Geschäftsstelle Dresden:
Königsbrücker Landstraße 40
01109 Dresden
Tel: 0351 8881251

Niederlassung Böblingen:
Otto-Lilienthal-Straße 36
71034 Böblingen
Tel: 07031 7145660

mail@sodalitas-gmbh.de
www.sodalitas-gmbh.de
Fax: 0351 8881252

IT-Ticker 02/2021

Der IT-Ticker 02/2021 informiert Sie über folgende Themen:

Empfehlungen des EDSA für Drittlandtransfers aktualisiert

Der Europäische Datenschutzausschuss (EDSA) hat am 18.06.2021 nach Abschluss der öffentlichen Konsultation seine Empfehlungen für ergänzende Schutzmaßnahmen beim Transfer personenbezogener Daten in Drittländer außerhalb der EU und des EWR veröffentlicht. Es handelt sich dabei um eine Überarbeitung der im November 2020 veröffentlichen ersten Fassung der Empfehlungen.

Der EuGH hatte am 16.07.2020 entschieden, dass die Übermittlung personenbezogener Daten auf Grundlage des EU-US Privacy Shield unzulässig und bei der Nutzung von EU Standardvertragsklauseln eine eigene Wirksamkeitsprüfung durch die Verwender notwendig ist.

Der EDSA hält in der aktualisierten Fassung an dem von ihm entwickelten 6-Stufenmodell fest und verpflichtet den Datenexporteur zu einer individuelle Risikoanalyse und -dokumentation pro Datenübermittlung in ein Drittland. Zentrales Element dieser Risikoanalyse ist nach Randnummer 31 der Empfehlung eine Prüfung, ob und in welchem Umfang das Risiko eines behördlichen Zugriffs auf die Daten besteht.

Aus unternehmerischer Sicht ist insoweit erfreulich, dass sich der EDSA – ebenso wie die Europäische Kommission in den neuen Standardvertragsklauseln – in seinen finalen Empfehlungen für einen risikobasierten Ansatz bei der Beurteilung des Schutzniveaus beim Drittlandtransfer entschieden hat. Hierdurch entsteht ggf. mehr Rechtsicherheit für den Drittlandtransfer, wenn die Durchführung und Dokumentation einer Risikoanalyse im Einzelfall erfolgt.

Allein die Möglichkeit, dass ein Dienstleister im Rahmen der Wartung oder des Supports aus einem Drittland auf Daten zugreifen kann, reicht dem EDSA für die Annahme eines Drittlandtransfers aus. Dies trifft nicht nur Cloud-Provider sondern sehr viele international tätige Anbieter, die Support nach dem Follow-the-Sun-Prinzip arbeiten – also ihren Support rund um die Uhr anbieten und dabei stets von dort Support leisten, wo gerade reguläre Bürozeiten sind. Allerdings bestätigt der EDSA, dass wenn Anbieter aus der EU und dem EWR vertraglich eine Datenübermittlung in Drittländer ausdrücklich ausschließen (Randnummer 13), kein Drittlandtransfer angenommen wird.

Hinsichtlich der Möglichkeiten, sich für Datentransfers auf Ausnahmeregelungen nach Art. 49 DSGVO zu berufen, betont und bekräftigt der EDSA sein Verständnis, dass dies stets nur die Ausnahme und nie die Regel sein darf. Diese pauschale Aussage des EDSA dürfte jedenfalls hinsichtlich einer möglichen Einwilligung der Betroffenen fragwürdig sein. Die freie Entscheidung von Menschen, einem Drittlandtransfer zuzustimmen, kann der EDSA nach unserem Verständnis nicht beschränken. Gleichwohl müssen solche Einwilligungen allen Anforderungen von Art. 6, 7 und 49 DSGVO genügen.

Die in Annex 2 aufgeführten Beispielsfälle haben sich nicht wesentlich geändert. Der EDSA bleibt bei seiner Einschätzung, dass Datenverarbeitungen im Drittland aus seiner Sicht derzeit nicht möglich sind, wenn der Empfänger die Daten im Klartext lesen kann. Damit wären aber auch Datentransfers innerhalb von internationalen Unternehmensgruppen praktisch unmöglich (siehe dazu F.A.Z. Einspruch vom 16.11.2020 und unsere #UpdateIT Paneldiskussion zur Datenverarbeitung im Konzern). Der EDSA hält aber an seinem Beispiel fest, nachdem eine wirksame Pseudonymisierung eine geeignete Schutzmaßnahme sein kann, die einen Drittlandtransfer von Daten ermöglich.

Praxistipp:
Die Übermittlung personenbezogener Daten in Drittländer und der Einsatz von internationalen Cloud-Providern bleibt weiterhin schwierig. Die aktualisierten Empfehlungen des EDSA und die neuen EU-Standardvertragsklauseln müssen ab sofort zentraler Baustein jedes Datentransfers in ein Drittland werden. Unternehmen müssen ihre Risikoanalysen dokumentieren und sollten bei der Festlegung der Schutzmaßnahmen die Empfehlungen des EDSA unbedingt berücksichtigen. Eine einfache one-fits-all-Lösung gibt es leider weiterhin nicht. Die Prüftätigkeit der Behörden zeigt aber, dass Unternehmen sich hier unbedingt vorbereiten müssen.

Die SKW Taskforce Datenschutz unterstützt Sie gerne bei der Durchführung einer detaillierten Risikobewertung im Drittland (6-Stufenplan) oder bei der Implementierung der neuen Standardvertragsklauseln. Wir haben ein Tool zur Durchführung des Risk Assessments entwickelt und stellen dies unseren Mandanten gerne zur Verfügung.

Nikolaus Bertermann, Berlin
n.bertermann@skwschwarz.de
Dr. Oliver Hornung, Frankfurt/Main
o.hornung@skwschwarz.de
Hannah Mugler, Berlin
h.mugler@skwschwarz.de

EU-Kommission verabschiedet neue Standarddatenschutzklauseln für internationalen Datentransfer

Die EU-Kommission hat am 4. Juni 2021 die finale Fassung der neuen Standarddatenschutzklauseln (Standard Contractual Clauses oder abgekürzt SCC) für Übermittlungen personenbezogener Daten in Drittländer und weiterhin die finale Fassung der Standardvertragsklauseln für Auftragsverarbeitungsverträge für die Verarbeitung personenbezogener Daten in der Europäischen Union veröffentlicht.

Die Presseerklärung der EU-Kommission sowie die neuen Standarddatenschutzklauseln und die finale Fassung der Standardvertragsklauseln für Auftragsverarbeitungsverträge können über diesen Link abgerufen werden.

Neue Standarddatenschutzklauseln für den internationalen Datentransfer
Die Rechtmäßigkeit der Übermittlung von personenbezogenen Daten in Länder außerhalb der Europäischen Union und des Europäischen Wirtschaftsraums wird grundsätzlich in 2 Stufen festgestellt. Auf der 1. Stufe muss zunächst eine Rechtsgrundlage nach Art. 6 Abs. 1 DS-GVO (z. B. Art. 6 Abs. 1 lit. b) DS-GVO – Vertragserfüllung) für die Datenübermittlung vorliegen. Auf der 2. Stufe wird dann geprüft, ob bei dem Empfänger im Drittland ein angemessenes Datenschutzniveau für personenbezogene Daten besteht. Ein solches Schutzniveau kann für ein Land ganz oder teilweise für einen Sektor mit einem Angemessenheitsbeschluss durch die EU-Kommission festgestellt werden.

Nach Art. 46 DS-GVO kann ein angemessenes Schutzniveau auch durch geeignete Garantien hergestellt werden. Eine von diesen Garantien sind die Standarddatenschutzklauseln nach Art. 46 Abs. 2 lit. c) DS-GVO. Dabei handelt es sich um Musterverträge, die beide Parteien zum Einhalten eines mit der Europäischen Union vergleichbaren Datenschutzniveaus verpflichten. Diese wurden nunmehr endlich überarbeitet. Die neuen Standarddatenschutzklauseln lösen die bislang noch geltenden Standardvertragsklauseln für einen Transfer zwischen Verantwortlichen aus 2001 sowie den Datentransfer an Auftragsverarbeiter aus 2010 für Übermittlungen personenbezogener Daten in Drittländer ab.

Inhalte der neuen Standarddatenschutzklauseln
Die von der EU-Kommission verabschiedeten neuen Standarddatenschutzklauseln sehen im Vergleich zu den bislang geltenden Standardvertragsklauseln eine Reihe von Änderungen vor. Am auffälligsten ist, dass die neuen Standarddatenschutzklauseln einem modularen Ansatz im Sinne eines Baukastenprinzips folgen. Zukünftig gibt es also nur noch einen Satz an Standarddatenschutzklauseln zum internationalen Datentransfer, der je nach konkreter Ausgestaltung des jeweiligen Datentransfers durch Verwendung bestimmter und das Weglassen anderer Textbausteine angepasst werden kann.

Die neuen Standarddatenschutzklauseln gelten sowohl für Übermittlungen zwischen Verantwortlichen (Modul 1) als auch für einen Datentransfer an Auftragsverarbeiter (Modul 2). Zudem gelten die neuen Standarddatenschutzklauseln auch für einen Weitertransfer von einem Auftragsverarbeiter an einen weiteren Auftragsverarbeiter (sog. Unterauftragnehmer) (Modul 3) sowie für einen Datentransfer von einem Auftragsverarbeiter an einen Verantwortlichen (Modul 4).

Weitere, neue Inhalte sind u. a. (i) die Möglichkeit des Beitritts anderer Unternehmen zu den Standarddatenschutzklauseln, (ii) Offenlegung von Angaben zu allen Verantwortlichen bei Verträgen zwischen Auftragsverarbeitern, (iii) konkrete Regelungen zu den technischen und organisatorischen Schutzmaßnahmen, (iv) umfassende Haftungsregeln sowie (v) eine strenge Hierarchieklausel, die von den Vertragsparteien strikt zu beachten ist.

Neu ist insbesondere auch eine sog. Kopplungsklausel, wonach jederzeit neue Vertragspartner in bestehende Standarddatenschutzklauseln aufgenommen werden können. Damit verfolgt der europäische Gesetzgeber den Zweck, dass ein Auftraggeber etwa bei gemeinsamer Verantwortlichkeit einen anderen Auftraggeber aufnehmen kann, um das Vertragsverhältnis zur Auftragsverarbeitung mit dem Dienstleister datenschutzrechtlich abzusichern.

Ebenso wurde die Beauftragung von weiteren Auftragsverarbeitern als sog. Unterauftragnehmer neu geregelt. Für den wichtigsten Anwendungsfall der neuen Standarddatenschutzklauseln – einem Datentransfer an Auftragsverarbeiter (Modul 2) – gelten jedoch die gleichen Grundsätze, wie dies Art. 28 Abs. 2 und Abs. 4 DS-GVO für einen Vertrag zur Auftragsverarbeitung vorsieht. Der Auftraggeber kann im Vertrag zur Auftragsverarbeitung entscheiden, ob er jeder Änderung zur Beauftragung von Unterauftragnehmern durch den Auftragsverarbeiter zustimmt oder ob eine allgemeine Genehmigung dahingehend erklärt, dass der Auftragsverarbeiter nur über die Änderung zu Unterauftragnehmern informieren muss, der Auftraggeber dann allerdings ein Widerspruchsrecht erhält.

Insgesamt ermöglichen die neuen Standarddatenschutzklauseln Unternehmen mehr Flexibilität bei der Vertragsgestaltung. Ob die Anwendung aber in der Praxis tatsächlich erleichtert wird, bleibt abzuwarten. Zudem wurden mit den Modulen 3 und 4 zwei neue Konstellationen zum internationalen Datentransfer eingeführt und es bleibt abzuwarten, ob deren Umsetzung in die Praxis zu Problemen führt.

Schrems II-Verpflichtungen
Die neuen Standarddatenschutzklauseln enthalten weiterhin zahlreiche Verpflichtungen um die hohen Anforderungen des Europäischen Gerichtshofs zu Schrems II und die damit korrespondierenden Vorgaben des Europäischen Datenschutzausschusses für den Drittlandtransfer zu beachten.

So sehen die neuen Standarddatenschutzklauseln – wie vom Europäischen Datenschutzausschuss gefordert – eine dokumentierte Risikoeinschätzung verbindlich vor („Transfer Impact Assessment“). Beide Parteien müssen versichern, dass sie keine Zweifel an der Einhaltung europäischer Datenschutzstandards im Land des Datenimporteurs haben. Zur Erfüllung der Rechenschaftspflicht nach Art. 5 Abs. 2 DS-GVO ist das Transfer Impact Assessment zu dokumentieren und den Datenschutzaufsichtsbehörden auf Verlangen vorzulegen.

Aufgrund ihrer Natur als Vertragsklauseln können aber die neuen Standarddatenschutzklauseln etwaige Konflikte mit nationalem Recht von Drittländern nicht abschließend lösen. Im Gegenteil: Die EU-Kommission weist in ihrem Beschluss zu den Standarddatenschutzklauseln sogar ausdrücklich darauf hin, dass der Datentransfer auf Basis der Standarddatenschutzklauseln nicht stattfinden sollte,

wenn das Recht und die Rechtspraxis in Drittländern den Datenimporteur daran hindern, vertragliche Verpflichtungen einzuhalten (vgl. Randnummer 19 des Beschlusses der EU-Kommission).

Datenexportierende Unternehmen müssen daher bei Verwendung der neuen Standarddatenschutzklauseln und darauf gestützte Datenübermittlungen in Drittländer jeweils im Einzelnen prüfen, welchen Gesetzen der jeweilige Datenimporteur im Drittland, an den sie die Daten übermitteln möchten, und etwaige weitere Empfänger unterliegen und ob diese Gesetze die von ihnen mit Unterzeichnung der Standarddatenschutzklauseln gegebenen Garantien beeinträchtigen. Demzufolge ist es unabdingbar die einzelnen Datentransfers zu analysieren und zu prüfen, welche Gesetze des Drittlandes zur Anwendung kommen und welche zusätzlichen Garantien der Auftragsverarbeiter anbietet. Geeignete, ergänzende Garantien können zusätzliche Maßnahmen vertraglicher, organisatorischer oder technischer Art sein.

Vertraglich und organisatorische Maßnahmen allein werden im Allgemeinen nicht genügen, dem Zugriff staatlicher Stellen des Drittlands auf personenbezogene Daten entgegenzuwirken. Als zusätzliche Schutzmaßnahme nennt der Europäische Datenschutzausschuss insbesondere Verschlüsselungstechnologien sowie den Einsatz von Anonymisierungs- und/oder Pseudonymisierungstechniken, wenn insbesondere nur das EU-Unternehmen die Zuordnung vornehmen kann.

Umsetzungszeitraum
Die offizielle Version der neuen Standarddatenschutzklauseln wird in den kommenden Tagen im EU-Amtsblatt veröffentlicht. Die bisherigen Standardvertragsklauseln dürfen ab dem Zeitpunkt der offiziellen Veröffentlichung nur noch 3 Monate lang abgeschlossen werden. Diese Karenzzeit dient dem Zweck, laufende oder bereits abgeschlossene Vertragsverhandlungen auf der Grundlage der bisherigen Standardvertragsklauseln nicht gegenstandslos werden zu lassen.

Spätestens mit Ablauf weiterer 15 Monate müssen jedoch alle bestehenden Standardvertragsklauseln auf die neuen Regelungen umgestellt werden. Für datenexportierende Unternehmen stehen also umfangreiche Nachverhandlungen zu den bisher verwendeten Standardvertragsklauseln an.

Handlungsmaßnahmen für Unternehmen
Zusammenfassend lässt sich festhalten, dass die neuen Standarddatenschutzklauseln eine Reihe von Änderungen gegenüber den bislang geltenden Standardvertragsklauseln vorsehen. Der modulare Baukasten der neuen Standarddatenschutzklauseln berücksichtigt die Anforderungen des Europäischen Gerichtshofes zur Schrems II-Entscheidung. Jedoch wird der Abschluss der neuen Standarddatenschutzklauseln aufgrund der Notwendigkeit einer verpflichtenden Risikoeinschätzung nicht mehr einfach nur eine reine „Abhakübung“ sein. Auf Unternehmen kommt daher zukünftig mit Abschluss der neuen Standarddatenschutzklauseln viel Arbeit zu.

Alle laufenden Datentransfers in Drittländer auf Grundlage der bisherigen Standardvertragsklauseln müssen innerhalb der nächsten ca. 18 Monate auf die neuen Standarddatenschutzklauseln umgestellt werden.

Für Unternehmen ergibt sich folgender Handlungsbedarf:

- Durchführung eines Datenmappings um zu prüfen, welche personenbezogenen Daten Unternehmen aufgrund von Standardvertragsklauseln in Drittländer übermitteln und in welchen Fällen die neuen Standarddatenschutzklauseln abzuschließen sind;
- Analyse der neuen Standarddatenschutzklauseln – ggf. mit anwaltlicher Hilfe und Anpassung der neuen SCC auf die konkreten Bedürfnisse des Unternehmens bzw. der Unternehmens-Gruppe;
- Etablierung eines standardisierten Prozesses zur Durchführung des Transfer Impact Assessments sowie Dokumentation des Transfer Impact Assessment;
- Umgehende Kontaktaufnahme mit Dienstleistern zum Abschluss der neuen Standarddatenschutzklauseln;
- Etablierung der neuen Standarddatenschutzklauseln auch beim konzerninternen Datentransfer in Drittländer mit Festlegung welches Modul zum Drittlandtransfer benötigt wird.

Da der internationale Datentransfer in Drittländer aktuell im Fokus der Datenschutzaufsichtsbehörden steht und seit letzter Woche in Deutschland Prüfaktionen zum internationalen Datentransfer vorgenommen werden, sollten Unternehmen sehr zeitnah ein Projekt aufsetzen und den hier vorgestellten Handlungsbedarf umsetzen.

Dr. Oliver Hornung, Frankfurt/Main
o.hornung@skwschwarz.de
Franziska Ladiges, Frankfurt am Main
f.ladiges@skwschwarz.de

Deutsche Aufsichtsbehörden prüfen internationale Datenübermittlungen

Die „Schonfrist für Unternehmen“ nach Erlass des Schrems II-Urteils durch den EuGH ist nun endgültig vorüber.

Am 1. Juni 2021 kündigten verschiedene Aufsichtsbehörden in Deutschland an, im Rahmen einer länderübergreifenden Kontrolle die Datenübermittlungen durch Unternehmen in Staaten außerhalb der Europäischen Union zu überprüfen. Vor allem Unternehmen in Bayern, Berlin, Brandenburg, Hamburg, Niedersachsen, Rheinland-Pfalz und dem Saarland müssen mit entsprechenden Anfragen der Aufsichtsbehörde rechnen. Es ist jedoch nicht ausgeschlossen, dass sich noch weitere Behörden an der Umfrage beteiligen.

Ziel der Prüfung ist es die Erwartungen des EuGHs zu erfüllen, dass Behörden unzulässige Transfers aussetzen oder verbieten. In seiner Schrems-II-Entscheidung erklärte der EuGH am 16. Juli 2020 das EU-US-Privacy-Shield ohne Übergangsfrist für ungültig. Gleichzeitig betonte er, dass Datenübermittlungen zwar auf Grundlage der Standarddatenschutzklauseln weiterhin zulässig sind. Der Verantwortliche muss sich jedoch davon überzeugen, dass diese auch eingehalten werden können und insofern ein gleichwertiges Schutzniveau für personenbezogenen Daten gewährleistet werden kann. Dies soll bei Bedarf durch die Verwendung wirksamer zusätzlicher Maßnahmen sichergestellt werden.

Obwohl es noch immer keine zufriedenstellende Lösung für eine rechtmäßige Datenübermittlung vor allem in die USA gibt, wird dies nun durch die Aufsichtsbehörden geprüft. Die teilnehmenden Behörden werden ausgewählte Unternehmen in ihrem Zuständigkeitsbereich auf Grundlage von gemeinsamen Fragenkatalogen anschreiben. Zudem konzentrieren sich die Behörden auf verschiedene Bereiche: Mailhoster, Webhoster, Tracking, Bewerberportale und konzerninterner Datenverkehr. Jede Aufsichtsbehörde entscheidet dabei individuell, in welchen dieser Themenfelder sie prüft und ob der Fragenkatalog regional angepasst wird.

Praxistipp
Unternehmen sollten sich nach der Ankündigung darauf einstellen, von der zuständigen Aufsichtsbehörde angeschrieben zu werden. Die Fragebögen sollten dann nicht etwa ignoriert, sondern ordnungsgemäß mit anwaltlicher Unterstützung befüllt werden. Vor allem bei einer Datenübermittlung in die USA sind zudem die Empfehlungen des Europäischen Datenschutzausschusses zu berücksichtigen und im besten Fall zu dokumentieren. Demnach sind die folgenden Schritte durchzuführen:

1. Analyse der Datentransfers in Drittländer („Know Your Transfers“)
2. Identifikation der verwendeten Transferwerkzeuge
3. Beurteilung der Wirksamkeit der Transferwerkzeuge
4. Identifizierung angemessener ergänzender Maßnahmen
5. Implementierung ergänzender Maßnahmen
6. Regelmäßige Evaluierung

Dr. Oliver Hornung, Frankfurt/Main
o.hornung@skwschwarz.de
Franziska Ladiges, Frankfurt am Main
f.ladiges@skwschwarz.de

Das IT-Sicherheitsgesetz 2.0 tritt in Kraft

Nach dem „ersten“ IT-Sicherheitsgesetz aus 2017 legt der deutsche Gesetzgeber jetzt nach und verschärft die gesetzlichen Pflichten zur Sicherheit informationstechnischer Systeme.

Am 27.05.2021 wurde das Zweite Gesetz zur Erhöhung der Sicherheit informations-technischer Systeme (IT-Sicherheitsgesetz 2.0) im Bundesgesetzblatt verkündet (BGBl. I S. 1122). Der ganz überwiegende Teil des IT-Sicherheitsgesetzes tritt damit am 28.05.2021 in Kraft. Einige der Regelungen werden erst etwas später zum 01.12.2021 wirksam.

Neben rund 1.500 neuen Planstellen in verschiedenen Ministerien der Bundesverwaltung sieht das Gesetz in erster Linie Änderungen des BSI-Gesetzes (BSIG) vor. Das BSI erhält zusätzliche Aufgaben und Kompetenzen, auch auf dem Gebiet des Verbraucherschutzes. Inhaltlich sieht das zukünftige BSIG im Wesentlichen drei Neuerungen vor:

- Durch die Einführung von Unternehmen im besonderen öffentlichen Interesse wird der Anwendungsbereich des BSIG erweitert.
- Der Einsatz von kritischer Komponenten in KRITIS wird reguliert. Das BSI hat zukünftig die Möglichkeit, den Einsatz solcher Komponenten zu unterbinden, wenn ihr Hersteller nicht vertrauenswürdig ist.
- Ebenfalls neu ist das freiwillige IT-Sicherheitskennzeichen für IT-Produkte, das der Verbrauchertransparenz auf dem Bereich der IT-Sicherheit dienen soll.

Das „need-to-know“ zu diesen drei Stichworten fassen wir im Folgenden knapp zusammen:

Unternehmen im besonderen öffentlichen Interesse
Neben den bereits derzeit durch das BSIG regulierten „Kritischen Infrastrukturen“ und „digitalen Diensten“ werden zukünftig auch „Unternehmen im besonderen öffentlichen Interesse“ unmittelbar durch das BSIG verpflichtet. Unternehmen im besonderen öffentlichen Interesse sind nach § 2 Abs. 14 BSIG-neu:

1. Unternehmen, die Güter im Sinne von § 60 Abs. 1 Nr. 1 und 3 AWV herstellen oder entwickeln;
2. Unternehmen, die nach ihrer inländischen Wertschöpfung zu den größten Unternehmen in Deutschland gehören und daher von erheblicher volkswirtschaftlicher Bedeutung sind. Dazu zählen auch Zulieferer solcher Unternehmen, die wegen ihrer Alleinstellungsmerkmale von besonderer Bedeutung sind. Die maßgeblichen Kennzahlen wird das BSI durch Rechtsverordnung gesondert festlegen; und
3. Unternehmen, die Betreiber eines Betriebsbereichs der oberen Klasse der Störfall-Verordnung oder diesen gleichgestellt sind.

Unternehmen im besonderen öffentlichen Interesse im Sinne der Nr. 1 und 2 müssen sich beim BSI registrieren und eine für das BSI erreichbare Stelle benennen. Zudem sind diese Unternehmen zukünftig verpflichtet, alle zwei Jahre eine Selbsterklärung zur IT-Sicherheit gegenüber dem BSI abgeben. Für Unternehmen im Sinne der Nr. 3 ist dies jeweils optional.

Zudem müssen Unternehmen im besonderen öffentlichen Interesse bestimmte Störungen ihrer Systeme, Komponenten und Prozesse an das BSI melden.

Kritische Komponenten
Neu ist außerdem die vor allem im Kontext der 5G-Infrastruktur öffentlich diskutierte Regulierung kritischer Komponenten durch das geänderte BSIG.

Der Begriff „kritische Komponenten“ beschreibt – stark verkürzt – Software und Hardware, die für Kernfunktionen einer kritischen Infrastruktur (KRITIS) eingesetzt wird und welche entweder durch Gesetz als kritische Komponente bestimmt wurde oder eine aufgrund eines Gesetzes als kritisch bestimmte Funktion realisiert.

Die Regulierung kritischer Komponenten betrifft damit primär KRITIS-Betreiber. Kritische Komponenten dürfen künftig nur noch eingesetzt werden, wenn der Hersteller der Komponente eine Garantieerklärung gegenüber dem KRITIS-Betreiber abgegeben hat. Daraus muss auch hervorgehen,

ob und wie der Hersteller hinreichend sicherstellt, dass die kritische Komponenten über keine technischen Eigenschaften verfügt, um missbräuchlich auf Sicherheit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der KRITIS einzuwirken. Die Anforderungen an die Garantieerklärung legt das BMI gesondert fest.

Zudem hat das BSI künftig die Befugnis, den Einsatz kritischer Komponenten und in Einzelfällen sogar den Betrieb der kritischen Infrastruktur an sich zu untersagen, wenn der Hersteller der Komponenten sich als nicht vertrauenswürdig erwiesen hat. Mittelbar hat die Regulierung kritischer Komponenten damit auch substantielle Auswirkungen auf Hersteller kritischer Komponenten.

IT-Sicherheitskennzeichen
Zur Verbesserung der Information von Verbrauchern zur IT-Produktsicherheit führt das IT-Sicherheitsgesetz 2.0 für vom BSI separat festzulegende Produktkategorien ein einheitliches IT-Sicherheitskennzeichen ein.

Hersteller oder Anbieter von Produkten dieser Kategorien können beim BSI die Freigabe zur Verwendung des IT-Sicherheitskennzeichens beantragen. Erteilt das BSI die beantragte Freigabe, kann der Hersteller das Kennzeichen für das Produkt verwenden, indem er das Etikett des IT-Sicherheitskennzeichens auf dem Produkt anbringt oder elektronisch veröffentlicht.

Das Kennzeichen besteht aus einer Zusicherung des Herstellers, wonach das Produkt bestimmte IT-Sicherheitsanforderungen erfüllt (Herstellererklärung) und einer Information des BSI über sicherheitsrelevante IT-Eigenschaften des Produkts (Sicherheitsinformation). Das Etikett des IT-Sicherheitskennzeichens verweist auf eine Internetseite, auf der Herstellererklärung und Sicherheitsinformation für das Produkt abrufbar sind.

Das IT-Sicherheitskennzeichen ist freiwillig. Weder ist das IT-Sicherheitskennzeichen Voraussetzung für den Vertrieb von Produkten im Bundesgebiet, noch sieht das IT-Sicherheitsgesetz 2.0 ausdrücklich eine rechtliche Wirkung des IT-Sicherheitskennzeichens gegenüber Verbrauchern zu.

Dr. Daniel Meßmer, München
d.messmer@skwschwarz.de

Kopie sämtlicher Arbeits-E-Mails? - Umfang des Auskunftsanspruchs weiter ungeklärt

Das Bundesarbeitsgericht (BAG) hat am 27. April 2021 (Az.: 2 AZR 342/20) entschieden, dass ein entlassener Arbeitnehmer von seinem früheren Arbeitgeber nicht die Herausgabe einer Kopie seiner gesamten E-Mail-Kommunikation von ihm und über ihn verlangen kann. Da das BAG diese Entscheidung aber auf zivilprozessuale Vorgaben stützt, bleibt weiterhin ungeklärt, wie weit der datenschutzrechtliche Auskunftsanspruch reicht und damit auch, wie aufwendig dieser für Unternehmen werden kann.

Sachverhalt und Entscheidung
Geklagt hatte ein Wirtschaftsjurist, der schon nach einem Monat in seiner Probezeit wieder entlassen worden war. Im Rahmen des Kündigungsschutzprozesses machte er auch einen datenschutzrechtlichen Auskunftsanspruch gem. Art. 15 DSGVO geltend. Er verlangte Auskunftserteilung der verarbeiteten personenbezogenen Daten über ihn sowie die Übergabe entsprechender Kopien davon und zwar einschließlich des gesamten E-Mail-Verkehrs zu seiner Person. In der Sache ging es damit um die umstrittene Reichweite des datenschutzrechtlichen Auskunftsanspruchs über die gespeicherten personenbezogenen Daten aus Art. 15 Abs. 3 DSGVO, der auch einen Anspruch auf Überlassung einer Kopie dieser Daten vorsieht.

Das LAG Niedersachsen (Urt. v. 9.6.2020 – Az.: 9 Sa 608/19) hat dem Kläger teilweise Recht gegeben, nämlich soweit es sich um personenbezogene Daten handelt, die der Arbeitgeber verarbeitet hatte. Nur dies deckt sich laut LAG Niedersachsen mit dem Auskunftsanspruch nach Art. 15 Abs. 1 DSGVO. Seine eigene elektronische Korrespondenz mit dem Unternehmen müsse dem Kläger aber nicht übermittelt werden, weil der Kläger diese selbst kennt. Nach dem Schutzzweck gebe es daher auch keinen Anlass, diesen gesamten E-Mail-Verkehr zur Verfügung zu stellen.

Das BAG hat die Klage auf Überlassung einer Kopie der im Arbeitsverhältnis versandten E-Mails in der Revisionsinstanz jetzt ebenfalls abgelehnt. Die Frage der Reichweite dieses Anspruchs klärt das BAG damit aber nicht, weil es die Ablehnung formal begründet: Der Klageantrag auf Überlassung einer Kopie der gesamten E-Mails sei nämlich zu unbestimmt (§ 253 Abs. 2 Nr. 2 ZPO) und das Auskunftsbegehren sei auch nicht im Wege der Stufenklage (§ 254 ZPO) geltend gemacht worden. Laut BAG ist daher unklar, von welchen E-Mails der Kläger genau eine Kopie begehrt. Solange die Nachrichten aber nicht konkret bezeichnet werden, könnten sie nach einem Urteil auch nicht vollstreckt werden (s. Pressemitteilung des BAG vom 27.4.2021).

Hintergrund und uneinheitliche Rechtsprechung
Seit der Einführung der DSGVO versuchen ehemalige Arbeitnehmer bzw. deren Vertreter häufig, den Anspruch auf Datenkopie nach Art. 15 Abs. 3 DS-GVO als prozesstaktisches Mittel zu einem Anspruch auf Aktenherausgabe auszuweiten, um zusätzliche Informationen zur Begründung ihrer Klage zu erlangen oder um Druck für die Zahlung einer höheren Abfindung auszuüben.

Die Rechtsprechung zur Reichweite des Auskunftsanspruchs ist sehr uneinheitlich. Während beispielsweise das LG Köln (Urt. v. 18. März 2019 – Az.: 26 O 25/18) den Auskunftsanspruch eher restriktiv beurteilt und vermeiden will, dass Arbeitnehmer eine unzulässige Ausforschung des Arbeitgebers betreiben, legten das LAG Baden-Württemberg (Urteil v. 20. Dezember 2018 – Az.: 17 Sa 11/18) und das OLG Köln (Urteil vom 26. Juli 2019 – 20 U 75/18) ihren Entscheidungen einen eher weit gefassten Datenbegriff zugrunde. Das LG Heidelberg hat mit Urteil vom 6. Februar 2020 (Az.: 4 O 6/19) zumindest einen Auskunftsanspruch bezogen auf Backup-Dateien eines E-Mail-Kontos wegen des unverhältnismäßigen Aufwands in der Wiederherstellung abgelehnt.

Ausblick
Das BAG zieht sich in seiner aktuellen Entscheidung auf die oben geschilderten, zivilprozessualen Vorgaben zurück und lässt damit auch die Frage, ob das Recht auf Überlassung einer Kopie gem. Art. 15 Abs. 3 DSGVO auch die Erteilung eines Duplikats von E-Mails umfassen kann, weiterhin offen.

Die Entscheidung des BAG ist dennoch für die Praxis nicht unbedeutend. Denn das BAG hat klargestellt, dass die betroffene Person, die die Auskunft einfordert, deutlich machen muss, welche E-Mails ihr in Kopie zur Verfügung gestellt werden sollen. Leider hat das BAG hier deutliche Worte vermissen lassen.

Das BAG hätte zudem die Möglichkeit gehabt, die Frage, ob das Recht auf Überlassung einer Kopie nach den Vorgaben der DSGVO auch eine Kopie E-Mails umfassen kann, dem EuGH zur Beantwortung vorzulegen. Auch dies hat das BAG nicht getan und es ist daher gut möglich, dass das BAG meint, dass der EuGH anderer Auffassung ist und die Sache anders entschieden hätte.

Der Auskunftsanspruch des Art. 15 DSGVO schwebt damit weiter wie ein Damoklesschwert über jedem (ehemaligen) Arbeitsverhältnis. Das BAG hat mit der aktuellen Entscheidung aber zumindest die Hürde für die Geltendmachung des Auskunftsanspruchs erhöht. Der Antrag auf Erteilung einer „Datenkopie“ nach Art. 15 Abs. 3 DSGVO muss jetzt jedenfalls ausreichend konkretisiert sein. Es bleibt abzuwarten, ob das BAG in den Entscheidungsgründen, die noch nicht veröffentlicht sind, weitere Angabe dazu macht, wie eine Konkretisierung aussehen sollte.

Esther Noske, Frankfurt/Main
e.noske@skwschwarz.de

Bayerische Datenschutzaufsicht zeigt Mailchimp Anwender gelbe Karte – kein Bußgeld, aber letzte Warnung

Während die große Schar der Datenschutzanwender in Deutschland immer noch auf ein Signal der Aufsichtsbehörden wartet, wie ein praktisch umsetzbarer Kompromiss zwischen modernen Cloud Services einerseits und dem Datenschutz andererseits aussehen könnte, ist nun die erste Entscheidung hierzu seitens des Bayerischen Landesaufsichtsamts für den Datenschutz (BayLDA) bekannt geworden. Mit Datum 15.3.2021 hat die Behörde einem Betroffenen gegenüber mitgeteilt, dass die Übermittlung von dessen E-Mail Adresse durch einen Verantwortlichen an den populären Newsletter Versender Mailchimp aufgrund fehlender zusätzlicher Datenschutzmaßnahmen unzulässig war (Az. LDA-1085.1-12159/20-IDV).

Der Sachverhalt
Der Betroffene hatte sich beim BayLDA bezüglich der Nutzung des Newsletter-Tools Mailchimp durch ein Münchner Unternehmen beschwert. Er gab an, dass die Weitergabe von E-Mail-Adressen von Abonnenten des Newsletters der Beschwerdegegnerin an den Anbieter von Mailchimp (The Rocket Science Group LLC, ein in den USA ansässiges Unternehmen) nach Art. 44 ff. DSGVO rechtswidrig sei und mit einem Bußgeld bestraft werden müsse. Demgegenüber hatte der Verantwortliche mitgeteilt, dass er Mailchimp nur zweimal genutzt habe und bereits die Nutzung eingestellt habe.

Die Übermittlung der E-Mail Adresse des Betroffenen an Mailchimp erfolgte auf Basis von EU-Standarddatenschutzklauseln (Standard Contractual Clauses - SCCs). Laut BayLDA gab es Anhaltspunkte dafür, dass der Anbieter von Mailchimp als „electronic communication service provider" unter das US-Überwachungsrecht (FISA702 (50 U.S.C. § 1881)) fällt. Daher könnte die Gefahr bestehen, dass die übertragenen E-Mail Adressen von US-Geheimdiensten eingesehen werden. Vor dem Hintergrund der EuGH-Entscheidung „Schrems II" (C-311/18) habe der Verantwortliche nicht geprüft, ob zusätzliche Maßnahmen zum Schutz der übertragenen Daten vor US-Überwachung getroffen worden seien. Allein die fehlende Prüfung ergänzender Schutzmaßnahmen war der Grund, aus dem die Aufsichtsbehörde einen Verstoß gegen die DSGVO feststellte.

Das BayLDA sah allerdings keine Veranlassung, den Verantwortlichen auch noch mit einem Bußgeld zu bestrafen. Die nur gelegentliche Nutzung und die Tatsche, dass nur die wenig sensiblen E-Mail Adressen in die USA übermittelt wurden, gemeinsam mit der Feststellung, dass noch immer keine finale Leitlinie der Aufsichtsbehörden zum internationalen Datentransfer vorliege, machten aus dem Verstoß für das BayLDA einen nur leicht fahrlässigen Verstoß, der keine Geldbuße rechtfertige. Das ist für Unternehmen (zumindest in Bayern) ebenso beruhigend wie der Hinweis des BayLDA, dass Bußgelder nicht der Durchsetzung der Rechte und Freiheiten einzelner Betroffener dienten und daher diese Betroffenen auch nicht die Verhängung von Bußgeldern erzwingen könnten. Deren Wiedergutmachungsinteresse ist im Rahmen des Schadensersatzes nach Art. 82 DSGVO geltend zu machen.

Praxistipp:
Für die Kunden von Mailchimp ist die Feststellung wichtig, dass dessen Nutzung per se noch nicht datenschutzwidrig sein soll. Allerdings unterstreicht das BayLDA auch, dass allein vertragliche Maßnahmen (auch keine SCC) nicht als Schutz bei der Übermittlung personenbezogener Daten an US Service Provider ausreichen. Zusätzliche Maßnahmen technisch oder organisatorischer Art wie z.B. Verschlüsselung oder die Einwilligung der Betroffenen müssen jedenfalls geprüft werden. Auch die Bedeutung der Dokumentation der Prüfung wird durch die Entscheidung nochmal deutlich hervorgehoben. Für Neuanmeldungen zu Newslettern wäre zu prüfen, ob zusätzlich eine ausdrückliche und informierte Einwilligung nach Art. 49 Abs. 1 Buchst. a DSGVO eingeholt wird. Erfreulich ist auch der Umstand, dass das BayLDA allzu optimistischen Verbraucherklägern die Grenzen ihres Handelns aufgezeigt hat und insbesondere dem Einzelnen das Recht auf die Verhängung von Bußgeldern gegen Dritte verwehrt hat.

Dr. Matthias Orthwein, München
m.orthwein@skwschwarz.de