DIE DSGVO UND DER BREXIT – WAS IST TUN, WENN DER AUFTRAGSVERARBEITER IM VEREINIGTEN KÖNIGREICH SITZT?

1. Vorab: Der Stand der Dinge nach dem 25. Mai 2018 - wie sind die Unternehmen aufgestellt?

Meiner Auffassung nach hat die DSGVO in erster Linie die KMUs erheblich belastet. Der Umfang der Verordnung und die Abstraktheit der Vorschriften machten es nicht einfach, die Vorgaben nachzuvollziehen. Schon die angeblich „einfachsten“ Begrifflichkeiten, wie die Definition der „personenbezogenen Daten“ in Artikel 4, Ziffer 1 der DSGVO, haben Fragen hervorgerufen.

Noch schwieriger war es die Vorgaben in die Praxis umzusetzen, bei 99 Artikeln und 173 „Gründen“, die eigentlich nur Rahmenbestimmungen enthalten und eine Anleitung für die konkrete Umsetzung der mit empfindlichen Sanktionen bewehrten Vorgaben leider vermissen lassen.

Eine weitere und gewaltige Schwierigkeit ist, dass noch keinerlei Gerichtsentscheidungen zur DSGVO oder eine Durchsetzungspraxis der Aufsichtsbehörden existieren, was die Orientierung für Unternehmen bedeutend erschwert. Die Qualität der Rechtsberatung im Vorfeld war meines Erachtens durchwachsen, von hervorragend bis offensichtlich falsch. Viele KMUs können sich eine hochwertige Rechtsberatung in benötigter Breite gar nicht leisten. Die ganz „Großen“, wie zum Beispiel Facebook, gegen die sich die DSGVO wohl richtete, können sich mit ihren Teams von Beratern, Anwälten, Technikern und anderen Fachprofis sowieso ohne weiteres anpassen.

Man muss sich im Klaren sein, dass die DSGVO den Unternehmen abverlangt sowohl die beträchtlichen organisatorischen, technischen und rechtlichen Maßnahmen zu implementieren, um den Vorgaben der DSGVO gerecht zu werden als auch jederzeit in der Lage zu sein, die Compliance mit der DSGVO u.a. durch detaillierte Dokumentation nachzuweisen. Wie gesagt, das ist eine gewaltige Belastung, vor allem für kleinere Unternehmen.

Bei alldem ist es nachvollziehbar, wenn viele Unternehmer unsicher sind bzw. nicht von sich guten Gewissens behaupten können, alles ausreichend und richtig umgesetzt zu haben. Ich

glaube, eine solche Sicherheit ist unter gegebenen Umständen kaum möglich.

Erst die behördliche Durchsetzungspraxis der Mitgliedsstaaten wird zeigen, wie die DSGVO letztendlich zu beurteilen ist. Eine der Fragen dabei ist, ob die nationalen Aufsichtsbehörden genug qualifiziertes Personal und finanzielle Mittel haben werden, um der DSGVO den „Lebensgeist einzuhauchen“. Interessant wird auch zu beobachten sein, wie die Konsistenz der Aufsichtspraxis über die Mitgliedsstaaten hinweg in der Praxis gewährleistet wird. Die behördliche Durchsetzungspraxis wird die sprichwörtliche Stunde der Wahrheit für die DSGVO sein.

2. Mögliche Szenarien nach dem Brexit: UK als „Drittland“ oder eine Übernahme der DSGVO durch die Briten?

Die britische Regierung tut gerade alles, um nach dem Brexit kein „Drittland“ im Sinne der DSGVO zu sein. „The House of Lords European Union Committee“ hat bereits 2017 Bedenken geäußert, dass eine Divergenz in datenschutzrechtlichen Standards eine Art zollähnliches Handelshindernis sein könnte, das dem Vereinigten Königreich zum Nachteil gereichen könnte. Datentransfers zwischen der EU in dem Vereinigte Königreich sind also wichtig für die britischen Unterhemen.

Nach dem Brexit würde das Vereinigte Königreich ein „Drittland“ im Sinne der DSGVO werden. Das Vereinigte Königreich muss dann die Europäische Kommission überzeugen, dass es ein adäquates Schutzniveau für die Daten, die im Vereinigten Königreich verarbeitet werden, bieten kann, damit Datentransfers zwischen dem Vereinigten Königreich und der EU wie vor dem Brexit weiterhin möglich sind. Im Detail ist der Vorgang in den Absätzen 1 bis 3 des Artikels 45 DSGVO beschrieben. In Absatz 1 des Artikels 45 der DSGVO heißt es:

„Eine Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation darf vorgenommen werden, wenn die Kommission beschlossen hat, dass das betreffende Drittland, ein Gebiet oder ein oder mehrere spezifische Sektoren in diesem Drittland oder die betreffende internationale Organisation ein angemessenes Schutzniveau bietet. Eine solche Datenübermittlung bedarf keiner besonderen Genehmigung.“

Zu diesem Zweck haben die Briten das Data Protection Act 2018 erlassen. Die britische Regierung hat entschieden, die DSGVO bzw. die GDPR, wie die Verordnung auf Englisch

heißt, in das englische Recht einzugliedern.

Es ist jedoch der Europäischen Kommission überlassen, darüber zu entscheiden, ob das Vereinigte Königreich ein angemessenes bzw. ein adäquates datenrechtliches Schutzniveau bietet, damit das Vereinigte Königreich von der EU nicht wie ein „Drittland“ behandelt wird. Ob und wann die Kommission darüber entscheiden wird, liegt ebenfalls in den Händen der Kommission. Auch kann die Kommission die getroffene positive Entscheidung nachträglich rückgängig machen, falls sich mit der Zeit Divergenzen im Schutzniveau entwickeln, das kann man ebenfalls Artikel 45 entnehmen.

Die Kriterien, die die Kommission bei der Beurteilung des „gebotenen Schutz-niveaus“ zugrunde legt, sind Artikel 45 Absatz 2 DSGVO zu entnehmen. Der Text der DSGVO ist online erhältlich.

Übrigens, ein Novum ist, dass die Kommission auch die Adäquanz von (nur) bestimmten Industriesektoren anerkennen kann. Es gibt einige Sektoren, die dafür besonders geeignet sind, da sie bereits jetzt relativ hohe Datenschutzstandards aufweisen, zum Beispiel Versicherungen.

Letztlich wird also die Europäische Kommission entscheiden, nicht das Vereinigte Königreich. Wie gesagt, hat das Vereinigte Königreich seine Entscheidung bereits getroffen. Wie die Entscheidung der Kommission ausfallen wird, kann man zur Zeit leider, wie bei allem, was mit Brexit zu tun hat, unmöglich voraussagen.

3. Konkret: Was sollen Unternehmen in Bezug auf bestehende Auftragsverarbeitungsverträge tun, zum Beispiel wenn ein EU-Unternehmen mit einem Datenverarbeiter im Vereinigten Königreich arbeitet?

Zuallererst wäre die eigentlich selbstverständliche Tatsache erwähnenswert, dass gemäß Art. 28 DSGVO die Verarbeitung durch einen Auftragsverarbeiter auf der Grundlage eines Vertrags erfolgen muss, der den Vorgaben des Absatzes 3 des Artikels 28 entsprechen muss. Die Einzelheiten kann man dort nachlesen.

Die einfachste Variante Nr.1: Vertragspartner innerhalb des EWR

Am einfachsten und am sichersten ist es natürlich mit Partnern bzw. Auftragsverarbeitern innerhalb des EWR zu arbeiten, wenn das im Einzelfall möglich ist.

Die einfachste Variante Nr.2: Der Angemessenheitsbeschluss der Kommission gemäß Art. 45 DSGVO

Falls die Europäische Kommission die Adäquanz des britischen Schutzniveaus anerkennt, würde damit grundsätzlich die vor Austritt Großbritanniens Anfang 2019 bestehende Lage in Bezug auf Datenschutz fortgesetzt werden.

Die etwas komplizierteren Varianten

Unternehmen sollten sich der Risiken bewusst sein, wenn sie die personenbezogene Daten ins Ausland übermitteln, zum Beispiel bezüglich Kunden oder Arbeitnehmer. Auch nach der DSGVO dürfen personenbezogene Daten nicht ins Ausland außerhalb des Europäischen Wirtschaftsraums (EWR) übermittelt werden ohne geeignete Schutzmaßnahmen. Die Strafen für die Verstöße sind signifikant: von erheblichen Geldbußen bis hin zu Sperrung der Übertragung.

Sollte die Kommission die Anerkennung der Adäquanz verweigern, müssten die betroffenen Unternehmen daher auf andere Mittel zurückgreifen, die ihnen die DSGVO zum Glück zur Verfügung stellt. Das Ganze nennt sich „Datenübermittlung vorbehaltlich geeigneter Garantien“ und findet sich in Art. 46 der DSGVO, vor allem in dessen Absatz 2. Danach dürfen die „personenbezogenen Daten“ in Drittländer nur übermittelt werden, wenn geeignete Garantien vorgesehen wurden.

Verbreitet sind u.a. die folgenden drei Typen der geeigneten Garantien:

- Standarddatenschutzklauseln
- Verbindliche interne Datenschutzvorschriften
- EU-US „Privacy Shield“

In Artikel 46 Absatz 2 Buchstaben (e) und (f) sind zwei neue geeignete Maßnahme vorgesehen: genehmigte Verhaltensregeln und genehmigte Zertifizierungsmechanismen. Die weitere Entwicklung wird zeigen, ob sich diese neue Formen werden etablieren können.

Auf das EU-US „Privacy Shield“ wird nachfolgend nicht weiter eingegangen. Das wird in einem separaten Beitrag erörtert werden.

Standardschutzklauseln

Unter den in Absatz 2 des Art. 46 aufgelisteten Maßnahmen finden sich ebenfalls die Standarddatenschutzklauseln, die von der Europäischen Kommission erlassen werden. Darunter fallen auch bereits seit Jahren existierende Standardvertragsklauseln der Europäischen Kommission, zum Beispiel für Auftragsverarbeitungen. Diese Klauseln sind u.a. online mit wenigen Mausklicks auf den Webseiten der Europäischen Union zu finden.

Die Standardvertragsklauseln der Europäischen Kommission sind konzipiert worden, damit Datenexporteure und Datenimporteure keine Verträge aushandeln und die Genehmigung der Aufsichtsbehörden einholen müssen. Mit anderen Worten, um den international tätigen Unternehmen das Leben deutlich zu erleichtern. Derzeit gibt es zwei Varianten von Standardvertragsklauseln, die für Übermittlungen zwischen den Verantwortlichen gelten und zwei Varianten von Standardvertragsklauseln, die für Übermittlungen zwischen den Verantwortlichen und Auftragsverarbeitern gelten. Bezüglich der Gültigkeit der Standardvertragsklauseln wird derzeit Rechtsstreit geführt. Es ist wahrscheinlich, dass die Standardvertragsklauseln aktualisiert werden, um die Anforderungen der DSGVO zu reflektieren. Die Standardvertragsklauseln bleiben in Kraft bis sie gegebenenfalls gemäß Artikel 46 Absatz 5 geändert oder ersetzt werden.

Die Standardvertragsklauseln sollten in den Vertrag mit dem im Vereinigten Königreich ansässigen Auftragsverarbeiter aufgenommen werden.

Verbindliche interne Datenschutzvorschriften

Interessant sind auch „verbindliche interne Datenschutzvorschriften“ gemäß Art. 47, insbesondere für Unternehmensgruppen, deren Gesellschaften in und außerhalb des EWR

tätig sind. Das ist ein nützliches Werkzeug, nicht nur um Transfers personenbezogener Daten in „Drittländer“ gemäß den Vorgaben der DSGVO abzusichern, sondern auch um einen global einheitlichen Datenschutzstandard innerhalb der Unternehmensgruppe zu etablieren, ohne sich mit Verträgen „abzumühen“, wie vorstehend beschrieben. Vermutlich werden zahlreiche Unternehmen von dieser Vorschrift Gebrauch machen.

Sonstiges

Einen Blick wert sind auch die Ausnahmetatbestände des Artikels 49 sowie die dazugehörigen Gründe (111) und (112) der DSGVO. Die wenigen Absätze kann man einfach mal durchlesen.

4. Wie sollen Unternehmen die bis zum Brexit übrig bleibende Zeit am effektivsten nutzen?

Man sollte bereits jetzt die Maßnahmen gemäß den Artikeln 46, 47 DSGVO ins Auge fassen und überlegen, welche Alternative die eigene unternehmerische Wirklichkeit am besten abbilden würde, wie man es umsetzen könnte sowie natürlich was dabei organisatorisch und finanziell zu bewerkstelligen wäre. Nochmals, die einfachste Lösung ist natürlich die Zusammenarbeit mit Partnern innerhalb des EWR.

Wie bei allen grenzüberschreitenden Verträgen mit Vereinigtem Königreich, sollte man unbedingt an die sog. Brexit-Klauseln denken. Wie der Name sagt, kann man sich mit den Brexit-Klauseln für den Fall des Brexits absichern, indem etwa Preisanpassungen, Neuverhandlungen oder Kündigungsrechte vereinbart werden. Es existieren bereits diverse Varianten von Brexit-Klauseln, von relativ einfachen bis sehr ausdifferenzierten bzw. sehr anspruchsvollen und sehr effektiven Varianten. Brexit-Klauseln können angesichts der mit Brexit verbundenen Unsicherheiten für beide Seiten interessant sein, es loht sich daher auch bei bereits geschlossenen Verträgen mit dem Vertragspartner über die entsprechende Vertragsergänzung zu sprechen. Jetzt wäre die Zeit, sich diesem Themenbereich zu widmen.

Stand der Darstellung: Juni 2018