LOSCHELDER

Newsletter Datenschutzrecht
November 2022

Sehr geehrte Damen und Herren,

das Jahr neigt sich langsam dem Ende zu und in diesem Jahr haben auch wir Datenschützer eine wichtige Jahresendfrist einzuhalten: Spätestens am 27. Dezember 2022 müssen alle EU-Standardvertragsklauseln auf die neuen Klauseln aus 2021 umgestellt sein. Näheres dazu und auch zu den aktuellen Entwicklungen in Sachen US-Transfer haben wir in unserem ersten Beitrag aufbereitet.

Keinen Beitrag finden Sie zu den derzeit laufenden Abmahnungen in Sachen „**Google Fonts**“. Das hat einen einfachen Grund: Es füllt keinen Beitrag. Aktuell versenden zwei Kanzleien unzählige Abmahnschreiben. Das Vorgehen ist höchst bedenkenswert und wohl rechtsmissbräuchlich. Einige Kollegen sind schon erfolgreich gerichtlich dagegen vorgegangen, teils haben sie sogar Strafanzeige erstattet. **Unsere Empfehlung:** Wie schon im Juli in unserem Newsletter berichtet, sollte Google Fonts unbedingt lokal eingebunden werden. Im Übrigen können Sie die Abmahnschreiben i.d.R. ignorieren oder allenfalls (bei RAAG regelmäßig wegen fehlender Vollmacht) zurückweisen. Wir sehen in den uns bisher bekannten Fällen keinen Anlass zur Zahlung und meist auch keinen Anlass, geltend gemachte Auskunftsansprüche zu erfüllen.

Im aktuellen Newsletter informieren wir Sie dafür über neue Pflichten in Sachen Datensicherheit für Hersteller von Software und ihre Anwender und über neue Entwicklungen in Sachen DSGVO-Schadensersatzansprüche.

Rund um Schadensersatzklagen wegen (angeblicher) DSGVO-Verstöße dreht sich auch unser nächstes **Lunch@Loschelder-Webinar**, zu dem wir Sie hiermit herzlich einladen:

Kommt jetzt die DSGVO-Klagewelle? Wann Schadensersatzansprüche berechtigt sind.

Nach einem Datenschutzverstoß können betroffene Personen Schadensersatz verlangen und vor den Zivilgerichten durchsetzen. Derzeit nehmen Schadensersatzklagen rasant zu. Ein prominentes Beispiel ist der Fall „Google Fonts“. Gründe für Schadensersatzklagen können etwa eine verspätete Auskunftserteilung, eine unzulässige Videoüberwachung, nicht gewünschte Cookies oder eine Datenpanne sein. Gerichte haben in derartigen Fällen vielfach Ansprüche in vierstelliger Höhe zugesprochen. Oft sind geltend gemachte Ansprüche aber auch nicht berechtigt. Wie kann sich Ihr Unternehmen also aufstellen, um

Schadensersatzforderungen angemessen zu begegnen? In unserem lunch@loschelder-Webinar stellen wir Ihnen die aktuelle Best Practice vor.

Donnerstag, den 08.12.2022 | 12.00 bis 12.30 Uhr
Referenten: Dr. Kristina Schreiber / Dr. Simon Kohm

Anmeldung unter: webinare@loschelder.de

Wir freuen uns sehr über Ihr Interesse an unserem Newsletter!

Schließlich: Sie können der **Verwendung Ihrer Daten für diesen Newsletter-Versand jederzeit widersprechen,** indem Sie den Newsletter abbestellen. Bitte scrollen Sie dazu ans Ende dieser E-Mail.

Inhalt

Übergangsfrist für Drittstaatentransfer endet: Standardvertragsklauseln aktualisieren!

Im Sommer 2021 hat die EU-Kommission neue Standardvertragsklauseln für den Drittstaatentransfer personenbezogener Daten veröffentlicht. Die Übergangsfrist zur Implementierung der Klauseln läuft am 27. Dezember 2022 ab. Verantwortliche sollten daher jetzt ihre Datentransfers in Drittstaaten unter die Lupe nehmen und gegebenenfalls die neuen Standardvertragsklauseln einführen. Dabei ist auch in den Blick zu nehmen, was sich in den USA in Sachen Datentransfers getan hat.

Standardvertragsklauseln kommen in der Praxis in einer Vielzahl von Verträgen zum Einsatz, die einen Bezug zu Datenübermittlungen ins Ausland haben. Etwa für Betrieb von Cloud-Diensten mit Servern außerhalb der EU, datenverarbeitenden Anwendungen für Webseiten oder von E-Mail-Diensten, die von US-Anbietern bereitgestellt werden, werden angemessene Sicherheiten für den Drittstaatentransfer benötigt. Die Standardvertragsklauseln nach Art. 46 DSGVO sind dafür das wohl meistgenutzte Instrument.

Mit dem Durchführungsbeschluss EU/2021/914 vom 4. Juni 2021 hat die EU-Kommission nach über elf Jahren erstmals neue Standardvertragsklauseln erlassen, die Verantwortliche bis zum 27. Dezember 2022 implementiert haben müssen. Für Neuverträge gilt bereits seit dem 27. September 2021 die Pflicht, die neuen Standardvertragsklauseln zu Verwenden.

Zu beachten ist bei der Umstellung auf die neuen Standardvertragsklauseln:

- **Bußgeld- und Schadensersatzrisiko:** Werden alte Standardvertragsklauseln nicht bis zum 27. Dezember 2022 durch die neuen ersetzt und gibt es keine andere Absicherung des Datenschutzniveaus im Zielland, werden Daten unter Verstoß gegen Art. 44 ff. DSGVO ins Drittland übertragen. Dieser Verstoß ist nach Art. 83 Abs. 5 lit. c) DSGVO mit einem Bußgeld in Höhe von bis zu 4% des (Konzern-)Jahresumsatzes des Verantwortlichen bzw. der Unternehmensgruppe bewehrt.

- **Selbstläufer?** Die meisten großen Anbieter (insbesondere: Google, Facebook, AWS, Microsoft) haben die neuen Standardvertragsklauseln mittlerweile implementiert, auch

für Bestandskunden. Bei Google, Facebook und AWS gelten die neuen Standardvertragsklauseln automatisch für Neu- und Bestandskunden, bei Microsoft dagegen nur für Neukunden. Bestandskunden von Microsoft mit Verträgen, die älter sind als Oktober 2021, müssen aktiv werden, um die neuen Standardvertragsklauseln einzubeziehen, und ihre Verträge aktualisieren. Sofern vorhanden kann man sich dafür an den Account Manager oder den Microsoft Partner (CSP) wenden. Wer beides nicht hat, muss den Microsoft Support in Irland kontaktieren.

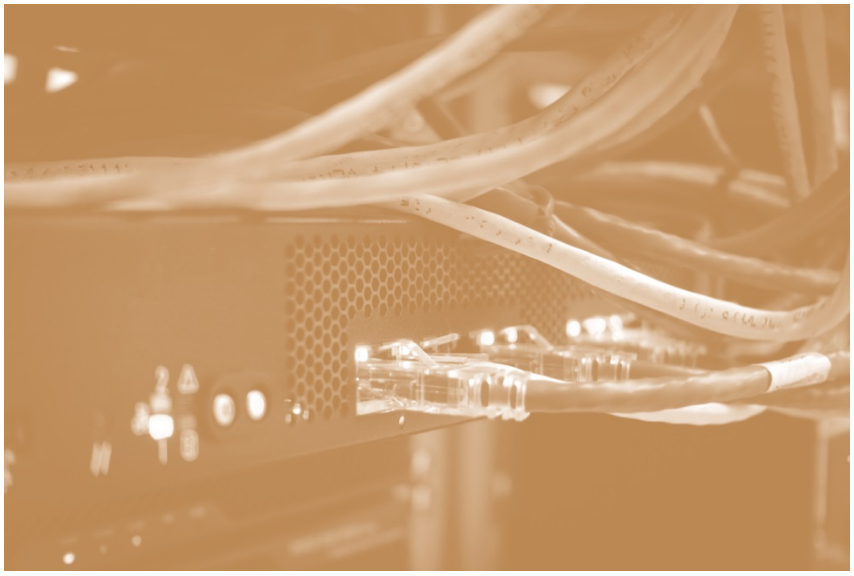
- **Reicht die Unterschrift?** Seit der EuGH-Entscheidung in Sachen Schrems II ist zudem klar: Mit dem bloßen Abschluss der Standardvertragsklauseln ist es nicht getan. Notwendig ist die Durchführung eines sog. *Transfer Impact Assessments* (TIA): Es muss geprüft werden, ob die nationalen Rechtsvorschriften im Zielland auch die Einhaltung der Standardvertragsklauseln zulassen.

  Zu einigen Ländern existieren dazu mittlerweile Gutachten der Datenschutzbehörden (China, Indien, Russland und USA).

  Ergeben sich danach Bedenken, müssen zusätzliche Maßnahmen ergriffen werden. Auch hierzu gibt es umfangreiche Empfehlungen der Behörden. Die Ergebnisse der Prüfung und ggf. die zusätzlichen Maßnahmen müssen dokumentiert werden.

- **US-Transfer künftig wieder sicher?** Für den Datentransfer in die USA werden die Standardvertragsklauseln möglicherweise in naher Zukunft nicht mehr gebraucht. Die EU und die US-Regierung haben ein neues Übereinkommen für den transatlantischen Datenverkehr („*Transatlantischer Datenschutzrahmen*“) verhandelt. Präsident Biden hat die vereinbarte Executive Order (EO) mit neuen Beschwerderechten und Begrenzungen der Behördenrechte unterzeichnet (siehe dazu dieses Papier). Dies verbessert das Datenschutzniveau in den USA deutlich, stellt aber noch keinen Angemessenheitsbeschluss nach Art. 45 DSGVO dar. Dies wird nun durch die EU-Kommission geprüft. Zwischenzeitlich sind allerdings bereits Zweifel laut geworden, ob die EO ausreicht (siehe etwa hier) – der weitere Prozess bleibt damit spannend.

Eine eingehende Analyse der Standardvertragsklauseln finden Sie in unserem Newsletter vom Juni 2021.



IT-Sicherheit als Mangel: Neue Pflichten für Softwarehersteller

Die EU-Kommission hat kürzlich den Entwurf eines Cyber Resilience Act (CRA) veröffentlicht. Sie verspricht sich eine höhere Cybersicherheit insbesondere durch besseres Produktdesign. Diese Anforderungen bergen jedoch etliche Schwierigkeiten für Softwarehersteller und -anbieter. Sie müssen zudem bei Missachtung der Anforderungen ein strenges Sanktionsregime fürchten, wenn der CRA so umgesetzt wird.

Der CRA ist Teil der Digitalstrategie der EU. Er soll in Ergänzung des Cybersecurity Act digitale Produkte auf dem europäischen Markt sicherer und damit die Wirtschaft insgesamt weniger anfällig für Cyberattacken machen. Dabei sollen Hersteller von Software („materieller und immaterieller digitaler Produkte“) einheitlichen Cybersicherheitsregeln für ihre Produkte unterworfen werden.

Konkret soll Cyberkriminalität entgegengewirkt werden, die allein 2021 weltweit Schäden von etwa 5 Billionen Euro angerichtet hat. Die EU sieht zwei zentrale Problemfelder: Fehlendes Wissen und Informationen über die sichere Verwendung von digitalen Produkten durch die Nutzer, aber auch unzureichende Cybersicherheit, die bereits von dem Design der Produkte selbst ausgeht.

Letzteres soll durch den CRA in Angriff genommen werden. Für Hersteller steigen die regulatorischen Anforderungen damit erheblich – von der DSGVO sind sie regelmäßig nicht direkt adressiert. Mit dem CRA wird auch insofern ein weitreichendes Sanktionsregime Einzug halten.

Erhöhte Cybersicherheit durch Produktdesign

Die Hersteller, Importeure und Händler von Software sollen nach dem Entwurf des CRA für die Lebensdauer des Produkts dessen Cybersicherheit gewährleisten und für etwaige Sicherheitslücken haften („Security by Design"). Diskutiert wird eine Begrenzung dieser sog. „Nachmarktpflicht" auf einen Zeitraum von fünf Jahren nach dem Inverkehrbringen des Produkts.

Aus der DSGVO bekanntes Sanktionsregime

Der CRA-Entwurf bestimmt, dass Sanktionen „wirksam, verhältnismäßig und abschreckend" sein sollen (Art. 53). Bei entsprechenden Verstößen sind denn auch Bußgelder in Höhe von bis zu 15 Millionen Euro oder 2,5% des gesamten weltweiten Umsatzes des sanktionierten Unternehmens vorgesehen (die höhere Grenze gilt).

Einbindung des CRA-Entwurfs in das New Legislative Framework

Der CRA-Entwurf fügt sich in das sog. New Legislative Framework (NLF) der EU ein. NLF bezeichnet ein EU-Harmonisierungskonzept mit einheitlichen Rahmenregelungen für den freien Warenverkehr unter besonderer Berücksichtigung der Produktsicherheit. Über das NLF werden Begriffe und rechtliche Rahmenbedingungen vereinheitlicht. Dies zeigt sich auch im CRA-Entwurf. Dies erleichtert den Normverpflichteten Verständnis und Umsetzung der Regelungen.

Gute Ansätze weiterentwickeln

Im aktuell vorliegenden Entwurf des CRA sind denn bereits überzeugende Ansätze enthalten, die indes noch weiterzuentwickeln sind: So bleibt z.B. die Einteilung in „critical" und „highly critical products" denkbar pauschal und holzschnittartig, ohne ausreichend den Verwendungszweck einzubeziehen. Auch ist die zu begrüßende EU-Konformitätserklärung für „sichere Produkte" nicht ausgereift:

Es fehlt noch an Regelungen zu den dafür notwendigen harmonisierten Normen, wann ein Produkt entsprechend sicher ist.

Neues zum DSGVO-Schaden: Reicht ein bloßer Ärger?

Die DSGVO-Schadensersatzklagen nehmen zu – dazu ergangene Rechtsprechung ebenfalls. In einem EuGH-Verfahren wurden unlängst die Schlussanträge des Generalanwalts zur Auslegung der zentralen Schadensersatznorm vorgelegt. Die dortigen Positionierungen helfen enorm bei einer Eindämmung der aktuellen Klageflut: Welche Anforderungen sind an das Vorliegen eines (immateriellen) Schadens im Sinne von Art. 82 DSGVO zu stellen?

Hintergrund des unter dem Az. C-300/21 geführten Vorabentscheidungsverfahrens ist ein vor dem OGH in Österreich geführter Rechtsstreit, in dem der Kläger von der Österreichischen Post AG 1.000 EUR Schadensersatz auf Grundlage von Art. 82 DSGVO geltend macht. Die Beklagte hatte ohne Einwilligung Informationen über die politischen Affinitäten der österreichischen Bevölkerung erhoben, um zielgruppengerichtet Wahlwerbung versenden zu können. Der hiervon betroffene Kläger fühlte sich von der ihm auf diese Weise zugeschriebenen politischen Gesinnung beleidigt und trug vor, dass das Verhalten der Beklagten bei ihm großes Ärgernis sowie ein Gefühl der Bloßstellung ausgelöst habe, für dessen Kompensation er mit seiner Klage immateriellen Schadensersatz verlangt. Aber ist dafür Schadensersatz zu zahlen?

Gegenstand des EuGH-Verfahrens

Um dies zu klären, hat der EuGH drei Fragen zu beantworten, von denen zwei praktisch besonders relevant sind (und von den deutschen Gerichten derzeit uneinheitlich beantwortet werden):

(1) Erfordert der Schadensersatzanspruch einen tatsächlich erlittenen Schaden beim Betroffen oder reicht jede DSGVO-Verletzung für die Bejahung eines Schadens?

(2) Reicht ein bloßes Ärgernis auf Seiten des Betroffenen für einen immateriellen Schaden oder muss mehr passiert sein?

Am 06.10.2022 hat der Generalanwalt am EuGH Manuel Campos Sánchez-Bordana seine Schlussanträge im Verfahren veröffentlicht. Seine Position lässt von Schadensersatzforderungen betroffene Unternehmen aufatmen:

- Ein Schaden muss dargelegt werden. Es genügt nicht, nur einen Datenschutzverstoß darzutun. Der DSGVO-Schadensersatz stellt keine Strafe für einen DSGVO-Verstoß dar, sondern soll erlittene Nachteile ausgleichen.

  Diese Ansicht des Generalanwaltes entspricht auch der mehrheitlich von den deutschen Gerichten vertretenen Rechtsaufassung, die für den Schadensersatzanspruch aus Art. 82 DSGVO überwiegend die Darlegung und den Nachweis eines tatsächlichen Schadens verlangt haben.

- Ein Ausgleich ist aber nicht bereits für ein bloßes Ärgernis oder Unmut zu zahlen.

Wie geht es weiter?

Die endgültige Entscheidung des EuGH steht noch aus, einen Termin zur Urteilsverkündung gibt es noch nicht. Ob der EuGH den Schlussanträgen folgt, ist offen – meistens ist das aber der Fall. Wir halten Sie informiert!

Wie viel Sicherheit muss sein?

Übermitteln Behörden Dokumente mit sensiblem Inhalt auf elektronischem Weg, stellt sich die Frage, welche Sicherheitsanforderungen dabei einzuhalten sind. In einer aktuellen Entscheidung hat das Verwaltungsgericht Frankfurt am Main klargestellt: Bei der elektronischen E-Mail-Kommunikation von Behörden ist grundsätzlich eine einfache Transportverschlüsselung notwendig, aber auch auseichend, um den datenschutzrechtlichen Anforderungen zu genügen.

Der Stand der Digitalisierung in deutschen Behörden wird häufig kritisiert. In der Regel herrscht dabei weitestgehend Einigkeit darüber, dass die Möglichkeiten des technischen Fortschritts, insbesondere in der elektronischen Kommunikation, nur langsam und unzureichend umgesetzt werden.

In dem nun von dem VG Frankfurt/Main entschiedenen Fall wehrte sich der Antragsteller jedoch gerade gegen eine behördliche Übermittlung von Dokumenten per E-Mail, weil er Bedenken hinsichtlich der Sicherheit der elektronischen Kommunikation hegte.

Als Händler von Produkten, die unter das Kriegswaffenkontrollgesetz fallen, ist der Antragsteller seit dem 1. April 2020 dazu verpflichtet, Meldungen über seine Kriegswaffenbestände elektronisch an das Bundesamt für Wirtschaft und Ausfuhrkontrolle (BAFA) zu übermitteln (§ 10 Abs. 3 Satz 1 KrWaffKontrGDV). In diesem Zusammenhang hat auch das

Bundesamt selbst die Vorgänge in seinem Aufgabenbereich weitestgehend auf den elektronischen Rechtsverkehr umgestellt und über die Antragsgegnerin mehrfach E-Mails mit personenbezogenen Daten des Antragstellers an diesen versandt. Dabei hielt es sich an die vom Bundesamt für Sicherheit und Informationstechnik (BSI) herausgegebenen Empfehlungen für IT-Sicherheit, wonach für den Versand von E-Mails hier eine einfache Transportverschlüsselung notwendig, aber auch ausreichend sei.

Bei einer Transportverschlüsselung handelt es sich um eine Verschlüsselung auf dem Übertragungsweg der E-Mail, die von den meisten E-Mail Providern standardmäßig angeboten wird. Hiermit wird die E-Mail-Kommunikation zwischen den Servern des Absenders, des Providers und des Empfängers verschlüsselt und vor dem Zugriff Dritter geschützt. Zu unterscheiden ist dies von der „Ende-zu-Ende-Verschlüsselung", bei der es sich um eine Verschlüsselung des Inhalts einer E-Mail handelt.

Dem Antragsteller ging die gewählte Transportverschlüsselung nicht weit genug. Er verlangte eine qualifizierte Verschlüsselung und regte an, die E-Mails mittels der Software Chiasmus verschlüsseln zu lassen. Grund hierfür war die Befürchtung, durch die seiner Ansicht nach unzureichende Verschlüsselung als Händler von Kriegswaffen identifiziert werden zu können. So könne er leicht Opfer von Kriminellen werden, die an die von ihm vertriebenen Produkte gelangen wollten.

Im einstweiligen Rechtsschutzverfahren versuchte er daher, der Antragsgegnerin die Übermittlung von seinen personenbezogenen Daten auf elektronischem Wege ohne höhere Sicherheitsstandards untersagen zu lassen. Das VG Frankfurt/Main sah einen entsprechenden öffentlich-rechtlichen Unterlassungsanspruch des Antragstellers jedoch nicht gegebenen und lehnte seinen Antrag vollumfänglich ab.

Elektronische Kommunikation im allgemeinen Verwaltungsverfahren

Dazu führte das Gericht aus, dass die Übermittlung elektronischer Dokumente im allgemeinen Verwaltungsverfahren zulässig ist, soweit der Empfänger hierfür einen Zugang eröffnet (§ 3a Abs. 1 VwVfG). Dieser Grundsatz gilt nach den spezialgesetzlichen

Vorschriften auch für die Kontroll- und Dokumentationspflichten nach dem Kriegswaffenkontrollgesetz.

Die gewählte Ausgestaltung der elektronischen Kommunikation mittels einer Transportverschlüsselung genüge zudem den datenschutzrechtlichen Anforderungen und verletze den Antragsteller daher nicht in seinen Rechten.

Verarbeitungsgrundsatz der Integrität und Vertraulichkeit

Dabei stellte das Gericht auf den Grundsatz der „Integrität und Vertraulichkeit" aus Art. 5 Abs. 1 lit. f DSGVO ab. Hiernach muss bei der Verarbeitung personenbezogener Daten eine angemessene Sicherheit gewährleistet sein. Dies schließt die Vornahme geeigneter technischer und organisatorische Maßnahmen (sog. „TOM") zum Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor Verlust, Zerstörung oder Schädigung der personenbezogenen Daten ein. Hierzu gehört auch, dass Unbefugte keinen Zugang zu den Daten haben und weder die Daten, noch die Geräte, mit denen diese verarbeitet werden, benutzen können (Erwägungsgrund 39 Satz 12 DSGVO).

Technische Anforderungen an die Sicherheit der Verarbeitung

Hinsichtlich der technischen Anforderungen für die sichere Verarbeitung personenbezogener Daten trifft Art. 32 DSGVO konkretere Vorgaben: Es sind diejenigen Maßnahmen zu treffen, die unter Berücksichtigung von acht Kriterien ein dem Risiko angemessenes Schutzniveau gewährleisten. Diese acht Kriterien sind: Stand der Technik, Implementierungskosten, Art, Umfang, Umstände und Zwecke der Verarbeitung sowie unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen.

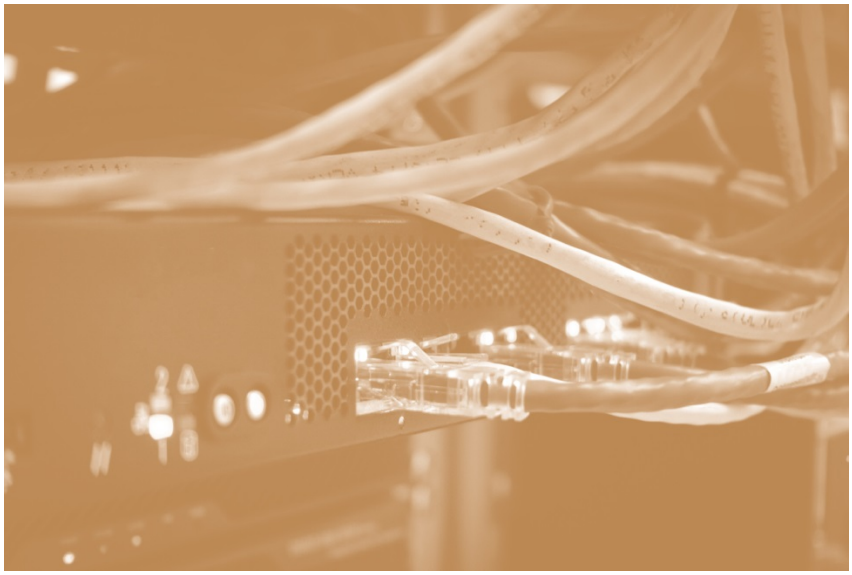
Hieraus folgerte das Gericht, dass lediglich eine unverschlüsselte elektronische Kommunikation unzulässig sei. Die Vorschrift mache jedoch keine Vorgaben in Bezug auf einzusetzende Verschlüsselungsalgorithmen oder bestimmte Schlüssellängen. Insofern habe die Antragsgegnerin durch die gewählte Transportverschlüsselung organisatorische Vorkehrungen zur Wahrung der Integrität und Vertraulichkeit nicht nur angestrebt, sondern bereits getroffen. Auf datenschutzrechtlicher Grundlage genüge dies gegenwärtig noch dem Standard, der zu verlangen sei.

Höhere Anforderungen für sensible Daten oder besondere Datenkategorien?

Offen ließ das Gericht allerdings die Frage, ob andere Maßstäbe angelegt werden müssen, wenn die elektronische Kommunikation die Verarbeitung personenbezogener Daten besonderer Kategorien im Sinne von Art. 9, 10 DSGVO betrifft.

Auch ob höhere Anforderungen an die Sicherheitsmaßnahmen für die Fälle gelten, in denen ein „Interesse krimineller und ressourcenreicher Dritter“ zu befürchten sei, ließ das Gericht unberücksichtigt, weil der Antragsteller ein solches Interesse Dritter im einstweiligen Rechtsschutzverfahren nicht ausreichend glaubhaft gemacht hatte.

Für diese hat jedoch bereits das VG Mainz mit Urteil vom 17. Dezember 2020 ausgeführt, dass insofern u.U. qualifizierte Schutzmaßnahmen zu ergreifen sind. Sofern aber keine Anhaltspunkte für besonders sensible Daten bestehen oder sonstige Umstände hinzutreten, sah auch das VG Mainz die Verwendung einer Transportverschlüsselung bei der elektronischen Kommunikation von Berufsgeheimnisträgern – in diesem Fall: Rechtsanwälten – für datenschutzrechtlich ausreichend.



Zu guter Letzt

Auch diesen Monat gibt es spannende Bußgelder. Eine französische Interessenvereinigung musste für DSGVO-Verstöße ein Bußgeld in Höhe von 250.000 Euro zahlen. Das Profiling eines britischen Unternehmens ohne Einwilligung der betroffenen Nutzer wurde von der zuständigen Behörde mit etwa 1.500.000 Euro sanktioniert. Die gleiche Behörde verhängte zudem ein sechsstelliges Bußgeld gegen ein Unternehmen wegen unzulässiger Anrufe zu Werbezwecken. Schließlich: Der EDSA hat Leitlinien für die Meldung von Datenpannen veröffentlicht.

- **Der Europäische Datenschutzausschuss (EDSA) hat Leitlinien zur Meldung von Datenpannen veröffentlich**

Art. 33 DSGVO verpflichtet Verantwortliche bekanntlich zur Meldung der dort genannten Datenpannen, u.U. sind nach Art. 34 DSGVO zudem die Betroffenen zu informieren. Welche Anforderungen aus Behördensicht dabei eingehalten werden sollten, listen die aktuellen Leitlinien 09/2022 des EDSA vom 10.10.2022. Sollte der Verantwortliche dieser Pflicht nicht genügen, kann das Bußgelder nach Art. 83 DSGVO mit sich bringen. Die Leitlinien sollen dem Verantwortlichen helfen, sich im Falle einer solchen Verletzung DSGVO-konform zu verhalten. Sie umfassen Erklärungen dazu, was als Datenpanne gesehen werden muss und wie sich Verantwortliche in bestimmten Situationen zu verhalten haben.

- **Frankreich: 250.000 Euro aufgrund von DSGVO-Verstößen gegen die wirtschaftliche Interessensvereinigung INFOGREFFE**

Gegen die Interessensvereinigung INFOGREFFE verhängte die französischen Aufsichtsbehörde CNIL ein Bußgeld in Höhe von 250.000 Euro nach Feststellung einiger Verstöße, die die Behörde bei einer Untersuchung der zugehörigen Website feststellte: Auf der Website haben Nutzer die Möglichkeit, rechtliche Informationen über Unternehmen abzurufen und darüber hinaus von den Handelsgerichten beglaubigte Dokumente zu bestellen. Bei der Untersuchung ging es insbesondere um die Fragen, ob festgelegte Datenaufbewahrungsfristen eingehalten und hinreichende Sicherheitsmaßnahmen ergriffen wurden. Beides verneinte die CNIL.

- **Großbritannien: 1,5 Mio. Euro Bußgeld wegen unzulässigem Profiling und Direktmarketinganrufen ohne Zustimmung**

Die britische Datenschutzbehörde ICO kontrollierte das Unternehmen Easylife, welches Haushaltsprodukte über Werbekataloge vertreibt. Hierbei stellte sich heraus, dass der Kauf von sog. „Trigger-Produkten" zu bestimmten Annahmen über den Gesundheitszustand der Kunden führte und im Folgenden Direktmarketinganrufe durch einen Drittanbieter durchgeführt wurden, bei denen gesundheitsbezogene Produkte angeboten wurden. 145.400 Kunden waren betroffen.

Die Datenschutzbehörde sah darin einen Verstoß gegen Art. 13 DSGVO, da keine Information über die Datenverarbeitung zu Profiling-Zwecken erfolgt war. Zudem fehlte eine Verarbeitungsgrundlage gem. Art. 9 DSGVO. Eine solche wäre erforderlich gewesen, da Gesundheitsdaten verarbeitet wurden.

Diese Reihe an Verstößen ahndete das ICO mit einem Bußgeld von ca. 1.550.000 Euro. Das hohe Bußgeld sollte abschreckende Wirkung für die gesamte Branche entfalten.

- **Großbritannien: über 150.000 Euro Bußgeld für Posh Windows Ltd wegen unzulässiger Werbeanrufe nach Adresshandel**

Das Fenster- und Verglasungsunternehmen Posh Windows Ltd. hatte im Zeitraum von Anfang August 2020 bis einschließlich April 2021 rund 461.062 unzulässige Werbeanrufe durch einen Dienstleister tätigen lassen. Die notwendigen Kontaktdaten hatte das Unternehmen zuvor von einem Datenhändler gekauft und mittels dieser Daten Anrufe zur Kundenakquise durchgeführt. Eine Einwilligung lag nicht vor. Selbst Personen, welche den Anrufen widersprochen hatten, wurden mehrfach kontaktiert. Das Unternehmen ging aggressiv vor und rief zudem mit unterdrückter Rufnummer an, um die Rückverfolgung des Anrufers zu verhindern.

Zudem zeigte sich das Unternehmen in den Untersuchungen der britischen Datenschutzbehörde ICO wenig kooperativ, machte nur wenige und größtenteils widersprüchliche Angaben. Dies führte zu einem Bußgeld von ca. 168.000 Euro.

- **Frankreich: Erneutes Millionen-Bußgeld für Clearview AI**

Die französische Datenschutzbehörde verhängte ein Bußgeld i.H.v. 20 Millionen Euro gegen das Unternehmen Clearview AI, welches ein Gesichtserkennungstool zur Identifizierung betroffener Personen anhand von Bildern und Videos, die online veröffentlicht wurden, betreibt. Clearview verfügt nach eigenen Angaben mittlerweile über mehr als 30 Milliarden Gesichtsfotos, welche alle aus dem Internet, vordergründig von Social-Media-Profilen, stammen. Das Unternehmen bietet Ermittlungsbehörden Zugang zu dieser Datenbank an. Diese nutzen die Bilder etwa zum Abgleich mit Fotos von Verdächtigen in Strafverfahren. Es ist nicht das erste Bußgeld, welches gegen Clearview AI aufgrund (angeblicher) Datenschutzverstöße verhängt wird.

Clearview ist zwar nicht in der EU niedergelassen, verarbeitet jedoch unter anderem personenbezogene Daten von Personen in der EU, weshalb die DSGVO anwendbar ist. Für diese Verarbeitung fehlen nach Ansicht der CNIL Rechtsgrundlagen, Anträge auf Löschung werden nicht beantwortet, eine aufsichtsbehördliche Anordnung wurde missachtet.

Als erschwerende Faktoren bei der Bemessung des Bußgeldes wurden unter anderem die Schwere der Verstöße und die Tatsache, dass die biometrische Vorlage von Gesichtern auf Bildern als sensible personenbezogene Daten i.S.d. Art. 9 DSGVO qualifiziert wurde, angeführt.

Clearview hatte zuvor bereits 8,9 Millionen Euro Bußgeld von der britische Datenschutzbehörde ICO auferlegt bekommen. Auch kanadische Behörden hatten dem Unternehmen bereits das Anbieten der Dienste in mehreren Provinzen untersagt.

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