DER BREXIT UND SEINE AUSWIRKUNGEN AUF DEN DATENSCHUTZ

Nach mehr als vier Jahren scheinbar endloser Verhandlungen seit der Entscheidung des britischen Referendums von 2016, die Europäische Union zu verlassen, schlossen die Parteien zum letztmöglichen Zeitpunkt am 24. Dezember 2020 ein Handels- und Kooperationsabkommen (im Folgenden als „TCA“ bezeichnet) ab. Das TCA legt Regelungen zu verschiedenen Bereichen fest, einschließlich der Verarbeitung von personenbezogenen Daten.

I. DIE FOLGEN FÜR DATENÜBERTRAGUNGEN

Nach dem seit dem 1. Januar 2021 geltenden TCA wurde eine Übergangsphase bis zum 30. Juni 2021 vereinbart, während der jegliche Übertragung von personenbezogenen Daten vom EWG in das UK nicht als Datenübertragung in ein Drittland angesehen wird. Dies ermöglicht eine Übertragung von personenbezogenen Daten in das Vereinigte Königreich unter Beachtung der DSGVO aber ohne weitere Beschränkungen. Ohne diese Vereinbarung würde das UK als Drittland gelten. Sobald die Übergangsphase endet und die Europäischen Kommission keinen Angemessenheitsbeschluss fasst, müssen andere Maßnahmen nach den Art. 44 ff. DSGVO ergriffen werden, um Datentransfers von der EU in das UK als Drittland zu legitimieren.

II. ANWENDBARES RECHT

Als Europäisches Recht gilt die DSGVO seit dem 1. Januar 2021 nicht mehr im Vereinigten Königreich. Soweit der Anwendungsbereich der DSGVO eröffnet ist, also insbesondere in Bezug auf Verantwortliche oder Auftragsverarbeiter mit Sitz in UK, die Personen im EWG Waren oder Dienstleistungen anbieten oder deren Verhalten beobachten, bleibt sie weiterhin gültig.

Das Vereinigte Königreich hat zudem eine britische Variante der DSGVO zum 01.01.2021 in Kraft gesetzt, das sog. „UK-GDPR“, welches im Wesentlichen die Regelungen der DSGVO übernommen hat. Ferner gilt auch der „UK Data Protection Act 2018“ (DPA 2018) im Vereinigten Königreich und auch für Verantwortliche und Auftragsverarbeiter, die wiederum Briten Waren oder Dienstleistungen anbieten oder deren Verhalten beobachten.

III. ZUSTÄNDIGE BEHÖRDE FÜR GRENZÜBERSCHREITENDE ANGELEGENHEITEN

Um bei grenzüberschreitenden Streitigkeiten zwischen der EU und dem UK nach dem 01. Januar 2021 in den Genuss der “One-stop Shop-Regelung” innerhalb der EU zu kommen, ist es für in dem UK ansässige Verantwortliche und Auftragsverarbeiter erforderlich, auch eine Niederlassung in einem Mitgliedsstaat der EU zu haben.

IV. EU-VERTRETER

Ab dem 1. Januar 2021 ist es für Verantwortliche und Auftragsverarbeiter, die ihren Sitz im

Vereinigten Königreich haben und auf welche die DSGVO nach Art. 3 Abs. 2 Anwendung findet, erforderlich, einen Vertreter nach Art. 27 DSGVO zu bestimmen.

V. ANGEMESSENHEITSBESCHLUSS

Auch das UK unterliegt dem Angemessenheitserfordernis der DSGVO, wonach Datenübertragungen in ein Drittland voraussetzen, dass dort ein angemessenes Datenschutzniveau vorliegt. Angemessenheit ist gegeben, wenn die Maßnahmen zum Schutz der Daten und die daraus resultierenden Rechte der Betroffenen, denen in der EU entsprechen. Sie sollten überlegen, welche alternativen Sicherungsmaßnahmen nach den Art. 44 ff. DSGVO für Sie in Betracht kommen, sollte die Europäische Kommission keinen Angemessenheitsbeschluss erlassen

DATENÜBERTRAGUNGEN IN DRITTLÄNDER

Nach den Vorgaben der DSGVO ist eine Übermittlung personenbezogener Daten in ein Drittland (das ist ein Staat außerhalb der EU) nur dann zulässig, wenn dieses Drittland ein angemessenes Schutzniveau gewährleistet und das durch die DSGVO gewährleistete Schutzniveau für natürliche Personen nicht untergraben wird. Regelungen zur Zulässigkeit einer Datenübermittlung in ein Drittland finden sich in den Art. 44-49 DSGVO. Da Großbritannien kein EU-Mitglied mehr ist, gilt es mit dem Ende der vereinbarten Übergangsphase nach dem 30. Juni 2021 grundsätzlich als Drittland.

I. ANGEMESSENHEITSBESCHLUSS

Wie dargestellt, erfolgt die Feststellung, ob für die Datenübermittlung in ein Drittland ein angemessenen Schutzniveau gewährleistet ist, u. a. per Angemessenheitsbeschluss. Anerkennt die Europäische Kommission mit einem Angemessenheitsbeschluss, dass ein ausreichendes Schutzniveau in einem Drittland gewährleistet ist, dürfen Verantwortliche aus EU-Mitgliedstaaten personenbezogene Daten in dieses Drittland übermitteln, ohne dass darüber hinaus zusätzliche Garantien erforderlich sind.

II. ALTERNATIVE RECHTSGRUNDLAGEN

Neben einem Angemessenheitsbeschluss kommen bspw. noch folgende Rechtsgrundlagen in Betracht:

- Standarddatenschutzklauseln,
- Ad-hoc-Verträge, die durch die zuständige Datenschutzbehörde autorisiert wurden,
- Binding Corporate Rules (BCR), die durch die zuständige Datenschutzbehörde autorisiert wurden,
- Einholung der ausdrücklichen Einwilligung von betroffenen Personen, soweit sie auf das Fehlen eines Angemessenheitsbeschlusses und angemessener Sicherheitsmaßnahmen hingewiesen wurden; oder
- bei Fehlen eines Angemessenheitsbeschlusses und angemessener Sicherheitsmaßnahmen: Durchführung oder Abschluss eines Vertrags, Übermittlung aus wichtigen Gründen des öffentlichen Interesses oder Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Zu klären ist, welche der von der DSGVO vorgesehenen, alternativen Rechtsgrundlagen für den Datentransfer geeignet ist. Dafür bedarf es einer Prüfung im Einzelfall samt Risikoevaluierung (Häufigkeit des Datentransfers, Datenarten, sonstige Verarbeitungskriterien etc.).

Im Hinblick auf die kürzlich ergangene "Schrems"-Entscheidung des EuGH ist bei dem Einsatz der EU-Standardvertragsklauseln darauf zu achten, dass stets eine Risikobewertung im Hinblick darauf erfolgen muss, ob das geltende Recht im Zielland ein angemessenes Datenschutzniveau gewährleistet. Was das für die Praxis bedeutet, bleibt abzuwarten.

III. SANKTIONEN BEI VERLETZUNG VON ART. 44 FF. DSGVO

Wenn keine valide Rechtsgrundlage für eine Datenübertragung gegeben ist, liegt ein Verstoß gegen die DSGVO vor und es droht eine Strafe in Höhe von bis zu 20 Millionen EUR oder 4% des weltweiten Jahresumsatzes.

Unternehmen müssen daher unverzüglich reagieren, sollte die Kommission nach Ende der Übergangsphase keinen Angemessenheitsbeschluss zu Großbritannien fassen.

VEREINBARUNG MIT DEM VEREINIGTEN KÖNIGREICH ÜBER DIE GRENZÜBERSCHREITENDE DATENVERARBEITUNG

I. DAS HANDELS- UND KOOPERATIONSABKOMMEN

Die wichtigste Bestimmung des TCA zum Datenschutz sieht vor, dass personenbezogene Daten für einen Zeitraum von vier Monaten ab dem Ende der Übergangszeit (1. Januar 2021) ohne weitere Garantien von der EU in das Vereinigte Königreich übertragen werden dürfen. Auch vereinbart wurde, dass diese viermonatige Frist automatisch um weitere zwei Monate verlängert wird, sofern sich weder die EU noch Großbritannien anderweitig erklärt.

II. ANGEMESSENHEITSBESCHLUSS

Ein Angemessenheitsbeschluss ist eine formelle Entscheidung der Europäischen Kommission gemäß Art. 45 DSGVO, welche bestätigt, dass ein Drittland über ein angemessenes Datenschutzniveau verfügt, wie es von der DSGVO gefordert wird. Großbritannien bemüht sich gegenwärtig um den Erhalt eines solchen Angemessenheitsbeschlusses. Der Angemessenheitsbeschluss führt dazu, dass personenbezogene Daten von der EU (inklusive Norwegen, Liechtenstein und Island) in das Drittland ohne weitere Schutzmaßnahmen übertragen werden können. Sobald die Europäische Kommission einen Angemessenheitsbeschluss erlässt, endet die mit dem TCA vereinbarte Übergangsphase.

III. ALTERNATIVLÖSUNGEN

Die britische Datenschutzbehörde (das Information Commissioner's Office), wies darauf hin, dass Unternehmen sich während der Übergangsphase auch darauf vorbereiten sollten, alternative Datenübertragungsmechanismen zu installieren für den Fall, dass kein Angemessenheitsbeschluss ergehen sollte. Die Datenübertragungsmechanismen, die eine alternative Lösung bieten können, sind in den Artikeln 46 bis 50 der DSGVO festgelegt. Diese Bestimmungen regeln die generellen Anforderungen der Übertragung personenbezogener Daten vom EWG in ein Drittland, d.h. ein Land außerhalb des EWG. Die Einstufung des UK als Drittland ist durch die vereinbarte Übergangsphase verschoben.

IV. WEITERE KOOPERATION

Die EU und das Vereinigte Königreich haben außerdem vereinbart, auf bilateraler und multilateraler Ebene in Datenschutzfragen durch Erfahrungsaustausch und Kriminalitätsbekämpfung zusammenzuarbeiten. In Bezug auf den Ort der Datenspeicherung einigten sich beide Parteien, dass keiner von ihnen die Speicherung oder Verarbeitung personenbezogener Daten in ihrem Hoheitsgebiet verlangt.

NEUE DATENSCHUTZREGELN IM UK: DER UK-VERTRETER

Wohl hat die Briten einiges an der EU gestört. Die DSGVO gehörte aber offensichtlich nicht dazu, denn zum 1. Januar 2021 wurde eine „UK-GDPR“ in Kraft gesetzt, die ihrer Vorgängerin inhaltlich sehr ähnelt.

I. DER UK-VERTRETER

Übernommen wurde insbesondere auch das Erfordernis eines „Vertreters“, wie wir es aus Art. 27 DSGVO für nicht in der EU ansässige Firmen kennen.

Unternehmen, die keine Niederlassung in Großbritannien haben, aber Waren oder Dienstleistungen gegenüber UK-Bürgern anbieten oder deren Verhalten überwachen, haben nach Art. 27 UK-GDPR einen Vertreter zu bestellen. Dies umfasst insbesondere Anbieter aus dem Onlinebereich wie aber auch IT-Unternehmen, die derartige Daten für ihre Kunden verarbeiten. Es gilt selbst dann, wenn das IT-Unternehmen nur eine Auftragsverarbeitung vornimmt, also die Daten im Namen eines Dritten verarbeitet.

Wie sein europäisches Vorbild soll der UK-Vertreter als Ansprechpartner vor Ort fungieren und ggf. anfallende Kommunikation mit der britischen Datenschutzbehörde „British Information Commissioner's Office“ übernehmen. Er ist zudem Zustellungsempfänger für den gesamten Schriftverkehr mit Bezug zum Datenschutz in dem UK. Das soll vermeiden, dass man durch Überwindung der Landesgrenzen bei der Kommunikation zu viel Zeit verliert.

II. QUALIFIKATION DES VERTRETERS

Der Vertreter kann eine Firma oder natürliche Person sein, die in dem UK niedergelassen oder wohnhaft ist. Er ist schriftlich gegenüber der britischen Datenschutzbehörde zu benennen. Er muss Zugriff auf das Verarbeitungsverzeichnis des Unternehmens haben (Art. 30 UK-GDPR) und umfassend bevollmächtigt sein, für das Unternehmen zu handeln. Entsprechend sollte er über ausreichend Kenntnisse im Datenschutzrecht verfügen. Er muss zudem in der Datenschutzerklärung des Unternehmens mit seinen Kontaktdaten genannt werden.

III. MÖGLICHE SANKTIONEN

Die Sanktionen bei einem Verstoß gegen die UK-GDPR sind ähnlich drakonisch wie die nach der DSGVO: Es können Bußgelder bis zu GBP 8.700.000 bzw. 2% des weltweiten Jahresumsatzes eines Unternehmens verhängt werden. Ergo sollten auch bei personenbezogenen Daten von Personen aus dem Vereinigten Königreich die gleichen Schutzmaßnahmen ergriffen und Prinzipien angewendet werden wie bei Daten von EU-Bürgern.

IHRE BREXIT-CHECKLISTE IN SACHEN DATENSCHUTZ

Die folgende Liste soll eine Hilfestellung geben, um zu eruieren, welche Schritte Ihr Unternehmen zur Anpassung an die durch den Brexit verursachte neue Rechtslage ergreifen muss.

- Welche Daten Ihres Unternehmens werden in dem Vereinigten Königreich verarbeitet?
- Welche Daten von britischen Staatsbürgern werden durch Ihr Unternehmen verarbeitet?
- Liegt für jeden Verarbeitungsprozess eine Rechtsgrundlage vor?
- Ist im Verarbeitungsverzeichnis Großbritannien als neues Drittland vermerkt?
- Bei Einwilligungen: Sind diese ausreichend dokumentiert oder müssen Informationen zu der neuen Rechtslage nachgereicht werden?
- Müssen Maßnahmen ergriffen werden, um ein angemessenes Datenschutzniveau sicherzustellen? Liegen Ihnen seitens der Unternehmen, mit denen Sie in dieser Hinsicht zusammenarbeiten, ausreichende Informationen vor?
- Sind Datenschutzerklärungen (Mitarbeiter, Webseite, Kunden) zu ergänzen bezgl. eines Hinweises auf die Datenverarbeitung in dem UK oder auf einen UK-Vertreter?
- Ist bei Auskunftsanfragen von Betroffenen nach Art. 15 DSGVO sichergestellt, dass die Betroffenen auch über eine Datenverarbeitung in Großbritannien informiert werden?
- Müssen bezgl. einzelner Verarbeitungsprozesse neue Datenschutz-Folgenabschätzungen durchgeführt bzw. diese aktualisiert werden?

KONTAKT

Bulgarien:
Cornelia Draganova
Cornelia.Draganova@schindhelm.com

Deutschland:
Karolin Nelles
Karolin.Nelles@schindhelm.com

Sarah Schlösser
Sarah.Schloesser@schindhelm.com

Frankreich:
Maurice Hartmann
Maurice.Hartmann@schindhelm.com

Italien:
Tommaso Olivieri
Tommaso.Olivieri@schindhelm.com

Österreich:
Michael Pachinger
M.Pachinger@scwp.com

Julia Spitzbart
J.Spitzbart@scwp.com

Polen:
Anna Materla
Anna.Materla@sdzlegal.pl

Rumänien:
Helge Schirkonyer
Helge.Schirkonyer@schindhelm.com

Spanien:
José Tornero
J.Tornero@schindhelm.com

Tschechien/Slowakei:
Monika Wetzlerova
Wetzlerova@scwp.cz

Türkei:
Müge Şengönül
Muge.Sengonul@schindhelm.com

Ungarn:
Beatrix Fakó
B.Fako@scwp.hu

Herausgeber, Medieninhaber, Redaktion: Saxinger Chalupsky & Partner Rechtsanwälte GmbH | Böhmerwaldstraße 14 | 4020 Linz | FN 185084 h LG Linz | DVR : 0623695 | Tel: +43 732 603030 linz@scwp.com | Saxinger, Chalupsky & Partner Rechtsanwälte GmbH ist Mitglied der SCWP Schindhelm Services SE, Allianz europäischer Wirtschaftskanzleien | Alle Angaben erfolgen trotz sorgfältiger Bearbeitung ohne Gewähr und können im Einzelfall die individuelle Beratung nicht ersetzen. Die Haftung der Autoren oder der Herausgeberin ist ausgeschlossen.