichtlich unter anderem mit dem Argument vor, man habe schon immer transparent über alle Datenverarbeitungen informiert, aber so sicher, dass man die Datenschutzerklärung einfach unverändert lassen wollte, war man sich dieser Sache offenbar doch nicht. Die Änderungen beschränken sich auf eine transparentere Information der Betroffenen. Die materiellen Datenflüsse sind gleich geblieben.

- **Italien: 3,3 Mio. Euro wegen unrechtmäßiger Werbeanrufe**

Die italienische Datenschutzbehörde nahm Ermittlungen gegen Sky Italia wegen einer Vielzahl von Beschwerden wegen unerbetener Werbeanrufe auf. Einige der Betroffenen hatten zuvor der Verwendung ihrer Telefonnummern für Werbemaßnahmen ausdrücklich widersprochen. Sky Italia hatte mit mehreren Unternehmen Werbeverträge abgeschlossen, aufgrund derer die Unternehmen die Kunden via SMS kontaktierten, die Produktpalette von Sky vorstellten und fragten, ob sie von Sky Italia kontaktiert werden möchten. Die Nummern von Kunden, die dies bejahten,

wurden an Sky Italia übermittelt. Hierbei ging Sky Italia fälschlicherweise davon aus, dass die Betroffenen mit ihrer Einwilligung in die Weitergabe der Daten auch der Verwendung zu Werbezwecken zugestimmt hatten. Vor Bewerbung des Angebots hätte Sky Italia aber laut der Behörde explizit eine Einwilligung hierzu einholen müssen. Außerdem seien die von einigen Betroffenen getätigten Widersprüche nicht ordnungsgemäß erfasst und deren Existenz vor der Verwendung ihrer Telefonnummer für Werbeanrufe nicht geprüft worden. Insofern hatten Betroffene auch trotz ausdrücklichen Widerspruchs Werbeanrufe erhalten. Zudem informierte Sky Italia die Betroffenen nicht darüber, woher das Unternehmen ihre Daten hatte und wie diese verarbeitet wurden. Die italienische Datenschutzbehörde verhängte aufgrund dieser Vorwürfe eine Geldbuße i.H.v. 3,3 Mio. Euro.

- **Spanien: 3 Mio. Euro wegen unrechtmäßiger Verarbeitung von Daten zur Einschätzung der Kreditwürdigkeit**

Mangels hinreichend spezifischer Grundlage für die Verarbeitung personenbezogener Daten und mangels ausreichender Betroffeneninformationen belegte die spanische Datenschutzbehörde die Unternehmensgruppe Grupo CaixaBank mit einer Geldbuße i.H.v. 3 Mio. Euro. Die Unternehmensgruppe hatte bei einem dritten Unternehmen Daten zu einigen Betroffenen abgefragt, obwohl diese schon längst nicht mehr Kunden des Finanzinstituts waren und nicht wirksam in die Datenverarbeitung eingewilligt hatten. Trotzdem hatte das Finanzinstitut Daten mit Bezug zur Kreditwürdigkeit der Betroffenen angefragt und verarbeitet.

- **Norwegen: Erpressungstrojaner führt mangels ausreichenden Sicherheitsniveaus zur Bebußung einer Gemeinde**

Die norwegische Datenschutzbehörde belegte die Gemeinde Østre Toten mit einem Bußgeld i.H.v. 409.656 Euro in der Folge eines Ransomware-Angriffs, von dem ca. 30.000 Dokumente von Einwohnern und Beschäftigten der Gemeinde betroffen waren. Bei dieser Art eines Hacker-Angriffs auf die IT-Systeme der Gemeinde wurden die in den Systemen gespeicherten Daten von den Angreifern kopiert und verschlüsselt sowie existierende Sicherheitskopien gelöscht, um für die Entschlüsselung oder Freigabe ein Lösegeld zu fordern. Die betroffenen Dokumente

enthielten unter anderem Informationen zu Ethnie, politischer Einstellung, Religionszugehörigkeit, sexueller Orientierung, Gesundheitszustand und Bildungsgrad der Betroffenen sowie deren nationale ID und Kontonummer. Ca. 2.000 der Dokumente wurden anschließend im Dark Web veröffentlicht. Der Gemeinde sei der Vorwurf zu machen, keine hinreichenden Sicherheitsmaßnahmen vorgenommen zu haben. Weder habe es ein ausreichendes Backup- und Protokollierungssystem noch ein Zwei-Faktor-Authentifizierungs-System bei Anmeldung in die Systeme der Gemeinde gegeben.

## 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. Malte Göbel
+49(0)221 65065-337
malte.goebel@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