LOSCHELDER

Newsletter Datenschutzrecht
Oktober 2021

Sehr geehrte Damen und Herren,

mit dem Herbst kommen neue Themen für die Datenschützer: Anforderungen an die E-Mail-Verschlüsselung nach einer aktuellen Orientierungshilfe der DSK, aktuelle Entwicklungen zu den datenschutzrechtlichen Betroffenenrechten und mehr Klarheit zu den Zuständigkeiten bei der Website-Kontrolle.

Wir haben uns zudem die neuen DPAs von Amazon Web Services (AWS) und Microsoft genauer angesehen: Beide umfassen jetzt die erneuerten Standardvertragsklauseln. Die Nutzung der Services von AWS und Microsoft ist damit rechtssicherer geworden, wenn die neuen DPAs für die eigenen Produkte gelten. Sorglos dürfen personenbezogene Daten aber auch damit nicht in die USA übermittelt werden.

Zu guter Letzt haben wir wieder interessante Entwicklungen im knappen Überblick zusammengestellt: von Cookie-Bannern, die im UK abgeschafft werden sollen, über Bonus-Hopper bis hin zu interessanten Bußgeld-Entscheidungen.

Für alle Leserinnen und Leser, die sich mit der Gestaltung von Websites und anderen Online-Angeboten beschäftigen, ein Hinweis auf ein Webinar zu ab dem 1. Dezember geltenden 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

Sicherheit beim E-Mail-Versand: Wie viel Verschlüsselung muss sein?

Erreicht meine E-Mail den Empfänger auf dem Sicherheitsniveau einer Postkarte? Wie sicher sind die Daten, die ich per Mail verschicke? Wann ist eine angemessene Datensicherheit gewahrt und ein Verstoß gegen die DSGVO damit ausgeschlossen? Wir haben eine neue Orientierungshilfe der Datenschutzkonferenz zum Thema Verschlüsselung für Sie genauer betrachtet.

Die Datenschutzkonferenz erläutert in einer neuen Orientierungshilfe, welche Schutzmaßnahmen Unternehmen bei der Kommunikation per E-Mail einhalten müssen.

In der Pflicht sind dabei Empfänger und Absender: Einige Verschlüsselungsmaßnahmen können nur durch beide Kommunikationspartner wirksam umgesetzt werden. Deshalb haben sowohl die Sender als auch die Empfänger von E-Mails die notwendigen technischen Maßnahmen zu ergreifen, um die Sicherheit und Vertraulichkeit der Kommunikation zu gewährleisten.

Risiken unzureichender Verschlüsselung

Eine unzureichende Verschlüsselung kann einen Datenschutzverstoß begründen. Dies kann zu einer Verwarnung führen (siehe hierzu das Verfahren vor dem VG Mainz, über das wir im Newsletter aus April 2021 berichteten). Möglich sind abhängig vom Einzelfall (Verschulden, Ausmaß, Schäden) auch Bußgelder und Schadensersatzansprüche von Betroffenen.

Neben dem Datenschutzrecht müssen Unternehmen auch eine andere Folge unzureichender Verschlüsselung beachten, die zu ganz erheblichen kommerziellen Schäden führen kann: Unternehmens-Know-How und andere sensible Informationen sind nach dem Geschäftsgeheimnisschutzgesetz nur dann Geschäftsgeheimnisse, wenn Unternehmen hinreichende Schutzmaßnahmen ergreifen. Die Verschlüsselung von E-Mails könnte eine solche erforderliche Schutzmaßnahme sein … Mehr dazu können Sie hier im Geheimnisblog lesen.

Verschlüsselungsstandards in der E-Mail-Kommunikation

Die Verschlüsselung von Daten ist eine geeignete technische Schutzmaßnahme, um die Datensicherheit zu gewährleisten.

Art. 32 DSGVO sagt dies ausdrücklich. Bei der E-Mail-Kommunikation kommen grundsätzlich zwei Arten der Verschlüsselung in Betracht:

- Die **Transportverschlüsselung** als „äußere Hülle“ in zwei Formen:

  - einfache Transportverschlüsselung
  - qualifizierte Transportverschlüsselung

  Die **einfache Transportverschlüsselung basiert** häufig auf den weit verbreiteten SSL oder TLS-Protokollen. Die **qualifizierte Transportverschlüsselung** wird durch weitere kryptografische Authentifizierungselemente ergänzt. So kann durch die Nutzung einer Kombination aus öffentlichen und privaten Schlüsseln etwa sichergestellt werden, dass die Geräte und Server, mit denen auf die Emails zugegriffen wird, auch tatsächlich die berechtigten Geräte des Empfängers sind (über die dahinterstehende Verschlüsselungstechnik informiert das BSI).

  Sobald die E-Mail auf dem Server des Empfängers angekommen ist, wird sie entschlüsselt. Dies geschieht auf der Grundlage symmetrischer Schlüssel, das heißt sowohl der Versender wie auch der Empfänger nutzen denselben Schlüssel. Die Transportverschlüsselung stellt einen Schutz der Kommunikation gegen passives Abfangen während des Übermittlungsvorgangs dar (daher **Transport**verschlüsselung). Ihr Nachteil ist, dass entschlüsselte Emails von den Servern abgegriffen werden können.

- **Ende-zu-Ende-Verschlüsselung der Inhalte**

  Bei der **Ende-zu-Ende-Verschlüsselung** wird die E-Mail nicht nur auf dem Transportweg, sondern auch bei der Zwischen- und Weiterverarbeitung auf dem Server des Empfängers verschlüsselt. Durch die Nutzung spezifischer Verfahren wie S/MIME oder OpenPGP werden asymmetrische öffentliche und private Schlüssel kombiniert: Die Nachricht wird mit einem öffentlichen Schlüssel verschlüsselt, kann aber nur mittels des privaten Schlüssels, den nur die berechtigten Empfänger haben, entschlüsselt werden.

Der Vorteil dieses Verfahrens ist, dass der Zugriff unbefugter Dritter weitestgehend ausgeschlossen ist. Einen Überblick über gängige Verfahren und Tools bietet das BSI. Wird die E-Mail abgefangen, können die Inhalte nicht gelesen werden: Sie werden erst beim Empfänger mit einem bei diesem vorhandenen Schlüssel entschlüsselt. *(mehr dazu beim Bundesamt für Sicherheit in der Informationstechnik und der Datenschutzkonferenz)*

Welche Verschlüsselung ist wann zu wählen?

Für die Auswahl des Verschlüsselungsgrades gilt der risikobasierte Ansatz des Art. 32 DSGVO. Dies bedeutet: Je höher das Risiko für die Betroffenen, desto sicherer muss die E-Mail verschlüsselt werden. Dabei ist sowohl der Inhalt der Daten zu berücksichtigen, als auch das Risiko, dass auf diese im Laufe der Kommunikation (Transport und/oder Speicherung) zugegriffen wird.

1. *Unternehmen müssen **zertifizierte E-Mail-Provider** wählen*

   Der E-Mail-Provider sollte die Zertifizierung über die Einhaltung der technischen Anforderungen der Technischen Richtlinie 03108-1 des BSI erhalten haben (Erläuterungen im Überblick des BSI). Dies stellt sicher, dass die wesentlichen technischen Voraussetzungen für eine angemessene Verschlüsselung über den E-Mail-Provider, etwa durch entsprechende Anweisungen oder Konfigurationen, mit diesem auch umgesetzt werden können.

2. *Immer* **einfache Transportverschlüsselung** *bei personenbezogenen Daten*

   Wenn E-Mails mit personenbezogenen Daten (also praktisch immer) verschickt werden, müssen diese immer (einfach) transportverschlüsselt sein (so die Aufsichtsbehörden). Die Transportverschlüsselung stellt das Mindestmaß dar, um eine angemessene Datensicherheit zu erreichen. Die Verschlüsselung sollte die Anforderungen der Technischen Richtlinie 02102-2 des BSI erfüllen und über die SMTPS und TLS-Protokolle aufgebaut sein; umfassende Hinweise zur Verwendung von TLS nach der Technischen Richtlinie 02102-2 veröffentlichte das BSI (siehe auch die Leitlinie des BSI).

3. ***Qualifizierte Transportverschlüsselung*** *bei höherem Risiko,* ***Ende-zu-Ende-Verschlüsselung*** *bei hohem Risiko, z.B. bei Gehaltsdaten, Gesundheitsdaten, Gewerkschaftsinformationen u.v.m.*

   Für die E-Mail-Kommunikation mit hohen Risiken ist für eine angemessene Datensicherheit regelmäßig die Ende-zu-Ende-Verschlüsselung oder zumindest die qualifizierte Transportverschlüsselung zu wählen. Ob die Ende-zu-Ende-Verschlüsselung oder die qualifizierte Transportverschlüsselung erforderlich ist, hängt aber auch nach der Auffassung der Datenschutzkonferenz von den für die Betroffenen bestehenden Risiken, der konkreten Ausgestaltung des Übertragungsweges und etwaiger Kompensationsmaßnahmen ab.

   Entsprechend müssen Versender und Empfänger die technische Infrastruktur schaffen, um diesen Verschlüsselungsgrad zu ermöglichen. Dies bedeutet zumindest die Einhaltung der Technischen Richtlinie 02102-2 des BSI. Für die Ausgestaltung einer zuverlässigen Ende-zu-Ende-Verschlüsselung und den Einsatz der S/MIME und OpenPGP-Protokolle können die Hinweise des BSI beachtet werden.

Verzicht auf eine hinreichende Verschlüsselung?

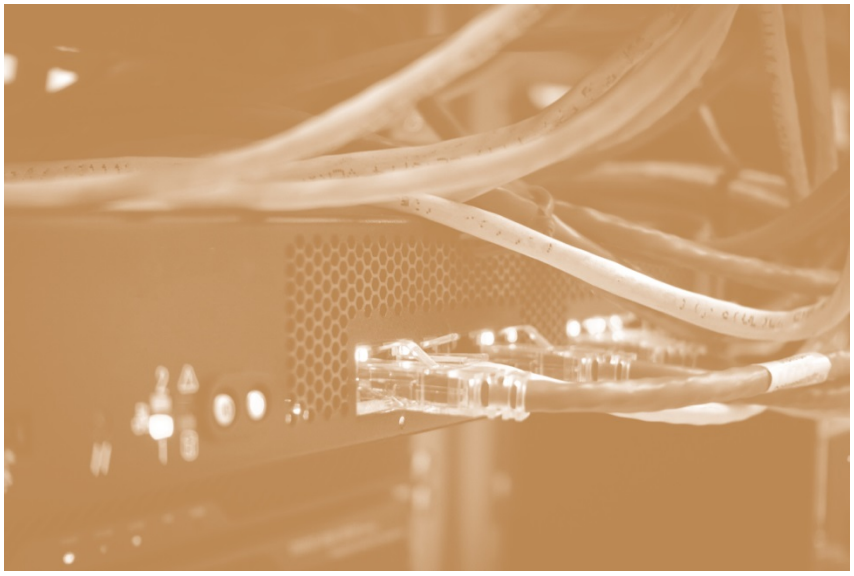
Höchst umstritten ist, ob Betroffene selbst auch auf eine angemessene Datensicherheit beim Versand ihrer Daten per E-Mail verzichten können. Diese Frage stellt sich in der Praxis insbesondere beim Versand von Gesundheitsdaten per E-Mail.

Eine Einwilligung in eine „unangemessene" niedrige Datensicherheit ist nach überzeugender Ansicht möglich, jedenfalls dann, wenn alternativ auch eine angemessene Datensicherheit angeboten wird. Dazu haben wir hier ausführlich berichtet.

Zu berücksichtigen ist aber, dass es für einen wirksamen Verzicht bzw. eine Einwilligung auf den Betroffenen ankommt. Dieser muss nicht identisch mit dem Empfänger oder dem Sender sein, sodass es hier maßgeblich auf den Inhalt der E-Mail ankommt. Daran kann man erkennen, dass sich ein solcher Ansatz für eine unternehmensweite Handhabe grundsätzlich nicht anbietet, da sie im Alltag vom Inhalt der Mail abhängt und ggf. einer Einzelfallprüfung bedarf, was nicht praktikabel ist.

Dokumentation der ergriffenen Maßnahmen

Unabhängig davon, welche konkreten Verschlüsselungsmaßnahmen ergriffen wurden, sollten diese, wie die verwendeten Protokolle und Standards, umfassend dokumentiert werden. Die Datenschutzkonferenz fordert, dass die Einhaltung der im Rahmen der Orientierungshilfe aufgestellten Anforderungen an die Verschlüsselungs- und Signaturverfahren nachgewiesen werden müssen. Dies entspricht der allgemeinen Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO.



Aktuelles zu den Betroffenenrechten

Auch über drei Jahre nach Inkrafttreten der DSGVO bleiben hinsichtlich der Betroffenenrechte nach Art. 12-23 DSGVO viele offene Fragen, die für den Unternehmensalltag von enormer Bedeutung sind. Klärung bringen nach und nach behördliche und gerichtliche Entscheidungen – einige aktuelle Entwicklungen stellen wir Ihnen in diesem Beitrag zusammen.

Unverzügliches Löschen nach Art. 17 DSGVO

Einen für die Praxis illustrativen Hinweis zum Löschungsanspruch nach Art. 17 DSGVO bringt eine Entscheidung der schwedischen Datenschutzaufsichtsbehörde (hier in englischer Sprache abrufbar). Nach Art. 17 DSGVO sind die personenbezogenen Daten des Betroffenen auf dessen Verlangen hin durch den Verantwortlichen

„unverzüglich“ zu löschen, soweit kein Erlaubnisgrund für die weitere Verarbeitung vorliegt.

Aber wann erfolgt eine Löschung „unverzüglich“? Laut der schwedischen Behörden sind **16 Tage** noch ausreichend. Ein solches Zeitfenster erfordert zwar unmittelbares Handeln, gibt aber dabei noch Luft für die notwendige Prüfung, ob das Löschungsbegehren gerechtfertigt ist.

Art. 17 DSGVO enthält keine starre Frist. Je nach Einzelfall kann ein „unverzügliches Handeln“ auch ein schnelleres Handeln erfordern oder ein größeres Zeitfenster erlauben. Dabei ist eine Anlehnung an das deutsche Rechtsverständnis möglich, nach dem unverzüglich handelt, wer ohne schuldhaftes Zögern tätig wird.

Welche Daten nach Art. 20 DSGVO zu übertragen sind

Nach Art. 20 DSGVO haben betroffene Person das Recht, eine Übertragung der sie betreffenden personenbezogenen Daten zu verlangen. Dieses Recht umfasst nur solche Daten, die die Betroffenen dem Verantwortlichen bereitgestellt haben.

Das VG Weimar hat dies jüngst bestätigt und konkretisiert: Ein Antragsteller hatte von der zuständigen Behörde Übertragung seiner Approbationsurkunde und Verifizierung derselben verlangt. Der Antragsteller hatte der Behörde zuvor Namen und Geburtsdatum übermittelt, anhand derer die Behörde verifiziert hat, ob eine Approbation vorliegt, und sodann die entsprechende Approbationsurkunde ausgestellt hat. Der Antragsteller konnte aus Art. 20 DSGVO weder Übertragung der Approbationsurkunde, noch des Verifizierungsergebnisses verlangen: Beides sind keine Daten, die der Betroffene der Behörde bereitgestellt hatte; für die Übermittlung der Approbationsurkunde bestehen zudem landesrechtliche Spezialvorschriften (vgl. Beschluss vom 02.03.2021 – Az. 2 E 209/21).

Identifizierungspflicht

Auskunft, Löschung und Übertragung von Daten – die Betroffenenrechte der Art. 15 ff. DSGVO müssen und dürfen Verantwortliche nur erfüllen, wenn sie die Anspruchsteller eindeutig als diejenigen identifizieren können, deren personenbezogenen Daten sie verarbeiten. Es gilt die sog. Identifizierungspflicht. Diese schließt aus, dass

ein beliebiger Dritter über Auskunftsrechte u.a. mit den Daten anderer nach Belieben verfahren kann. Feste Vorgaben an ein Procedere kennt die DSGVO allerdings nicht.

Ist in der Praxis eine Person mit den überlassenen Daten nicht eindeutig identifizierbar, sind weitere Angaben zur Identifizierung anzufordern. Dies ist z.B. der Fall, wenn ein Newsletterabonnent Auskunft verlangt, aber seine E-Mail-Adresse nicht benennt, unter der er den Newsletter bezieht. Der Verantwortliche sollte den Anspruchsteller dann auffordern, die E-Mail-Adresse anzugeben und die Auskunft sodann an diese E-Mail-Adresse übersenden.

Die Anforderungen an die Identifizierung dürfen nicht überspannt werden, wie ein aktuelles Beispiel des österreichischen Bundesverwaltungsgerichts zeigt (Entscheidung vom 21.06.2021): Ein Vereinsmitglied begehrte die Kündigung seiner Mitgliedschaft nebst Löschung seiner personenbezogenen Daten. Während die Kündigung umgesetzt wurde, lehnte der Verein das Löschbegehren ab mit der Begründung, die Identität des Betroffenen sei nicht hinreichend geklärt. Man brauche noch eine Ausweiskopie, um dem Löschbegehren nachzukommen. Trotz händischer Unterschrift auf Kündigung und Löschbegehren könne nicht ausgeschlossen werden, dass dieses nicht vielleicht auch von einer anderen Person stamme. Besonders hohe Hürden gelten dann, wenn Auskunft über sensible Daten nach Art. 9 DSGVO verlangt wird, also bspw. Auskunft über Gesundheitsdaten. Hier wird im Regelfall nur eine persönliche Aushändigung gegen eindeutigen Identitätsnachweis in Betracht kommen.

Eine solches Verlangen ging dem Gericht zu weit: Es sei nicht ersichtlich, warum die schriftliche Löschaufforderung mit händischer Unterschrift nicht ausreiche, um den Betroffenen mit hinreichender Sicherheit zu identifizieren. Hat der Verein im Hinblick auf die Kündigung nicht an der Identität gezweifelt, könne er dies auch bei der Löschung von Daten nicht vorbringen.

Keine Daten nur zur Identifizierung

Für den umgekehrten Fall regelt die DSGVO: Personenbezogene Daten sind nicht nur aufzubewahren, um Personen identifizieren und dann die Betroffenenrechte erfüllen zu können. Bekanntes Praxisbeispiel sind die Einwilligungen auf Websites: Diese werden über „Consent-Cookies“ gespeichert. Verlangt ein Betroffener Auskunft

beim Websitebetreiber, etwa unter Angabe seines Namens und seiner E-Mail-Adresse, kann der Websitebetreiber nicht erkennen, ob dieser Betroffene eingewilligt hat. Die DSGVO regelt, dass dies auch nicht sein muss: Ein Consent-Cookie reicht aus. Es ist nicht erforderlich (und wäre wohl sogar unzulässig), bei jeder Website-Einwilligung Name und E-Mail-Adresse abzufragen, nur, um spätere Anfragen beantworten zu können.

Die Pflicht zur Identifizierung dient also der Lösung einer Konfliktlage zwischen Betroffenenrechten und dem Grundsatz der Datenminimierung, nach dem die zu verarbeitenden Daten auf das für die Zwecke der Verarbeitung notwendige Maß zu beschränken sind. Es gilt, eine Balance zu finden zwischen der Erfüllung der Betroffenenrechte einerseits und der Vermeidung der Preisgabe zusätzlicher Daten andererseits. Beide Aspekte sind Ausfluss einer effektiven Durchsetzung der DSGVO. Eine Speicherung personenbezogener Daten „auf Vorrat“, um direkt auf mögliche Auskunftsersuchen reagieren zu können, ginge zu weit (EG 64, S. 2).

Neue DPAs von AWS und Microsoft: Ist jetzt alles gut?

AWS und Microsoft haben in den letzten Wochen neue Verträge zur Datenverarbeitung veröffentlicht („data processing agreement/addendum", kurz „DPA"). Damit gelten für die Angebote dieser beiden großen Dienstleister jetzt insbesondere die neuen Standardvertragsklauseln. Sind damit alle „US-Probleme" gelöst? Ganz so einfach ist es nicht.

Worum geht es?

Für viele von Ihnen ist es inzwischen der tägliche Begleiter: Risikohinweise bei einem Datentransfer in die USA. Kaum ein größeres Reizthema begleitet die Datenschützer nun seit über einem Jahr. US-Dienstleister können kaum ohne Datenschutzrisiko genutzt werden, denn zumindest für Support-Dienstleistungen greifen fast alle von ihnen aus den USA heraus auf die Kundendaten zu. Und in den USA ist, so der EuGH im vergangenen Jahr, ein angemessenes Datenschutzniveau ohne eine – nicht absehbare – politische Lösung kaum mehr zu erreichen. Das ist eine Patt-Situation. Denn ohne US-Dienstleister kann kaum ein Unternehmen wirtschaften. EU-Lösungen sind in der gleichen Praktikabilität schlicht nicht flächendeckend verfügbar.

Was tun?

In der Praxis ist die Risikominimierung das zu erreichende Ziel. Grundlage für die Absicherung des Datenschutzniveaus (und damit der Einhaltung der DSGVO) sind in den meisten Fällen die sog. Standardvertragsklauseln (oder auch: Standarddatenschutzklauseln) der EU-Kommission. Diese mussten in den letzten Monaten dann jeweils umfangreich mit „zusätzlichen Maßnahmen" ergänzt werden, um den Anforderungen des EuGH möglichst gut zu entsprechen. Je nach genutztem US-Dienst können etwa Daten hochwirksam verschlüsselt oder so pseudonymisiert werden, dass der US-Dienstleister (und auch die US-Geheimdienste) diese keiner Person zuordnen können. Das ist aufwendig und nicht immer eine umsetzbare Lösung.

Im Juni hat die EU-Kommission neue Standardvertragsklauseln veröffentlicht („Standard Contractual Clauses", kurz „SCC"). Viele von den nach der EuGH-Entscheidung im Sommer 2020 entwickelten „zusätzlichen Maßnahmen" für einen besseren Datenschutz sind implementiert. Das betrifft z.B. Informations- und Abwehrpflichten, wenn Geheimdienste aus dem Drittstaat auf Daten zugreifen wollen.

Enthalten sind jetzt auch Dokumentationspflichten, was das nationale Recht im Drittstaat überhaupt zulässt und erlaubt an Datenzugriffen.

Seit dem 27.09.2021 müssen für alle neuen Verträge mit Drittstaatentransfer diese neuen SCC 2021 verwendet werden. Altverträge können noch bis Dezember 2022 umgestellt werden.

Rechtssicher ist ein Drittstaatentransfer auch mit den neuen SCC 2021 nicht ohne weiteres. Die neuen Klauseln helfen aber ungemein, Rechtssicherheit zu erreichen.

Und was ist jetzt mit AWS und Microsoft?

Amazon Web Services Inc. („AWS") und Microsoft haben in den letzten Tagen neue Datenschutzvereinbarungen veröffentlicht. Die DPA sind kein eigener Vertragstyp, sondern enthalten die Regelungen zur Auftragsverarbeitung nach Art. 28 DSGVO und Standardvertragsklauseln für den Drittstaatentransfer. Letztere sind notwendig, da beide Unternehmen i.d.R. zumindest aus den USA heraus im Support-Fall auf personenbezogene Daten zugreifen können. Ohne gesonderte Einstellung werden die in den Cloud-Diensten der beiden Anbieter abgelegten Daten auch außerhalb der EU und des EWR gespeichert. Die vertragliche Vereinbarung des DPA ist damit verpflichtend, um überhaupt datenschutzkonform agieren zu können.

Die augenfälligste Neuigkeit der beiden DPA: Es gelten jetzt die SCC 2021. Der frühe Umstieg war notwendig, da die SCC 2021 für alle jetzt neu abgeschlossenen Verträge zwingend ist.

Wann gelten die neuen DPA von AWS und Microsoft?

Neukunden, die erstmals Verträge mit AWS und Microsoft über Cloud-Dienstleistungen, also z.B. auch Microsoft 365 oder Office 365 abschließen, schließen damit auch die neuen DPA ab.

Für Bestandskunden behält sich AWS weitreichende Änderungsrechte vor. Regelmäßig genügt schon eine Information über neue Vertragsregelungen und die Weiternutzung durch den Kunden, damit AWS von einer Vertragsänderung ausgeht. Vertragsrechtlich gibt es durchaus Fragezeichen, ob dies möglich ist. Für die Vereinbarung des neuen DPA aber hilft dies, da sich die Rechtssicherheit für die

Kunden erhöht, letztlich zu seinem Vorteil ist und soweit ersichtlich auch keine Mehrkosten hervorgerufen werden.

Microsoft regelt in seinen DPA, dass jeweils die beim erstmaligen Erwerb eines Produkts geltende Fassung vereinbart wird. Auch ist vorgesehen, dass bei Updates jeweils auch gleich die neue Vertragsfassung mit vereinbart wird, jedenfalls für die betroffenen Produktteile: Der Kunde stimmt dem nach den Microsoft-Vorstellungen also letztlich mit Installation zu. Um die SCC 2021 als Bestandskunde von Microsoft zu aktivieren, ist also eine derartige Änderung erforderlich, solange Microsoft nicht aktiv eine Vertragsänderung einleitet. Dies ist nach den Vertragsregelungen von Microsoft regelmäßig bei hoheitlichen Vorgaben ohne weiteres möglich. Für die SCC 2021 werden also vermutlich spätestens im Dezember 2022 auch Bestandskunden von Microsoft „aktiviert".

Und was gilt inhaltlich?

Inhaltlich halten beide Anbieter die Regelungen kurz: Die SCC 2021 werden nicht wiederholt, sondern es wird nur auf sie verwiesen. Microsoft sieht die Anwendung des Moduls „Auftragsverarbeiter zu Auftragsverarbeiter" vor, weil die Daten von der irischen Microsoft-Gesellschaft, die Auftragsverarbeiterin der Kunden ist, an einen Unterauftragnehmer in den USA übermittelt werden. AWS überlässt es dem Kunden, welches Modul gilt: Je nachdem, ob der Kunde selbst Auftragsverarbeiter oder Verantwortlicher ist, gilt das Modul „Auftragsverarbeiter zu Auftragsverarbeiter" oder aber „Verantwortlicher zu Auftragsverarbeiter", da AWS immer aus Auftragsverarbeiter auftritt.

Dem Leitgedanken der SCC 2021 entspricht dies nicht. Die Kommission sieht vor, dass diese Klauseln explizit vereinbart werden zwischen den Parteien. Ob das wirklich nötig ist, ist noch offen.

Allerdings besteht ein anderes Hindernis für diese Lösung: Die SCC 2021 verlangen etliche Dokumentationspflichten. Datenimporteure wie AWS und Microsoft müssen den Kunden unterstützen bei der Aufbereitung des nationalen Rechts der Drittstaaten und die Einhaltung der Klauseln dokumentieren. Das alles ist mit einem bloßen Verweis auf die SCC 2021 nicht getan. Der EuGH hat im vergangenen Jahr dieser Praxis ausdrücklich eine Absage erteilt. Die neuen DPA von AWS und Microsoft alleine genügen damit nicht, um den Anforderungen der SCC 2021 zu genügen. Ergänzend müssten die beiden

Unternehmen mindestens Informationen bereitstellen über das nationale Recht in den Drittstaaten, in denen sie die Daten verarbeiten. Kunden müssten dies aus datenschutzrechtlicher Sicht verlangen. Vertragsrechtlich kann man sicher darüber streiten, ob die Angaben nicht proaktiv bereitgestellt werden müssen.

Was darüber hinaus die Regelungen für die Auftragsverarbeitung anbelangt, sind beide DPA denkbar kurz. Sie regeln die Pflichten von AWS und Microsoft bei der Auftragsverarbeitung weit unterhalb der Regelungsdichte, die die Kommission in ihrem neuen Muster für einen Vertrag nach Art. 28 DSGVO vorgelegt hat. Verpflichtend ist das neue Muster von der Kommission nicht. Ob aber die vage gehaltenen Pflichten von AWS und Microsoft ausreichen, wird in den nächsten Monaten weiter zu diskutieren sein. Zweifel daran bestanden schon bisher, bevor die Kommission ihr umfangreiches Muster veröffentlicht und damit auch international neue Standards gesetzt hat.

Zu guter Letzt

Auch in den letzten Wochen gab es wieder einige spannende News: Das UK will die Cookie-Banner abschaffen. Der HamBfDI hat Vattenfall mit einem Bußgeld wegen unzureichender Informationen von abgelehnten Kunden belegt. Und in Italien sorgte eine Fernüberwachungssoftware, mit der Studierende bei Prüfungen überwacht wurden, für Aufsehen. Zu guter Letzt gab es Prüfungen rund um die Modernisierung von Parkuhren und den Datentransfer von Mautstationen. Bemerkenswert: Fast alle Bußgelder wurden wegen unzureichender Betroffeneninformationen verhängt.

- **UK möchte Cookie-Banner abschaffen**

Im Vereinigten Königreich wird derzeit über eine Abschaffung der Cookie-Banner diskutiert, da viele Nutzer bei Cookie-Bannern gleichgültig auf „Akzeptieren" klicken würden, anstatt sich mit den genauen Optionen zu beschäftigen. Um dieses Problem zu lösen, stellt die britische Regierung zwei Optionen zur Diskussion, die aus der Debatte um die ePrivacy-Verordnung wohl bekannt sind: Analyse-Cookies und ähnliche Technologien könnten allgemein ohne Einwilligung des Nutzers erlaubt werden. Oder aber Unternehmen könnte es allgemein erlaubt werde, ohne Einwilligung Daten vom Nutzer-Endgerät zu verarbeiten, soweit dafür berechtigte Interessen vorliegen. Beide Optionen sind nicht revolutionär, Option 1 findet sich im aktuellen ePrivacy-Verordnungsentwurf. Ob dadurch die Cookie-Banner verschwinden, ist indes mehr als fraglich: Für Tracking-Cookies und damit die meisten Marketing-Tools müssten weiterhin Einwilligungen eingeholt werden und dafür würden weiterhin Cookie-Banner benötigt.

- **Bonus-Hopper im Energiesektor: 900.000 Euro wegen unzureichender Informationen**

Der HamBfDI verhängt gegen das schwedische Energieunternehmen Vattenfall Europe Sales GmbH ein Bußgeld in Höhe von über 900.000 Euro. Der Vorwurf: Vattenfall prüfte bei Vertragsanfragen, die mit Bonuszahlungen verbunden waren, routinemäßig, ob die potentiellen Neukunden in der Vergangenheit bereits Vertragspartner waren – ohne diese über die Prüfung zu informieren. Kunden, die schon einmal Energie von Vattenfall bezogen hatten, wurden als potentielle „Bonus-Hopper" (Kunden, die häufig Strom- und Gasunternehmen wechseln, um günstige Verträge mit Boni zu nutzen) abgelehnt. Für diesen Abgleich nutzte Vattenfall Rechnungen

aus früheren Vertragsbeziehungen mit besagten Kunden, die nach steuer- und handelsrechtlichen Vorgaben ohnehin für bis zu zehn Jahre aufbewahrt werden mussten.

Spannend: Geahndet wurde ausschließlich ein Verstoß gegen die Informationspflichten (Art. 12-14 DSGVO). Eine unerlaubte Datenverarbeitung (zweckfremde Verwendung der aus handels- und steuerrechtlichen Gründen gespeicherten Daten) wurde nicht festgestellt – hier bleibt also Spielraum.

- **Frankreich: 1,75 Mio. Euro wegen zu langer Datenspeicherung und unzureichender Informationen**

Die französische Datenschutzbehörde verhängte gegen das französische Unternehmen AG2R LA MONDIALE ein Bußgeld in Höhe von 1,75 Mio. Euro. Während ihrer Inspektion des Unternehmens stellte die Datenschutzbehörde fest, dass das Versicherungsunternehmen die Daten von mehr als zwei Millionen Personen über einen übermäßig langen Zeitraum (länger als drei oder fünf Jahre) aufbewahrte, einschließlich einiger Gesundheits- und Bankdaten. Die gesetzlich zulässigen Aufbewahrungsfristen über das Vertragsende hinaus seien überschritten worden. Zudem seien bei Telefonkampagnen kontaktierte Personen nicht hinreichend darüber informiert worden, dass das Telefongespräch aufgezeichnet wurde.

- **Italien: 800.000 Euro aufgrund einer Parkuhrmodernisierung mit Nummernschilderfassung**

Die Stadt Rom muss ein Bußgeld in Höhe von 800.000 Euro zahlen, da der Betrieb von einigen Parkuhren gegen die DSGVO verstoße. Um keine Tickets mehr vorzeigen zu müssen, wurden einige der Verwaltung unterstehende Parkuhren im Rahmen einer Modernisierung dahingehend modifiziert, dass die Nutzer zur Personalisierung von Zahlungen ihre Nummernschilder in die Parkuhr eingeben müssen. Diese Daten sowie auch die Uhrzeit, das Anfangs- und Enddatum des Halts und den gezahlten Betrag verarbeiteten die das System betreibenden Unternehmen sowie auch mehrere zwischengeschaltete Unternehmen. Weder seien die betroffenen Personen der DSGVO entsprechend angemessen informiert oder die datenschutzrechtliche Rolle der weiteren an der Verarbeitung beteiligten Unternehmen bestimmt worden, noch seien angemessene Sicherheitsmaßnahmen ergriffen oder die Speicherdauer der erhobenen Daten festgelegt worden.

- **Norwegen: 500.000 Euro wegen Datentransfers nach China für ein Mautunternehmen**

Das Unternehmen Ferde AS registriert die Pkw-Durchfahrten an ihren Mautstationen. Wenn ein Pkw ohne Mauttransponder durchfährt oder dieser nicht ordnungsgemäß registriert wird, wird ein Foto des Nummernschilds gemacht und zur automatischen optischen Erkennungsbearbeitung versendet. Reicht die Bildqualität hierfür nicht, wird das Bild zur manuellen Untersuchung an eine Firma weitergeleitet, die Mitarbeiter in China hat. Diese Weiterleitung betrifft jährlich etwa 12,5 Mio. Bilder. Aufgrund der Weiterleitung an Mitarbeiter in China werden die Daten gezwungenermaßen auch an das Drittland übertragen.

Die Datenbehörde erließ ein Bußgeld in Höhe von 499.373 Euro, da es an einer ausreichenden Auftragsverarbeitungsvereinbarung und hinreichenden Garantien für den Drittstaatentransfer gefehlt habe.

- **Italien: Unzulässiger Einsatz von Fernüberwachungssoftware bei Online-Prüfungen**

Gegen die private Wirtschaftsuniversität „Luigi Bocconi“ in Mailand wurde ein Bußgeld in Höhe von 200.000 Euro verhängt. Anlass war die Beschwerde eines Studierenden aufgrund eines während Online-Prüfungen verwendeten Überwachungssystems. Wegen der COVID-19-Pandemie sollten alternative Möglichkeiten zu Präsenzprüfungen mit ähnlichen Sicherheitsstandards zur Verfügung gestellt werden. Hierfür wurde die Fernüberwachungssoftware „Respondus“ des gleichnamigen Unternehmens eingesetzt. Das Unternehmen mit Sitz in den USA wurde als Auftragsverarbeiter für die Universität tätig. In zufälligen Intervallen wurden Videoaufnahmen und Screenshots von den Bildschirmen der Studierenden zwecks Identifizierung verdächtiger Verhaltensweisen gefertigt. Dabei wurden auch besonders sensitive biometrische Daten erfasst. Anschließend wurden die Aufnahmen manuell dahingehend untersucht, ob tatsächlich nicht erlaubte Handlungen begangen wurden.

Über den Einsatz von Respondus seien die Studierenden nicht ordnungsgemäß informiert worden. Daneben habe Respondus auch für den Verarbeitungszweck nicht erforderliche Daten erfasst und diese mit 12 Monaten länger als nötig gespeichert. Neben einem weiteren Verstoß der Universität gegen die Grundsätze der Datenminimierung und Speicherbegrenzung entbehre diese Verarbeitung

biometrischer Daten außerdem jeglicher Rechtsgrundlage. Als Voraussetzung zur Teilnahme an der Prüfung sei die Einwilligung der Studierenden nicht freiwillig erfolgt. Ferner fehlte eine Datenschutz-Folgenabschätzung der Hochschule, obwohl diese aufgrund des Risikos für die Betroffenen erforderlich gewesen sei, es fehlte an hinreichenden technischen Maßnahmen und trotz Unwirksamkeitserklärung durch das Schrems-II-Urteil des EuGH wurde die Verarbeitung weiterhin auf das EU-US-Privacy Shield Abkommen zwischen der EU und den USA gestützt.

- **Großbritannien: Bußgeld aufgrund unerbetener Werbenachrichten**

Die britische Datenschutzbehörde „Information Commissioner's Office" (ICO) hat ein Bußgeld in Höhe von 234.962 Euro gegen den britischen Autohändler „We Buy Any Car Limited" erlassen, weil dieses unerbetene Werbenachrichten via E-Mail und SMS ohne wirksame Einwilligung verschickt hatte.

Außerdem hat das ICO gegen den britischen Versicherer „Saga Services Limited" ein Bußgeld in Höhe von 176.222 Euro verhängt. Im Namen von Saga Services Limited wurden Werbe-E-Mails von Partnerunternehmen und Tochtergesellschaften des Unternehmens versandt. Für diese Direktmarketingkampagne wurden Kontaktlisten von Personen verwendet, von denen keine gültige Werbeeinwilligungen vorlagen. Im Vereinigten Königreich gelten mittlerweile nicht mehr die Regelungen der DSGVO. Stattdessen wurde eine inhaltlich weitgehend mit der DSGVO übereinstimmende UK-DSGVO erlassen, an der Unternehmen nunmehr ihren Datenschutz ausrichten müssen.

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