Sondernewsletter Datenschutz

Inhalt

Internationale Datenverarbeitung: Transfer Impact Assessments (TIA) und neue Standardvertragsklauseln (SCC)

I. Standardvertragsklauseln als Rechtfertigungsgrundlage für den internationalen Datenverkehr

Internationale Datentransfers – insbesondere in die USA, da das EU-US Privacy Shield „2.0“ noch auf sich warten lässt – müssen auf einen der gültigen Rechtfertigungsmechanismen im Sinne der DSGVO gestützt werden. Entscheidendes Instrument sind hier die EU-Standardvertragsklauseln (auch Standard Contractual Clauses – „SCC“). In Folge der Schrems-II Entscheidung ersetzte die Kommission im Juni 2021 die bisherigen SCC durch neue Versionen. Der Einsatz der neuen SCC wird ab dem 27. Dezember 2022 für neue Vereinbarungen, die (auch) personenbezogene Daten zum Gegenstand haben, verpflichtend. Ziel ist es, sicherzustellen, dass ein Datenschutzniveau gewährleistet wird, das dem der DSGVO entspricht. Vornehmlich geht es dabei um etwaige Datenzugriffe durch ausländische Behörden und die mangelnde Rechtsschutzmöglichkeit der Betroffenen in den jeweiligen Drittländern. Soweit kein angemessenes Datenschutzniveau im Drittland gewährleistet werden kann, sind zusätzliche Sicherheitsmechanismen zu ergreifen. Führt dies nicht zu einem maßgeblich verringerten Zugriffsrisiko, hat der Datentransfer zu unterbleiben.

Neben bürokratischen Schwierigkeiten liegt die besondere Herausforderung mit den neuen SCC in der nun notwendigen Risikoanalyse. Art. 14 der SCC normiert die Verpflichtung für Unternehmen, vor Abschluss der SCC ein sog. Transfer Impact Assessment („TIA“) hinsichtlich des Datenschutzniveaus im Drittland des Datenimporteurs durchzuführen. Im Rahmen der TIA wird u. a. das Risiko eines Zugriffs durch Dritte bei einem Datentransfer in Drittländern unter Berücksichtigung der Effektivität gegebener Abwehrmechanismen bewertet. Aufgezeigt werden soll so, inwieweit der Datenimporteur in der Praxis fähig ist, seinen Verpflichtungen aus den SCC nachzukommen.

II. Hilfestellungen der Aufsichtsbehörden

Durchzuführen ist das TIA von dem jeweiligen Datenexporteur, unabhängig von seinem Handeln als Verantwortlicher oder Auftragsverarbeiter. Erfolgt eine Weiterleitung der Daten durch den Datenimporteur an einen Subunternehmer, ist eine gesonderte Risikoeinschätzung durchzuführen. Aber was genau muss in einer TIA stehen?

Bisher gibt es noch nicht „das eine“ TIA-Formular, welches den Unternehmen zur Erfüllung ihrer gesetzlichen Pflicht an die Hand gegeben wird. Erste Indizien lieferte der Europäische Datenschutzausschuss (EDSA) mit seiner Veröffentlichung vom 18. Juni 2021 als Version 2.0 an Empfehlungen zur Umsetzung des Schrems II-Urteils (Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data). Unternehmen erhalten damit jedoch kaum Klarheit hinsichtlich der genauen Anforderungen an die Erstellung einer TIA, da es an einem konkret greifbaren Prüfkatalog mangelt. Ba-

sierend auf den verschiedenen Aussagen der Datenschutzbehörden und den bereits veröffentlichten Dokumenten kann jedoch grundsätzlich ein Muster für die TIA erstellt werden. Luther hat in diesem Rahmen ein eigenes Prüfschema entwickelt, das nachfolgend in Auszügen dargestellt wird:

III. Checkliste TIA

Für die Durchführung eines TIA empfiehlt sich dabei ein standardisierter Ansatz anhand von vier Prüfungsschritten:

- **Schritt 1:** Im ersten Schritt ist zunächst eine genaue Beschreibung des beabsichtigten Datentransfers erforderlich. Dazu gehören neben den in Rede stehenden Verarbeitungsprozessen auch die Kategorien der zu verarbeitenden Daten, etwa die Zwecke der Datenverarbeitung, die Kategorien von Betroffenen und technische Details zur Umsetzung des Datentransfers.

- **Schritt 2:** Im Hinblick auf die Parameter zur Risikoidentifikation ist vor allem die Betrachtung der Rechtslage des Drittlandes, in das die Daten übermittelt werden und die dortigen Rechtsgrundlagen, die einen Zugriff der Behörden des Drittlands ermöglichen können, von Relevanz. Ebenso ist das Bestehen von Verpflichtungen zur Offenlegung von Verschlüsselungsmechanismen gegenüber staatlichen Stellen zu berücksichtigen. Daneben ist zu hinterfragen, ob in dem betroffenen Drittland Informationspflichten gegenüber und effektive Rechtsmittel für die Betroffenen bestehen.

- **Schritt 3:** Risikominimierend können sich etwaige bestehende Sicherheitsvorkehrungen auswirken. In Betracht kommen z. B. geeignete Transport- bzw. Ende-zu-Ende Verschlüsselungen der personenbezogenen Daten bei der Übermittlung. Wichtig ist, nicht nur Maßnahmen festzulegen, sondern diese auch in der Praxis umzusetzen. Dazu gehört auch die Kontrolle der Maßnahmen: ergriffene Abhilfemaßnahmen sollten fortlaufend getestet und deren Wirksamkeit dokumentiert werden. Stellt sich zu einem späteren Zeitpunkt heraus, dass geplante Maßnahmen nicht (wirksam) realisiert werden können, müssen andere geeignete Maßnahmen ausgewählt oder die Übermittlungs- und Verarbeitungsvorgänge insgesamt angepasst werden.

- **Schritt 4:** Soweit auf Basis der vorgenannten Kriterien ein Datenzugriff durch Behörden des Drittlands nicht vollständig ausgeschlossen werden kann, ist sodann in einem letzten Schritt die abschließende Risikobewertung selbst vorzunehmen. Im Kern ist das Risiko eines Zugriffs durch Dritte im Drittland, der nicht im Einklang mit den Grundsätzen der DSGVO steht zu identifizieren und zu bewerten. Die Evaluation ist länderspezifisch und verarbeitungsspezifisch durchzuführen. Berücksichtigung finden kann die geltende Praxis der Behörden sowie frühere Erfahrungen der Beteiligten.

IV. Handlungsempfehlung

Aufgrund der Vielzahl von Datenverarbeitungsprozessen und dem üblichen Einsatz diverser Auftragsverarbeiter ist klar, dass die Erstellung einer TIA kein einmaliger Vorgang ist. Es sind neue Prozesse zu definieren und eine kontinuierliche Überprüfung und Anpassung der Risikoeinschätzung ist vorzunehmen. Angesichts des Arbeitsaufwands und des für die Lagebewertung in den Drittländern nötigen Fachwissens stellt der Pflichtenkatalog für Unternehmen eine große Hürde dar. Schwierigkeiten bestehen vor allem darin, Veränderungen in allen relevanten Drittländern im Auge zu behalten. Realistisch werden Unternehmen zumeist auf Auskünfte und eine Überwachung der Rechtslage durch die Datenimporteur und/oder zu beauftragende Rechtsbeistände im Drittland angewiesen sein. Hier empfiehlt es sich, den Datenimporteur seinerseits zu einer Überwachung der Rechtslage zu verpflichten. Fraglich bleibt, ob Unternehmen in Drittstaaten in der Praxis zur Transparenz sowie zum Aufbürden von teils weitreichenden zusätzlichen Verpflichtungen bereit sein werden.

V. Ausblick

Der internationale Datenverkehr stellt Unternehmen nach der Schrems-II Entscheidung wieder einmal vor erhebliche Schwierigkeiten. Eine Erhöhung des US-Datenschutzniveaus und eine baldige Neuauflage des EU-US-Privacy Shields als Übermittlungsinstrument ist nicht zu erwarten. An der Vereinbarung der SCC und der Durchführung einer TIA scheint damit bei der internationalen Datenverarbeitung momentan kaum ein Weg vorbeizuführen. Es bleibt abzuwarten, welchen Maßstab die europäischen Datenschutzbehörden bei der Überprüfung der TIAs zugrunde legen werden.

Update zum Drittlandtransfer in die USA: „Privacy Shield Reloaded“

Mit der Einigung zwischen EU und USA rückt eine Nachfolgevereinbarung des überkommenen „Privacy Shield“ wieder ein Stück näher.

Datenverarbeitungen könnten damit in naher Zukunft wieder auf sicherer Grundlage als in der jüngsten Vergangenheit erfolgen. Konkret würde eine Lockerung im Hinblick auf die Erforderlichkeit geeigneter Garantien für ein angemessenes Datenschutzniveau bei Verarbeitungen mit Transfer in die USA einhergehen (etwa Verwendung der neuen Standardvertragsklauseln). Zentraler Aspekt dieser Vereinbarung sollen die Grenzen für den Zugriff durch US-Geheimdienste und der Rechtsschutz für betroffene EU-Bürgerinnen und -Bürger sein. Dieses soll zukünftig in einem zweistufigen System Niederschlag finden, der ein ausreichendes Schutzniveau gewährleisten soll. Daneben beabsichtigen die EU und die USA, den Mechanismus für die Selbstzertifizierung von datenimportierenden US-Unternehmen weiterhin zu verwenden.

Wie es weiter geht:

- Datenverarbeitungen mit Transfer in die USA können zunächst weiterhin nur unter Abschluss der Standardvertragsklauseln sowie zusätzlicher Garantien erfolgen.
- Fortschreibung des Prozesses über eine Nachfolgevereinbarung:
  - Verschriftlichung und Akzeptanz der Vereinbarung
  - Umsetzung der Vorgaben durch die USA in innerstaatliches Recht
  - Erstellung eines Angemessenheitsbeschlusses durch die EU
  - Stellungnahme des Europäischen Datenschutzausschusses
  - Angemessenheitsbeschluss der EU

Neue EU-Standardvertragsklauseln nun auch für Datentransfers aus UK

I. Überblick

Am 21. März 2022 sind im Vereinigten Königreich (UK) zwei neue Datenübermittlungsmechanismen in Kraft getreten, die eine zeitgemäße und vereinfachte Übermittlung in Drittländer ermöglichen. Unternehmen, die in UK ansässig sind und personenbezogene Daten in Länder wie z. B. die USA übermitteln, müssen nun ihre Verträge anpassen.

Die EU-Standardvertragsklauseln (EU SCCs) stellen das am häufigsten verwendete Instrument dar, um einen internationalen Datentransfer von der EU in Drittländer zu legitimieren. Die von der EU entwickelten Vertragssets bieten Garantien für Datenübermittlungen, wenn sie zwischen den an dem Datentransfer Beteiligten vereinbart werden. Im Juni 2021 hat die EU neue SCCs eingeführt, die die bisherigen SCCs bis Dezember 2022 für Datentransfers aus der EU vollständig ablösen. Wegen des Brexits gelten diese allerdings nicht direkt für UK und wurden von der UK-Datenschutzaufsicht ICO bisher nicht für Datenübermittlungen nach UK-Datenschutzrecht anerkannt. Hierfür mussten weiterhin die alten EU SCCs abgeschlossen werden. Dieser Flickenteppich wurde nun beseitigt.

II. UK Addendum und IDTA

Die UK-Datenschutzaufsicht ICO hat eine flexible Herangehensweise vorgestellt: In UK ansässige Unternehmen können in Zukunft entweder die neuen EU SCCs mit einer speziellen Anlage für UK-Datentransfers („UK Addendum“) verwenden oder eine eigenständig für UK entwickelte Vereinbarung, das sog. International Data Transfer Agreement („IDTA“) abschließen.

Die Verwendung des UK Addendum bietet sich insbesondere an, wenn Unternehmen bei Datentransfers sowohl die UK- als auch die EU-Regelungen zum Datenschutz beachten müssen. Typischer Anwendungsbereich sind Datenübermittlungen innerhalb von Unternehmensgruppen (über sog. Intragroup Data Transfer Agreements) und Übermittlungen aus UK, die ebenfalls EU-Bezug aufweisen. Unter anderem in diesen Fällen ist es nun einfach möglich, zu den EU SCCs das UK Addendum abzuschließen, um auch die Vorgaben in UK zu erfüllen.

Für reine Datentransfers eines lokalen englischen Unternehmens kann hingegen der Abschluss des IDTA sinnvoller sein. Es ist jedoch zu erwarten, dass international tätige Dienstleister in den von ihnen angebotenen Verträgen eher auf das UK Addendum abstellen werden, da dieses an die bereits bekannten EU SCCs anknüpft und dieses Vorgehen den Umsetzungsaufwand minimiert.

III. Hinweise zur Anwendung des UK Addendum

Das UK Addendum enthält viele Änderungen zu den EU SCC. Augenscheinlich sind dort weitreichend Rückmeldungen aus dem im Herbst 2021 durchgeführten Konsultationsverfahren eingeflossen. Von Vorteil ist die hohe Flexibilität, die das UK Addendum bietet. Es kann als eigenständiges Dokument abgeschlossen oder in eine andere Vereinbarung mit aufgenommen werden. Unterschriften der Parteien im UK Addendum selbst sind ebenfalls nicht zwingend erforderlich, solange das UK Addendum in einer verbindlichen Weise geschlossen wird, so z. B. als Anlage zu einer anderen Vereinbarung. Das UK Addendum kann dem zwischen zwei Parteien zu vereinbarenden jeweiligen Modul der EU SCCs beigefügt werden oder diese nur einbeziehen. Daneben kann der zweite Abschnitt des UK Addendum durch eine Verweisung auf das Musterdokument ersetzt werden. Durch diese Möglichkeiten kann der Anwender entscheiden, nur die zwingend erforderlichen Angaben aufzunehmen und dadurch die Regelungen sehr kurz zu halten. Die Aufsichtsbehörde ICO hat angekündigt, zeitnah Leitfäden zu den neuen Übermittlungsmechanismen herauszugeben, die voraussichtlich auf der Webseite der ICO veröffentlicht werden.

In der Praxis ist daneben zu berücksichtigen, dass bei Verwendung der neuen EU SCCs für Datentransfers auch aus UK eine Risikoanalyse des jeweils geltenden Datenschutzniveaus im Drittland (sog. „Transfer Impact Assessment“ oder „TIA“) von den Vertragsparteien durchgeführt werden soll (Blogbeitrag zum Thema).

IV. Welche Umstellungsfristen gelten?

Seit dem 21. März 2022 können das UK Addendum oder das IDTA verwendet werden. Für einen Übergangszeitraum bis zum 21. März 2024 können die alten EU SCCs in UK weiter verwendet werden, soweit die zugrunde liegenden Verarbeitungsvorgänge sich nicht ändern. Ab dem 21. September 2022 müssen Unternehmen für neue Vereinbarungen sowie Vertragsänderungen das IDTA oder die neuen EU SCCs mit UK Addendum abschließen.

Für Datenübermittlungen aus der EU endet die Umsetzungsfrist für die Umstellung auf die neuen EU SCCs am 27. Dezember 2022, sodass es sich anbietet, in diesem Zeitraum auch direkt die Umstellung für UK mit vorzunehmen. Dies empfiehlt sich auch vor dem Hintergrund, dass die alten EU SCCs ein niedrigeres Datenschutzniveau bieten, als dies durch die neuen Klauseln ermöglicht wird. Eine zeitnahe Umsetzung auch für UK ist daher von Vorteil, um Datentransfers in Länder außerhalb der EU bzw. des EWR besser abzusichern.

Die folgende Grafik zeigt die Zeitachse für die Umstellung:

Auskunftsrecht nach Art. 15 DSGVO

I. Reichweite des datenschutzrechtlichen Auskunftsanspruchs

Seit Einführung der DSGVO im Mai 2018 ist die Reichweite des datenschutzrechtlichen Auskunftsanspruchs des Art. 15 DSGVO umstritten. Insbesondere ist bislang nicht geklärt, ob das Recht auf Auskunft (Abs. 1) und das Recht auf Erhalt einer Kopie der personenbezogenen Daten (Abs. 3) einen einheitlichen Anspruch bilden oder ob es zwei unterschiedliche Ansprüche sind. Speziell diese Abgrenzung ist jedoch von hoher praktischer Relevanz, weil sich für Verantwortliche die Frage stellt, ob sie im Falle der Geltendmachung eines Anspruchs auf Kopie (Abs. 3) diesen durch Übermittlung einer abstrakten Zusammenstellung der verarbeiteten Daten erfüllen können, also einer Kopie der Daten selbst, oder ob sie die Dokumente übermitteln müssen, welche die personenbezogenen Daten enthalten.

II. Bisherige Rechtsprechung

Die Rechtsprechung zur Auslegung von Art. 15 DSGVO ist nicht einheitlich.[1] In seinem Urteil vom 15.6.2021 bezog der BGH erstmalig zum Umfang des Auskunftsanspruch des Art. 15 DSGVO Stellung und bestätigte, dass die Norm einen sehr weiten Anwendungsbereich hat.[2] Ferner sei der Begriff der personenbezogenen Daten weit zu verstehen und umfasse auch interne Korrespondenz. Zwar bezieht der BGH bezüglich der rechtsdogmatischen Einordnung des Auskunftsrechts und des Rechts auf Kopie nicht explizit Stellung. Jedoch ist aus seinem Begriffsverständnis von personenbezogenen Daten und dem Inhalt der Entscheidung zu entnehmen, dass der BGH der Auffassung ist, dass Abs. 3 auch die Übermittlung von Kopien konkreter Dokumente erfasst.[3]

III. Leitfaden des EDSA

Der europäische Datenschutzausschuss (EDSA) veröffentlichte am 18. Januar 2022 seine Leitlinie 01/2022 zum Auskunftsrecht.[4] In dieser Leitlinie stellt er den Umfang des Auskunftsrechts und die Anforderungen an die Verantwortlichen dar. Die Reichweite des Auskunftsrecht ist auch nach Verständnis der EDSA sehr weit und umfasst grundsätzlich alle personenbezogenen Daten (z. B. vorhandene Papierdokumente, Gesprächsnotizen und Gesprächsaufzeichnungen, Aktivitätsprotokolle, Suchverläufe, Log-Files, IT-Vorfallsberichte). Nach Auffassung des EDSA ist das Auskunftsrecht in drei Bereiche aufzuteilen:

- Bestätigung darüber, ob personenbezogene Daten der Person verarbeitet werden oder nicht,
- Auskunft über die personenbezogenen Daten und
- Auskunft über die Informationen über die Verarbeitung (siehe Auflistung des Art. 15 Abs. 1 DSGVO).

Grundsätzlich sind danach Anfragen, sofern nicht explizit weniger oder anderes gefordert, so zu verstehen, dass alle personenbezogenen Daten des Betroffenen angefordert werden. Der Verantwortliche muss also alle seine Datensysteme nach personenbezogenen Daten des Betroffenen durchsuchen. Das Recht auf Kopie sieht der EDSA, neben der Möglichkeit der mündlichen Auskunftserteilung und der Einsicht vor Ort, als wichtigste Modalität der Auskunft über die personenbezogenen Daten des Betroffenen. Auch er geht davon aus, dass Kopien sämtlicher die personenbezogenen Daten enthaltender Dokumente herauszugeben sind. Ferner kann es nach der Leitlinie einer detaillierten Beantwortung nicht entgegengehalten werden, dass diese für den Verantwortlichen aufgrund des Umfangs der Auskunft besonders aufwändig sei.

IV. Ausblick

Die Reichweite des Auskunftsanspruch nach Art. 15 DSGVO ist derzeit in verschiedenen Vorlagefragen durch den EuGH zu entscheiden. Es bleibt abzuwarten, ob der EuGH die strenge Auslegung des EDSA übernimmt.

---

1 LAG Baden-Württemberg NZA-RR 2021, 410 Rn. 47.; OVG Münster Urt. v. 8.6.2021 – 16 A 1582/20, BeckRS 2021, 13156

2 NJW 2021, 2726 (Urteil); NJW 2021, 2692 (Besprechung des Urteils)

3 NJW 2021, 2692 Rn. 11.

4 Guidelines 01/2022 on data subject rights - Right of access | European Data Protection Board (europa.eu)

Einwilligung nach TTDSG auf Webseiten

I. Überblick

Das TTDSG bündelt die wesentlichen Datenschutzvorschriften für Telekommunikations- und Telemediendienste einschließlich Nutzertracking. Das TTDSG richtet sich an Diensteanbieter. Dabei erfasst es in einem technologieneutralen Ansatz alle Techniken und Verfahren aus dem Bereich des Speicherns und Auslesens von Informationen (z. B. „Hidden Identifiers“, „Cookies“, „Browser Fingerprinting“ und „Spyware“). Ausreichend ist es, das die Technologie die informationelle Integrität des Endgeräts berührt, wobei es sowohl für Daten mit als auch ohne Personenbezug gilt.

II. Einwilligung

Ein Nutzertracking ist nur mit Einwilligung möglich. Für Webseiten-Betreiber ist eine Ausnahme in § 25 Abs. 2 Nr. 2 TTDSG geregelt: Wenn das Auslesen von Daten aus einer Endeinrichtung bzw. beim Speichern von Daten auf der Endeinrichtung des Nutzers technisch unbedingt für die Nutzung der Webseite erforderlich ist (z. B. bei Warenkorb-Funktion, Chat-Bots oder zur Authentifizierung), entfällt die Pflicht zur vorgeschalteten Einwilligung.

III. Vorgaben an die Einwilligung

Wichtig ist, dass der Nutzer der Endeinrichtung die Einwilligung vor dem einwilligungsbedürftigen Zugriff auf das Endgerät erteilt. Er muss bereits bei Zugriff die Kenntnis über Zugriffsform, Zugriffsperson und Zugriffszweck, konkrete Speicherdauer und daran anknüpfende Datenverarbeitungsprozesse haben.

Die Erklärung muss der Nutzer durch ein aktives Handeln in eindeutiger Weise (z. B. durch das Anklicken einer Schaltfläche) für den konkreten Fall vornehmen. Ob eine Erklärung eindeutig ist, entscheidet sich nach der konkreten Gestaltung. Unzureichend ist insbesondere,

- dass eine Wahlmöglichkeit stets eine höhere Anzahl an Klicks erfordert,
- das Verwenden einer Generaleinwilligung oder Blankoeinwilligung für jeglichen Einsatz einer Technologie,
- dass der Nutzer untätig bleibt, auf der Webseite verbleibt, oder bereits Kästchen angekreuzt sind (Opt-Out-Verfahren).

Schließlich müssen die Möglichkeit zum Widerruf und die Freiwilligkeit der Einwilligung gewährleistet sein. Bedenken bestehen mit Blick auf die Freiwilligkeit insbesondere bei

- Dark Patterns,
- der vollständigen Sperrung einer Webseite durch Cookie-Walls.

IV. Bündelung der Einwilligungserklärungen

Eine Bündelung der Einwilligung nach DSGVO und nach TTDSG ist zulässig nach jüngsten Ausführungen der DSK. Entscheidend ist, dass die Texte sowohl auf das Auslesen und Speichern nach TTDSG als auch die weiteren Verarbeitungen nach DSGVO als getrennte Vorgänge mit divergierenden Rechtsgrundlagen hinweisen.

V. Einwilligungsbanner

Die Erkennbarkeit und Nachvollziehbarkeit sind die entscheidenden Faktoren für ein zulässiges Einwilligungsbanner. Zwecke und beteiligte Akteure müssen erkennbar sein. Auch die Benutzeroberfläche (etwa der Effekt einer Schaltfläche oder die Kennzeichnung der unterschiedlichen Buttons) ist relevant. Ist das Banner verständlich, so muss es sich auch mit den Informationen der Datenschutzerklärung decken, da sonst deren übergeordnetes Zusammenspiel die Intransparenz erzeugt. Insbesondere sollten widersprüchliche Informationen vermieden werden.

VI. Einsatz einer Consent-Management-Plattform

Neben Cookie-Bannern greifen Unternehmen immer häufiger auf Consent-Management-Plattformen (CMP) zurück, die eine umfassende und rechtskonforme Einwilligungslösung versprechen. Letztgenannte Konformität steht und fällt mit dem konkreten Einsatz der CMP und den betroffenen Vorgängen. Nicht jede Konfiguration auf einer Webseite ist von der CMP abgedeckt. Da die Verantwortlichkeit für die Webseite beim Anbieter verbleibt, sollte ein CMP erst im Anschluss an eine am Einzelfall ausgerichtete Prüfung eingesetzt werden.

VII. Anwendung auf andere Technologien

Immer häufiger verwenden Unternehmen Messungen ohne Verwendung von Cookies an, um so den Vorgaben an die Einwilligung zu entgehen. Ein aktuelles Beispiel mit Praxisrelevanz bietet das Tool Matomo. Es bietet vereinzelt Konfigurationsmöglichkeiten, die eine Einwilligung entbehrlich machen können. Allerdings kann auch hier ein einwilligungsbedürftiges Nutzertracking vorliegen. Denn das TTDSG ist grundsätzlich technologieneutral. Exemplarisch ist das Aufspielen eines Java-Script-Code. Findet über dessen Einsatz ein zusätzliches Auslesen von Informationen des jeweiligen Endgeräts statt, kann nur eine wirksame Einwilligung einen Verstoß gegen das TTDSG sicher ausschließen.

Europäische Datenschutzbehörden: Google Analytics ist nicht mit Unionsrecht vereinbar

I. Hintergrund

Der rechtskonforme Einsatz von Google Analytics ist bereits seit einiger Zeit datenschutzrechtlich fraglich. Nun gibt es gleich zwei neuere Entscheidungen der österreichischen und französischen Datenschutzbehörden, die bestätigen, dass Google Analytics nicht DSGVO-konform ist, da es bei der Nutzung des Dienstes zu einer datenschutzrechtlich unzulässigen Übermittlung von personenbezogenen Daten in das Drittland USA kommt.

II. Datenverarbeitung mit Google Analytics

Für die Nutzung von Google Analytics muss der Webseitenbetreiber einen Programmcode in den Quelltext der Webseite einfügen. Der Programmcode verweist auf eine Datei, die auf das Gerät des Nutzers heruntergeladen wird (Cookie). Wird die Webseite von dem Nutzer eines Browsers aufgerufen, wird der Quelltext einschließlich des Programmcodes und des Cookies ausgeführt. Damit wird das Tracking gestartet und Informationen auf den Google Analytics Server übertragen. Hierzu zählen Informationen zur HTTP-Anfrage des Nutzers, zu den Systeminformationen sowie zu First-Party Cookies. Die Informationen umfassen u. a. Browsertyp, Browsereinstellung, Sprache, Farbtiefe, Bildschirmauflösung und IP-Adresse.

Da Google jedem Nutzer anhand der oben genannten Parameter eine eindeutige Kennnummer zuweist und die Nutzer anhand der gesammelten Daten im datenschutzrechtlichen Sinne identifizieren kann, handelt es sich bei diesen Datensammlungen um personenbezogene Daten. Insofern ist das Erstellen dieser Nutzerprofile datenschutzrechtlich nur dann zulässig, wenn der Nutzer eine wirksame Einwilligung (Opt-In) erteilt hat.

Entscheidender Kritikpunkt für die Datenschutzbehörden ist, dass die Voraussetzungen für einen datenschutzkonformen Transfer personenbezogener Daten in ein Drittland nicht eingehalten werden. Damit personenbezogene Daten aus der

Europäischen Union in ein Drittland übermittelt werden dürfen, müssen geeignete Garantien vorliegen, die gewährleisten, dass das EU-Schutzniveau für die personenbezogenen Daten durch die Übermittlung in ein Drittland nicht unterlaufen wird. Der EuGH fordert für den Datentransfer in die USA, dass neben den neuen Standardvertragsklauseln zusätzliche Maßnahmen (additional safeguards) ergriffen werden, um das Schutzniveau im Empfängerland zu gewährleisten. Der alleinige Gebrauch der Standardvertragsklauseln reicht dabei nicht aus, da die Behörden in den USA nicht Vertragspartei sind und somit nicht an die Standardvertragsklauseln gebunden sind. Zusätzliche Maßnahmen konnten jedoch weder Google noch die Webseitenbetreiber überzeugend nachweisen, sodass die Datenschutzbehörden den Einsatz für rechtswidrig erklärten.

III. Ausblick

Zusätzlich zu den Entscheidungen der Datenschutzbehörden wird der rechtskonforme Einsatz von Tracking Tools auch mit Blick auf das TTDSG (Telekommunikation-Telemedien-Datenschutz-Gesetz) schwierig. Das Gesetz sieht vor, dass Cookies und vergleichbare Technologien nur eingesetzt werden dürfen, wenn der Betroffene zuvor eingewilligt hat, es sei denn, die Cookies sind technisch zwingend erforderlich. Diese Ausnahme ist eng zu verstehen und erfasst nur Cookies, die verwendet werden, um einen Einkaufskorb vorzusehen oder die Spracheinstellungen zu speichern. Tracking und Analyse-Cookies wie Google Analytics fallen nicht darunter. Außerdem stehen mit der E-Privacy-Verordnung und dem Digital Services Act zwei weitere EU-Regelungen in den Startlöchern, die den Datenschutz in der EU weiter verbessern sollen, auch gegenüber Tech-Giganten aus den USA.

Übertragung von personenbezogenen Daten im Rahmen eines Asset Deals

I. M&A-Transaktionen und Daten

Kundendaten gehören auch im Fall von Unternehmenstransaktionen zu den entscheidenden wertbildenden Faktoren. Anders als im Falle eines Share Deals oder einer Umwandlungsmaßnahme stellt die Übertragung von Kundendaten im Rahmen eines Asset Deals eine rechtfertigungsbedürftige Datenverarbeitung i.S.v. Art. 4 Nr. 2 DSGVO dar. Achten die Parteien bei Vollzug des Asset Deals nicht auf die datenschutzrechtliche Konformität der Übertragung, kann dies ein nicht unerhebliches Bußgeld zur Folge haben.

II. Hintergrund

Im Jahr 2021 hat der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit Bußgeldbescheide i.H.v. EUR 12.500 gegen zwei Energieversorger erlassen. Ein Energieversorger hatte seine Heizenergiesparte ausgegliedert und an einen anderen Energieversorger veräußert. Die betroffenen Kunden wurden über die Vertragsübergänge ihrer Strombelieferungsverträge informiert und ihnen wurde ein Widerspruchsrecht eingeräumt. Im Falle eines erklärten Widerspruchs sollten keine personenbezogenen Daten der Kunden an das neue Unternehmen übermittelt werden. Bei einer Vielzahl von Kunden wurden trotz ordnungsgemäß erklärtem Widerspruch die Strombelieferungsverträge migriert und damit erfolgte auch eine unrechtmäßige Übertragung der entsprechenden Kundendaten.

III. Wie vermeiden Sie bei einem Asset Deal ein Bußgeld?

Da es sich bei der Übertragung von Kundendaten im Rahmen eines Asset Deals um eine rechtfertigungsbedürftige Datenverarbeitung handelt, muss ein Erlaubnistatbestand vorliegen, um ein Bußgeld zu vermeiden.

- Nach Art. 6 Abs. 1 lit. a DSGVO ist die Übertragung der Kundendaten zulässig, wenn der Betroffene einwilligt. Diese Einwilligung muss durch den Veräußerer vor der Datenübertragung eingeholt werden und den Anforderungen des Art. 4 Nr. 11 DSGVO genügen, wonach der Betroffene seine

Einwilligung in die konkrete Datenübertragung an den Erwerber erteilen muss. Da bei der Verhandlung zum Asset Deal unklar ist, wie viele Kunden ihre Einwilligung in die Datenübertragung erteilen werden und regelmäßig davon auszugehen ist, dass die Resonanz auf derartige Anfragen nicht besonders hoch ist, stellt sich der Erlaubnistatbestand der Einwilligung in der Praxis als eher untauglich dar.

- Eine Datenübertragung ist auch zur Erfüllung eines bestehenden Vertragsverhältnisses, in dem die betroffene Person Vertragspartei ist, zulässig. Die Anwendbarkeit auf den Asset Deal ist umstritten. Zum einen wird vertreten, dass im Falle eines Asset Deals die Datenübertragung nur notwendig ist, um den Kaufvertrag zwischen Veräußerer und Erwerber zu erfüllen. Die von der Datenübertragung betroffene Person ist jedoch nicht Vertragspartei des Asset Deals. Zum anderen wird vertreten, dass bei Kundenvertragsübernahmen die Übertragung der Kundendaten schlichtweg erforderlich ist.

- Des Weiteren kommt der Erlaubnistatbestand des berechtigten Interesses in Betracht. Der Rückgriff auf diesen Erlaubnistatbestand ist von den Datenschutzaufsichtsbehörden grundsätzlich anerkannt. Die Datenschutzkonferenz hat 2019 in diesem Zusammenhang auch einen Katalog von Fallgruppen, die ein berechtigtes Interesse nach Art. 6 Abs. 1 lit. f DSGVO begründen, herausgegeben, zwischen denen in der praktischen Handhabung zu unterscheiden ist:

  - Kundendaten bei laufenden Verträgen: Nach dem Katalog der Datenschutzkonferenz bedarf der Vertragsübergang nach § 415 BGB der zivilrechtlichen Genehmigung und in dieser ist dann auch die datenschutzrechtliche Zustimmung zum Übergang der erforderlichen Daten als Minus enthalten.

  - Bei Bestandskunden ohne laufende Verträge und letzter Vertragsbeziehung älter als drei Jahre ist nur eine eingeschränkte Übermittlung der Kundendaten möglich. Zwar dürfen die Daten übermittelt werden, jedoch dürfen sie nur wegen gesetzlicher Aufbewahrungsfristen genutzt werden.

  - Daten von Kunden bei fortgeschrittener Vertragsanbahnung; Bestandskunden ohne laufende Verträge und letzter Vertragsbeziehung jünger als drei Jahre können im Wege der Widerspruchslösung mit einer ausreichend bemessenen Widerspruchsfrist von ca. sechs Wochen übermittelt werden. Der Widerspruch sollte möglichst einfach gestaltet sein, beispielsweise im Online-Verfahren. Bankdaten sind von der Widerspruchslösung ausgenommen und bedürfen zur Übermittlung der ausdrückliche Einwilligung des Kunden.

  - Daten, die im Zusammenhang mit der Übertragung offener Forderungen gegen Kunden stehen, dürfen an den neuen Gläubiger übertragen werden. Dies gilt nicht, wenn die Forderungsabtretung durch Vereinbarung ausgeschlossen wurde.

Die genannten Fälle umfassen nicht die Übertragung von besonderen personenbezogenen Daten der Kunden (u. a. rassische u. ethnische Herkunft, politische Meinung, sexuelle Orientierung). Die Übertragung dieser Kundendaten bedarf der informierten Einwilligung durch den Betroffenen. Sofern die Kundendaten zulässig übertragen wurden, darf der Erwerber die Kundendaten nur zu den Werbemaßnahmen nutzen, denen der Kunde ursprünglich gegenüber dem Veräußerer zugestimmt hatte. Der Erwerber muss nach Übertragung der Daten darauf achten, seinen Informationspflichten nach Art. 14 DSGVO gegenüber den Kunden innerhalb von einem Monat nachzukommen.

Facebook-Fanpages immer noch nicht datenschutzkonform

I. Gutachten der DSK

Nachdem im November 2021 das Oberverwaltungsgericht Schleswig die Deaktivierung einer Facebook-Fanpage aufgrund von Datenschutzmängeln im Jahr 2011 bestätigt hat, hat die Konferenz der Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) ein Gutachten zur datenschutzrechtlichen Konformität des Betriebes von Facebook-Fanpages erstellt. Ergebnis: Facebook-Fanpages sind nicht datenschutzkonform.

Facebook hole bereits keine nach Art. 6 Abs. 1 lit. a DSGVO und nach § 25 Abs. 1 TTDSG wirksame Einwilligung ein. Dabei sei bereits unklar, ob der Nutzer seine Einwilligung nach beiden Rechtsgrundlagen oder nur nach der ersteren Rechtsgrundlage erteile. Eine anderweitige Rechtsgrundlage für die Datenverarbeitung bestehe nicht.

Aufgrund der gemeinsamen Verantwortlichkeit, jedenfalls für die Verarbeitung zu sog. Insights, müssen Betreiber von Fanpages eine entsprechende Rechtsgrundlage nachweisen können. (Facebook Insights ist ein umfangreiches Tool, mit dem Seitenstatistiken zu Facebook Fanpages abgerufen werden können. Es bietet den Betreibern von Fanpages die Möglichkeit, die Interaktionen der Nutzer und Fans nachzuverfolgen und deren Entwicklung auszuwerten). Die Informationen seien jedoch derart oberflächlich und lückenhaft, dass eine Bewertung als Verantwortlicher auf Grundlage dieser Informationen nicht möglich sei. Aus den gleichen Gründen könnten Seitenbetreiber auch nicht ihren Verpflichtungen aus Art. 13 DSGVO nachkommen.

II. Risikoeinschätzung und datenschutzfreundliche Alternativen

Die DSK sieht das Gutachten als eine wichtige Grundlage für das Tätigwerden von Aufsichtsbehörden gegenüber öffentlichen und nicht öffentlichen Stellen an. Insofern ist das Risiko für zukünftige Untersagungsanordnungen gegenüber öffentlichen und nichtöffentlichen Facebook-Fanpage Betreibern (und ggf. sogar Bußgelder, wenn nicht Folge geleistet wird) erheblich gestiegen. Zwar gehen die Aufsichtsbehörden in Deutschland derzeit überwiegend gegen öffentliche Stellen mit Facebook-Fanpages vor, da ihnen eine besondere Vorbildfunktion zukommt. Es gibt jedoch bereits auch Äußerungen, dieses Vorgehen auch auf Unternehmen und andere private Betreiber auszuweiten. Da im Zusammenhang mit den o.g. Problemen mit Facebook (neuerdings Meta) dieses Jahr ggf. sogar entsprechende Urteile (z. B. bzgl. der Untersagung des Betriebs von Fanpages) erlassen werden können, muss insoweit auch mit einem strikteren Vorgehen gegen Unternehmen gerechnet werden.

III. Ausblick

Ein Hoffnungsschimmer ist der angekündigte Digital Markets Act, der für das Jahr 2023 geplant ist. Ziel der EU-Verordnung ist die Schaffung eines „fairen Geschäftsumfelds“, indem die Europäische Union die Marktmacht großer Internetplattformen – wie Meta – regulieren will. Für Facebook-Fanpages Betreiber bleibt zu hoffen, dass die EU die wirtschaftliche Wichtigkeit von Fanpages für Unternehmen erkennt und diese hinsichtlich datenschutzrechtlicher Anforderungen entlastet, während die Umsetzung der Anforderungen den großen Internetplattformen (sog. Gatekeepern) auferlegt wird.

Zulässigkeit von Produktwarnungen durch Aufsichtsbehörden

I. Produktwarnung bei IT-Produkten

Immer wieder kommt es vor, dass Aufsichtsbehörden öffentliche Produktwarnungen aussprechen, was für die Hersteller der betreffenden Produkte weitreichende Reputationsschäden zur Folge haben kann. Weltweite Beachtung hat zuletzt die öffentliche Warnung des Bundesamts für Sicherheit in der Informationstechnik (BSI) vor der Nutzung von Virenschutzprodukten des russischen Unternehmens Kaspersky gefunden. Grund für die Warnung vom 15. März 2022 war laut BSI das „Vorgehen militärischer und/ oder nachrichtendienstlicher Kräfte in Russland sowie die im Zuge des aktuellen kriegerischen Konflikts von russischer Seite ausgesprochenen Drohungen gegen die EU, die NATO und die Bundesrepublik Deutschland“. Daher sei der Einsatz von Kapersky-Programmen mit einem erheblichen Risiko eines erfolgreichen IT-Angriffs verbunden. Ein Eilantrag des Herstellers auf Erlass einer einstweiligen Anordnung auf Unterlassung und Widerruf der Warnung wurde durch das Verwaltungsgericht Köln bereits abgelehnt.

II. Voraussetzungen für behördliche Produktwarnungen

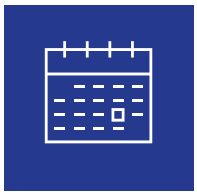
Im Regelfall ist eine spezielle, gesetzlich normierte Ermächtigungsgrundlage erforderlich, wenn eine Aufsichtsbehörde eine öffentliche Produktwarnung aussprechen möchte. Diese legt die Voraussetzungen für die Zulässigkeit von Produktwarnungen fest und kann darüber hinaus besondere Rechte der betroffenen Hersteller bestimmen, wie etwa ein Anhörungs- oder Informationsrecht im Vorfeld der öffentlichen Warnung. Für das BSI ergibt sich eine solche Ermächtigungsgrundlage aus § 7 BSIG. Hiernach ist das BSI ermächtigt, die Öffentlichkeit vor Sicherheitslücken in informationstechnischen Produkten und Diensten, vor Schadprogrammen und vor dem Verlust oder unerlaubten Zugriff auf Daten zu warnen, sowie über sicherheitsrelevante IT-Eigenschaften von Produkten zu informieren.

III. Gegenmaßnahmen betroffener Hersteller

Öffentliche Produktwarnungen können für die betroffenen Hersteller weitreichende Folgen haben. So sehen beispielsweise die Nutzungsbedingungen der gängigen App-Stores vor, dass Apps aus dem Store entfernt oder dort gesperrt werden können oder ihre Sichtbarkeit eingeschränkt werden kann, wenn diese sicherheitsbezogene oder den Ruf des Store-Betreibers betreffende Auswirkungen haben können. Eine öffentliche Warnung durch – in diesem Fall – das BSI würde solche Auswirkungen implizieren. Zudem könnte eine Warnung weitere Aufsichtsbehörden alarmieren, beispielweise die zuständige Datenschutzaufsichtsbehörde im Falle einer Warnung vor IT-Sicherheitslücken.

In vielen Fällen geht einer öffentlichen Produktwarnung eine entsprechende Untersuchung durch die jeweilige Aufsichtsbehörde voraus. In diesem Rahmen kann etwa das BSI gemäß § 7a BSIG Auskünfte, insbesondere zu technischen Details, von den Herstellern informationstechnischer Produkte und Systeme verlangen. Nimmt eine Aufsichtsbehörde daher Kontakt zu einem Hersteller auf und fordert etwa Nachweise oder andere Unterlagen zu den Produkten an, sollte mit der Aufsichtsbehörde umfassend kooperiert werden. Äußert sich die Behörde zu irgendwelchen Defiziten des Produkts, die sie im Rahmen ihrer Untersuchung ermittelt hat, sollten diese schnellstmöglich beseitigt und die Behörde hierüber proaktiv informiert werden. Eine engagierte Zusammenarbeit mit der Aufsichtsbehörde kann eine Produktwarnung so möglicherweise bereits im Voraus verhindern.

Veranstaltungen, Veröffentlichungen und Blog



Eine Übersicht mit unseren Veranstaltungen finden Sie hier.

Eine Liste unserer aktuellen Veröffentlichungen finden Sie hier.

Unseren Blog finden Sie hier.

Impressum

Verleger: Luther Rechtsanwaltsgesellschaft mbH
Anna-Schneider-Steig 22, 50678 Köln, Telefon +49 221 9937 0
Telefax +49 221 9937 110, contact@luther-lawfirm.com
V.i.S.d.P.: Dr. Michael Rath, Partner
Luther Rechtsanwaltsgesellschaft mbH
Anna-Schneider-Steig 22, 50678 Köln, Telefon +49 221 9937 25795
michael.rath@luther-lawfirm.com

Bildnachweis: MR.Cole_Photographer/Getty Images: Seite 1; Blue Planet Studio /Adobe Stock: Seite 3; putilov_denis/iStock: Seite 5; Julien Eichinger/Adobe Stock: Seite 9; sdecoret/Adobe Stock: Seite 10; goodluz/Adobe Stock: Seite 12;

Haftungsausschluss

Obgleich dieser Newsletter sorgfältig erstellt wurde, wird keine Haftung für Fehler oder Auslassungen übernommen. Die Informationen dieses Newsletters stellen keinen anwaltlichen oder steuerlichen Rechtsrat dar und ersetzen keine auf den Einzelfall bezogene anwaltliche oder steuerliche Beratung. Hierfür stehen unsere Ansprechpartner an den einzelnen Standorten zur Verfügung.

Aus Gründen der besseren Lesbarkeit verzichten wir auf die gleichzeitige Verwendung geschlechterspezifischer Sprachformen. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung grundsätzlich für alle Geschlechter. Die verkürzte Sprachform hat redaktionelle Gründe und beinhaltet keine Wertung.

Luther.

Bangkok, Berlin, Brüssel, Delhi-Gurugram, Düsseldorf, Essen, Frankfurt a. M., Hamburg, Hannover, Jakarta, Köln, Kuala Lumpur, Leipzig, London, Luxemburg, München, Shanghai, Singapur, Stuttgart, Yangon

Weitere Informationen finden Sie unter
www.luther-lawfirm.com
www.luther-services.com

unyer GLOBAL ADVISORS