Brexit

Checkliste für Digitalunternehmen

www.bvdw.org

Brexit – Checkliste für Digitalunternehmen

Inhaltsverzeichnis

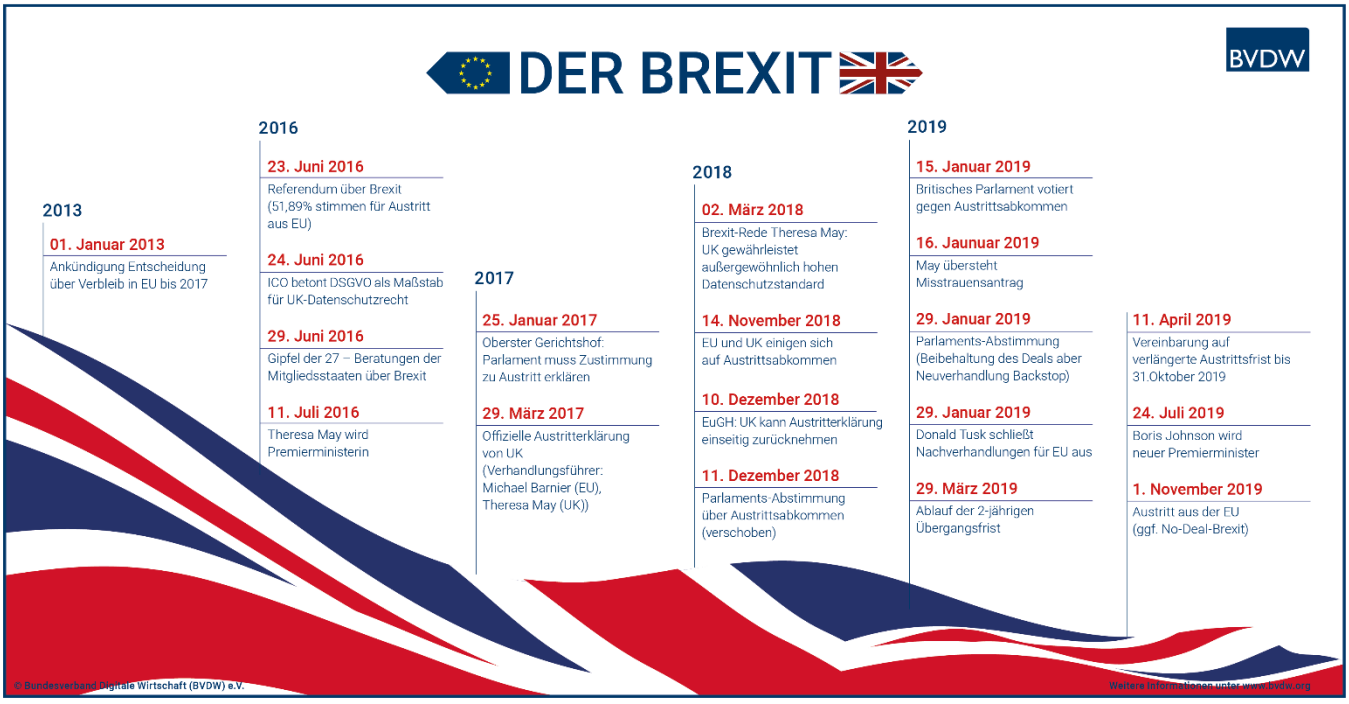
Brexit – Digitalunternehmen müssen vorbereitet sein 2
I. Datenschutz 3
1. Was regelt das ausgehandelte Austrittsabkommen mit Blick auf Datentransfers? 3
2. Was passiert bei ungeregeltem Brexit? 4
3. Rechtsgrundlagen für Datentransfers 4
4. Angemessenheitsbeschluss der EU-Kommission 5
5. Verwendung von EU-Standardvertragsklauseln 5
6. Einwilligung der Betroffenen 6
7. Datentransfer erforderlich zur Vertragserfüllung 6
8. Verbindliche Unternehmensregeln/Binding Corporate Rules (BCR) 6
II. Beschäftigte im Unternehmen 6
III. Steuern und Zölle 7
IV. EU-Marken und Patente 7
Über uns
Impressum

Brexit – Digitalunternehmen müssen vorbereitet sein

Am 29. März 2017 hat das Vereinigte Königreich (VK) offizielle den Austritt aus der Europäischen Union beantragt. Dem Antrag voraus ging ein Referendum, in welchem sich 51,89% der Briten für diesen Schritt ausgesprochen hatten. Über zwei Jahre verhandelten die Vertreter der EU und VK über die Bedingungen des Austritts mit dem Ziel der weitgehenden Gewährleistungen bestehender Wirtschaftsbedingungen.

Die Verhandlungen schlossen im November 2018 mit einem umfangreichen Vertragstext. Das britische Parlament stimmte in der Folge allerdings mehrfach gegen das von der EU zusammen mit der Regierung um Theresa May ausgehandelte Austrittsabkommen. Zwar hatte das britische Parlament am 29. Januar 2019 noch einmal gegen einen ungeregelten Austritt und für weitere Gespräche gestimmt und sich EU und VK zuletzt auf eine Verlängerung der Austrittsfrist bis 31. Oktober 2019 verständigt. Sollte das Vereinigte Königreich das Austrittsabkommen noch vor diesem Datum ratifizieren, würde ein Austritt am ersten Tag des Monats erfolgen, der auf den Abschluss des Ratifizierungsverfahrens folgt.

Ohne eine Annahme bewegt sich das Vereinigte Königreich jedoch weiter auf einen ungeregelten Brexit zu. Nach der Wahl von Boris Johnson zum neuen Premierminister im Juli 2019 sieht es auch kaum noch danach aus, als ob ein No-Deal-Brexit nun noch abzuwenden sein wird. Neuverhandlungen mit der EU hatte Ratspräsident Tusk zuvor bereits eine Absage erteilt. In diesem Fall wäre das Vereinigte Königreich ab dem 01. November 2019 kein EU-Mitglied mehr.



Die Unternehmen der digitalen Wirtschaft (und nicht nur diese) sollten daher lieber vorbereitet sein. Großbritannien ist Deutschlands fünftwichtigster Handelspartner. Die EU-Kommission bezifferte den Wert der europäischen Datenökonomie bis 2020 auf bis zu 739 Milliarden Euro. Laut dem Chef der britischen Handelskammern BCC, Adam Marshall, befindet sich die britische Wirtschaft wegen der Unklarheiten über die zukünftigen Handelsbeziehungen zwischen EU und VK in einer „Schockstarre". Der deutsche Industrie- und Handelskammertag (DIHK) befürchtet „massive Auswirkungen", die der deutschen Wirtschaft bei einem ungeregelten Brexit drohen.

Unternehmen der digitalen Wirtschaft müssen sich jetzt dringend auf ein No-Deal-Szenario vorbereiten. Dies betrifft insbesondere solche Unternehmen die

1. eine Niederlassung oder Betriebsstätte in VK haben
2. mit Systemen/Software arbeiten, die aus VK heraus angeboten werden (Software as a Service (SaaS)
3. Bestellungen oder Lieferungen über einen VK-Dienstleister abwickeln

Vorbereitungen sind hier vor allem mit Blick auf folgende Bereiche dringend anzuraten:

1. Datenschutz
2. Beschäftige im Unternehmen
3. Steuern und Zölle
4. EU-Schutzrechte (Marken und Bezeichnungen)

Die EU-Kommission informiert auf einer eigenen Webseite über Konsequenzen und Pläne im Falle eines No-Deal-Brexit. Hierzu hat sie entsprechende Mitteilungen veröffentlicht und Rechtsakte erlassen. Auch die britische Regierung hat bereits im Jahr 2018 sogenannte Technical Notices veröffentlicht, in denen sie ihre Handlungsabsichten für den Fall eines No-Deal-Brexit niedergelegt hat.

Nachfolgend geben wir Ihnen noch einmal einen Kurzüberblick zu den wichtigsten Themengebieten, die vom Brexit betroffen sein werden.

I. Datenschutz

Für die Digitalwirtschaft werden Datentransfers zwischen der EU und VK künftig nicht mehr so einfach wie noch derzeit realisiert werden können. In Unternehmen gilt es zu klären, ob und welche Datenübermittlungen an Unternehmen mit Sitz im Vereinigten Königreich erfolgen.

Dabei ist es wichtig zu wissen, dass nicht nur Übermittlungen personenbezogener Daten betroffen sind. Ausreichend ist bereits die Möglichkeit des Zugriffs auf (Kunden-) Datenbanken durch Unternehmen mit Sitz außerhalb der EU. In diesem Kapitel stellen wir die Konsequenzen eines ungeregelten Brexits für die Datenwirtschaft dar und informieren Unternehmen darüber, welche Maßnahmen nun ergriffen werden müssen, um auch nach dem 01. November 2019 rechtssicher Daten nach VK übermitteln zu können.

Neben der Suche nach alternativen Rechtsgrundlagen für Datentransfers sollten Unternehmen sollten übrigens auch schauen ob es daneben angezeigt ist, Daten möglichst nur noch innerhalb der EU zu verarbeiten oder verarbeiten zu lassen, da innerhalb der EU keine zusätzlichen Maßnahmen für Datentransfers notwendig sind.

1. Was regelt das ausgehandelte Austrittsabkommen mit Blick auf Datentransfers?

Da während des Übergangszeitraums das gesamte Unionsrecht weiterhin so gelten sollte, als ob das Land ein Mitgliedstaat gewesen wäre, hätten Datentransfers zunächst weiterhin wie gewohnt – also ohne weitere Vorkehrungen - stattfinden können. Die Frage des Datenschutzes ist in den Art. 70ff des Vertrages angesprochen. Nach Ablauf der Übergangszeit zum 31. Dezember 2020 sollte Großbritannien die Vorschriften der EU-Datenschutzgrundverordnung (DSGVO) und anderer relevanter Vorschriften dann weiterhin für diejenigen personenbezogenen Daten anwenden, die in dieser Zeit übermittelt bzw. ausgetauscht werden und bis die EU durch eine formelle Angemessenheitsentscheidung festgestellt hat, dass das britische Datenschutzregime gleichwertige Garantien bietet.

Der Austrittsvertrag hätte dem Vereinigten Königreich auch an anderer Stelle genützt. Die Übergangszeit hätte Großbritannien auch Spielraum für internationale Verhandlungen zu Datentransfers gegeben. So gelten Datenübermittlungen z.B. in die USA auf Grundlage des EU-US Privacy Shields nur für die Mitgliedsstaaten der Europäischen Union. Es hätten diesbezüglich entsprechende Vereinbarungen verhandelt werden können. Nun müssen britische Unternehmen darauf hoffen, dass US-Unternehmen ihre Verpflichtungen aus dem EU-US-Privacy-Shield explizit auch auf Datenübermittlungen aus dem Vereinigten Königreich erstrecken und entsprechend kurzfristig aktualisieren.

Am 11. April 2019 haben sich die EU und VK auf eine Verlängerung der 2-jährigen Austrittsfrist bis zum 31. Oktober 2019 verständigt. Bis dahin soll den Briten noch ein letztes Mal die Möglichkeit gegeben werden, die Exit-Strategie politisch zu klären. Nachdem mit Boris Johnson nun ein erklärter Brexit-Befürworter das Amt des Premierministers übernommen hat scheint kaum erwartbar, dass es zu einer grundsätzlichen Umkehr oder gar zu einem zweiten Referendum kommen wird. Gestiegen ist hingegen die Wahrscheinlichkeit, dass das Vereinigte Königreich die EU nun tatsächlich ohne Austrittabkommen mit der EU verlässt.

2. Was passiert bei ungeregeltem Brexit?

Ohne ein Austrittsabkommen werden die Regelungen des europäischen Binnenmarktes und der Zollunion ab dem 01. November 2019, Punkt 0:00 Uhr automatisch keine Anwendung mehr finden. Dies gilt auch für sekundärrechtliche Bestimmungen wie die DSGVO. Großbritannien ist ab Ende Oktober also bis auf Weiteres auch "datenschutzrechtliches Drittland". Datentransfers an Niederlassungen oder Auftragsverarbeiter sind dann nicht mehr ohne die Einhaltung spezieller Anforderungen realisierbar. Dies kann erhebliche Auswirkungen auf die Datenwirtschaft zwischen EU und VK haben.

Die deutsche Datenschutzkonferenz hat am 8. März 2019 ein Informationspapier zu den datenschutzrechtlichen Konsequenzen des Brexit veröffentlicht. Auf zwei Seiten werden in Kürze die allgemeinen Folgen eines geregelten und eines ungeregelten Brexits dargestellt. Auch der Europäische Datenschutzausschuss hat sich in einer Mitteilung vom 12.02.2019 zu den Konsequenzen eines No-Deal-Szenarios beim Brexit geäußert. In dem Papier werden 5 Schritte zur Vorbereitung auf Datentransfers nach VK aufgezeigt und die nachfolgend beschriebenen Übermittlungsgrundlagen aufgezeigt. Mit Blick auf die von der DSGVO neu eingeführten Tools der Codes of Conduct oder Zertifizierung kündigt der Ausschuss entsprechende Leitlinien an.

3. Rechtsgrundlagen für Datentransfers

Für die Frage der datenschutzrechtlichen Zulässigkeit von Datentransfers ist zunächst zwischen Transfers innerhalb der EU und an andere Drittstaaten zu unterscheiden. Zunächst bedarf es für alle Datentransfers einer geeigneten Rechtsgrundlage nach DSGVO. Die Übermittlung personenbezogener Daten in ein Nicht-EU-Land zusätzlich nur dann zulässig, wenn dieses Drittland ein angemessenes Datenschutzniveau gewährleistet oder die anderen Anforderungen an eine internationale Übermittlung erfüllt sind. Daraus ergibt sich ein 2-Stufen-Test:

1. Stufe: Generelle Zulässigkeit des Datentransfers

Auf der 1. Stufe ist vor allem Art. 6 Abs. 1 DSGVO zu beachten. Das heißt, dass es eine Rechtsgrundlage für die Übermittlung geben muss. Die verantwortliche Stelle muss Betroffene zudem über die Absicht zur internationalen Datenübermittlung informieren, Art. 13 Abs. 1 f) DSGVO. Darüber hinaus muss sie Informationen über Maßnahmen zur Einhaltung der besonderen Anforderungen an eine internationale Datenübermittlung (sog. Tools) zur Verfügung stellen. Ein Betroffener muss Zugang zu entsprechenden Dokumenten haben. Ein Verantwortlicher muss entweder eine entsprechende Kopie bereitstellen oder eine Fundstelle angeben.

2. Stufe: Einhaltung der besonderen Anforderungen an eine internationale Datenübermittlung

Auf der 2. Stufe können verschiedene Tools eingesetzt werden, um eine internationale Datenübermittlung zu rechtfertigen. Dazu gehören u.a.:

- Feststellung eines angemessenen Schutzniveaus in einem Drittstaat bzw. für einen Teilbereich/Sektor; Ein Drittstaat bzw. ein Teilbereich/Sektor gilt aufgrund einer solchen Feststellung als „sicher" im datenschutzrechtlichen Sinne (Angemessenheitsbeschluss der EU-Kommission, Art. 45 DSGVO).
- Genehmigung durch Aufsichtsbehörde, wenn ein Verantwortlicher eine ausreichende Datenschutzgarantie gibt, z.B. durch die Verwendung von EU Standardvertragsklauseln (Geeignete Garantien, Art. 46 Abs. 2 DSGVO).
- Binding Corporate Rules (BCRs) (Konzern-Datenschutzvorschriften, Art. 47 DSGVO)
- Einwilligung des Betroffenen zur Übermittlung in einen konkreten Drittstaat (Art. 49 Abs. 1 a) DSGVO).
- Übermittlung ist für die Erfüllung oder Durchführung eines Vertrags mit dem Betroffenen erforderlich und in seinem Interesse (Art. 49 Abs. 1 b) und c) DSGVO).
- Übermittlung aufgrund von genehmigten Verhaltensregeln (Art. 40 DSGVO).
- Übermittlung aufgrund einer Zertifizierung. (Art. 42 DSGVO)

4. Angemessenheitsbeschluss der EU-Kommission

Wie beschrieben, ist eine Übermittlung personenbezogener Daten in Drittländer - wie es dann VK wäre - nur unter eingeschränkten Voraussetzungen möglich. Hier ist von Bedeutung, ob es sich bei dem betreffenden Land um ein nach Ansicht der EU-Kommission „sicheres" oder „unsicheres" Drittland handelt. Die Entscheidung darüber trifft die EU-Kommission (sog. Angemessenheitsentscheidung).

Für Länder, denen die Einhaltung eines angemessenen Datenschutzniveaus (Art. 45 DSGVO) attestiert wurde, gelten dann keine besonderen Regelungen mehr. Daher sind in solche Länder Datentransfers jederzeit ad-hoc und damit problemlos möglich. Folgenden Ländern wurde ein angemessenes Datenschutzniveau bescheinigt:

Andorra	Argentinien	Färöer
Guernsey	Ilse of Man	Israel
Japan	Jersey	Kanada
Neuseeland	Republik Östlich des Uruguay	Schweiz
USA (siehe dazu unten)		

Besonderheit USA:

Die EU-Kommission kann auch nur sektorbezogene Entscheidungen treffen. Ein prägnantes Beispiel ist das EU-US Privacy-Shield für Übermittlungen in die USA. Hier wurde die Angemessenheit nicht bezogen auf das gesamte Rechtssystem der USA, sondern hinsichtlich der Eckvereinbarungen zur Zertifizierung von US-Unternehmen und der Interventionsmöglichkeiten von EU-Bürgern festgestellt. Die Anerkennung der Angemessenheit – ob insgesamt oder sektorbezogen – beinhaltet die Feststellung, dass die nationalen Datenschutz- und sonstigen Vorschriften des Drittlandes ein der EU entsprechendes Schutzniveau für die Bürger aufweisen.

Für das Vereinigte Königreich müsste die EU-Kommission nun neue Verhandlungen für einen Angemessenheitsbeschluss aufnehmen. Mit Blick auf die in den letzten Jahren nicht nur in Großbritannien erlassenen Geheimdienstgesetze erscheint bereits fraglich, ob es überhaupt sie einfach zur Feststellung der Angemessenheit kommen könnte. Während die gesetzliche Fiktion des hohen EU-Datenschutzniveaus für Mitgliedsstaaten immer wirkt, wird in Drittländern genau hingeschaut. Hier könnte beispielsweise der 2016 – unter der damaligen Innenministerin Theresa May – eingebrachte Investigatory Powers Act plötzlich als möglicher Stolperstein diskutiert werden.

Auch zeitlich hätte ein Austrittsabkommen mehr Spielraum verschafft. Denn ein solches Angemessenheits-Verfahren dauert. So wurden die Wirtschaftsverhandlungen mit Japan, die auch den zuletzt getroffenen Angemessenheitsbeschluss vorbereiteten und – ähnlich wie im Falle Kanada – nicht einmal das gesamte Rechtssystem, sondern nur ausgewählte Rechtsgebiete betrafen, bereits im Jahre 2013 aufgenommen. Legt man diese Zeit für die Neuverhandlung der EU mit dem Vereinigten Königreich zugrunde, hätte auch eine Übergangszeit von zwei Jahren wohl nicht vollständig ausgereicht, um zwischenzeitlich eine belastbare Lösung für unkomplizierte Datenübermittlungen zu finden.

5. Verwendung von EU-Standardvertragsklauseln

Die wohl pragmatischste Lösung im Falle eines ungeregelten Brexit wird in der Aufnahme von EU-Standardvertragsklauseln in bereits bestehende Verträge mit Dienstleistern aus VK oder Niederlassungen liegen. Bei diesen handelt es sich um Klauseln, welche im Jahre 2010 von der EU-Kommission entwickelt wurden, um die vertragliche Sicherstellung eines angemesseneren Datenschutzniveaus zu unterstützen.

Nach dem Safe-Harbor-Urteil des EuGH hatte die EU-Kommission am 17.12.2016 eine Änderung der Klauselvorgaben beschlossen. Auch die britische Datenschutzbehörde (ICO) gibt hier entsprechende Tipps zur Einbindung in Verträge.

Es gibt verschiedene Version je nachdem, ob das Unternehmen Verantwortlicher (Controller – Art. 4 Nr.7 DSGVO) oder Auftragsverarbeiter (Processor – Art. 4 Nr. 8 DSGVO) ist.

Klauseln für die Übermittlung zwischen Verantwortlichen
Set 1 Set 2

Klauseln für die Übermittlung zwischen Verantwortlichen an Auftragsverarbeiter
Set 1

6. Einwilligung der Betroffenen

Personenbezogene Daten dürfen auch weiterhin mit Einwilligung der Betroffenen nach VK übermittelt werden. Besonderheit hier: Die Einwilligungserklärung muss sich ausdrücklich auf den Umstand beziehen, dass die Daten in ein Land übermittelt werden, welches kein angemessenes Datenschutzniveau bietet bzw. ein solche nicht durch einen entsprechenden Angemessenheitsbeschluss der EU-Kommission bestätigt wurde. Ohne diesen Zusatz fehlt es ansonsten an der erforderlichen Transparenz gemäß Art. 49 DSGVO. Die Zulässigkeit ist danach nur gegeben:

„wenn] die betroffene Person [ ]in die vorgeschlagene Datenübermittlung ausdrücklich eingewilligt [hat], nachdem sie über die für sie bestehenden möglichen Risiken derartiger Datenübermittlungen ohne Vorliegen eines Angemessenheitsbeschlusses und ohne geeignete Garantien unterrichtet wurde."

7. Datentransfer erforderlich zur Vertragserfüllung

Vielfach wird man die Übermittlung allerdings auch auf vertragliche Füße stellen können. Nach Art. 49 Abs. 1 b) ist eine Übermittlung auch in ein Drittland ausnahmsweise zulässig, soweit:

„die Übermittlung [ ] für die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen oder zur Durchführung von vorvertraglichen Maßnahmen auf Antrag der betroffenen Person erforderlich [ist]."

Dies gilt zum Beispiel für Reisevertragsdaten bei Buchungen über ausländische Diensteanbieter.

8. Verbindliche Unternehmensregeln/Binding Corporate Rules (BCR)

Eine andere Möglichkeit, internationale Datentransfers innerhalb einer Unternehmensgruppe zu realisieren, ist die Erstellung verbindlicher Unternehmensregeln (BCR). BCRs werden vornehmlich von größeren Konzernen eingesetzt. Die hierfür notwendigen Maßnahmen sind sehr zeit-, kosten- und personalintensiv. Insbesondere eine Ausarbeitung, Abstimmung mit einer Datenschutzbehörde und Implementierung von BCRs. In Art. 47 DSGVO ist hier – anders als bei den Hinweisen zu Zertifizierungen(Art 42 DSGVO) oder Code of Conducts (Art. 40 DSGVO) keine Erleichterungen bezogen auf besondere Bedürfnisse von kleinen und mittleren Unternehmen.

II. Beschäftige im Unternehmen

Mit dem Austritt aus der EU verbunden ist der Wegfall von EU-Bürgerrechten für britische Staatsangehörige. Jeder Unionsbürger – und damit derzeit auch noch britische Staatsbürger - hat beispielsweise das Recht, ohne Visum in die Mitgliedstaaten der EU, des EWR (EU plus Island, Liechtenstein und Norwegen) und der Schweiz einzureisen. Im Rahmen der Arbeitnehmer-, Niederlassungs- und Dienstleistungsfreiheit können längerfristige Arbeitstätigkeiten in der gesamten EU ausgeführt werden (Artikel 3 Absatz 2 des Vertrags über die Europäische Union (EUV); Artikel 4 Absatz 2 Buchstabe a, Artikel 20, Artikel 26 und die Artikel 45-48 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV).

Bei einem No-Deal-Brexit entfällt die Freizügigkeit in beide Richtungen. Am 05.September 2019 hat das deutsche Bundeskabinett bereits Übergangsreglungen beschlossen, die Staatsangehörigkeit regelt. So sollen britische Staatsangehörige, die vor Ablauf der Übergangszeit (Frist: 31.Oktober 2019) einen Antrag auf Einbürgerung in Deutschland gestellt haben, Ihre britische Staatsangehörigkeit nicht verlieren.

Andersherum soll dies auch für Deutsche gelten, welche einen Einbürgerungsantrag in VK gestellt haben.

Auch die britische Regierung möchte die Rechte von EU-Bürgern und ihren Familienangehörigen schützen. Um Ihre Rechte zu erhalten, müssen sich EU-Bürger dafür über das so genannte EU Settlement Scheme registrieren. An diesem Programm, das am 29. März 2019 in Betrieb genommen wurde, müssen alle EU-Bürger teilenehmen, wenn sie auch nach dem 31. Dezember 2020 im Vereinigten Königreich leben möchten.

Unternehmen sollten prüfen, inwieweit Beschäftigte hier informiert und gegebenenfalls unterstützt werden müssen.

III. Steuern und Zölle

Seit dem 01.01.2015 gelten für Anbieter digitaler Dienstleistungen in der EU geänderte Vorschriften über die Abfuhr von Umsatzsteuer. Neben den typischen Anbietern von Telekommunikations-, Rundfunk- sowie Fernsehleistungen betrifft dies alle anderen Anbieter der digitalen Wirtschaft, welche sich mit Online-Services an nicht steuerpflichtige Personen (private Endkunden bzw. Verbraucher i.S.d.§ 13 BGB) wenden (B2C).

Soweit Unternehmen der der digitalen Wirtschaft hierfür einen „Mini-One-Stop-Shop" (vgl. § 18h UstG) im Vereinigten Königreich registriert haben, muss dieser beispielsweise künftig in einem EU-Mitgliedsstaat eingerichtet werden.

Für weltweit tätige Konzerne sollte geprüft werden, ob die operative Steuerung von EU-Geschäften noch über VK abgewickelt werden kann bzw. sollte. Hier hinein sollte auch die Prüfung von Lieferbeziehungen und Importe aus EU-Mitgliedsstaaten fallen. Bei einem No-Deal-Brexit müssen die Unternehmen die gleichen Verfahren für den EU-Handel anwenden wie für den Handel mit dem Rest der Welt. Für britische Unternehmen wird es für eine weiterhin einfache Ein- und Ausfuhr von Waren oder Dienstleistungen wichtig, die Möglichkeiten der Sicherstellung der automatisierten Zollabfertigung im Rahmen des EORI-Systems (Economic Operators' Registration and Identification) zu prüfen und gegebenenfalls Schritte einzuleiten, um an entsprechenden Ersatzprogrammen teilnehmen zu können.

Auf britischer Seite wird die Einfuhr von Waren aus der EU für Unternehmen mit einer EORI-Nummer beginnend mit „GB" ein vereinfachtes Übergangsverfahren eingerichtet, für welches sich die Unternehmen registrieren lassen müssen (TSP - transitional simplified procedures).

Ansonsten gelten die Handelsbestimmungen der WTO. Hinzuweisen ist hierbei auf die unterschiedliche Behandlung von Waren und Dienstleistungen im Bereich der digitalen Wirtschaft. Waren wie verpackte Software werden aufgrund der Bestimmungen des auch von der WTO getragenen Information Technology Agreements von 1196 weiterhin zollfrei bleiben. Dabei kommt es nicht darauf an, ob die Software cloud-basiert oder physisch (CD/DVD) vertrieben wird. Softwarebasierte Dienstleistungen (wie z.B. SaaS) hingegen gelten nicht als Produkt und fallen unter das Allgemeine Abkommen über den Handel mit Dienstleistungen (GATS). Ähnlich wie die WTO-Regeln für Waren legt auch GATS fest, dass der internationale Verkauf von Dienstleistungen zwischen WTO-Mitgliedern – und damit auch zwischen VK und EU - zollfrei ist.

Weitere nützliche Informationen zu Änderungen der Aus- und Einfuhrbestimmungen finden Sie auf der Webseite der Generalzolldirektion.

IV. EU-Marken und Patente

Seit 1994 gilt in der EU ein einheitliches Schutzrechtesystem für Marken und Geschmacksmuster. Bei einem No-Deal-Brexit verlieren sämtliche Unionsschutzrechte für den VK-Raum ihre Gültigkeit. Unter anderem wegen dieser unter Umständen weitreichenden Auswirkungen hatten die Verhandlungsführer zahlreiche Vorkehrungen im Austrittsabkommen vorgesehen. Unternehmen müssen also auch hier prüfen, inwieweit ein ungeregelter Austritt nun Auswirkungen auf Marken- und andere Schutzrechtsportfolios hat.

In den Technical Notices der britischen Regierung betreffend das Markenrecht wird ausgeführt, dass bereits eingetragene Unionsmarken auch im Falle eines No-Deal-Brexits einen gleichwertigen Schutz nach nationalem Markenrecht erhalten. Ein separater Antrag des Rechteinhabers soll nicht notwendig sein.

Nur soweit Anmeldungen zu diesem Zeitpunkt noch nicht abgeschlossen sind müssen Anmelder innerhalb von neun Monaten nach dem Brexitdatum eine neue, gebührenpflichtige Markenanmeldung beim britischen Markenamt vornehmen, um entsprechenden Markenrechtsschutz für das Vereinigte Königreich zu erhalten.

Für den Bereich des Patentrechts ändert sich bei einem No-Deal-Brexit hingegen kaum etwas. Europäische Patente sind weiterhin über das Europäische Patentübereinkommen (EPÜ), welches auch vom Vereinigten Königreich unterzeichnet wurde, geschützt. Da das zugrundeliegende Übereinkommen ein völkerrechtlicher Vertrag ist und nicht EU-Recht entspringt, ergeben sich hier keine Änderungen. Ausnahmen gelten hingegen für Patente, die besonderen Regeln auf Grundlage EU-rechtlicher Vorschriften bestehen (Arzneimittel, Pflanzenschutzmittel). Das Europäische Amt für geistiges Eigentum (EUIPO) gibt auf einer eigenen Webseite entsprechende Hinweise.

Über uns

Bundesverband Digitale Wirtschaft (BVDW) e.V.

Der Bundesverband Digitale Wirtschaft (BVDW) e.V. ist die Interessenvertretung für Unternehmen, die digitale Geschäftsmodelle betreiben oder deren Wertschöpfung auf dem Einsatz digitaler Technologien beruht. Als Impulsgeber, Wegweiser und Beschleuniger digitaler Geschäftsmodelle vertritt der BVDW die Interessen der digitalen Wirtschaft gegenüber Politik und Gesellschaft und setzt sich für die Schaffung von Markttransparenz und innovationsfreundlichen Rahmenbedingungen ein. Sein Netzwerk von Experten liefert mit Zahlen, Daten und Fakten Orientierung zu einem zentralen Zukunftsfeld. Neben der DMEXCO und dem Deutschen Digital Award richtet der BVDW eine Vielzahl von Fachveranstaltungen aus. Mit Mitgliedern aus verschiedensten Branchen ist der BVDW die Stimme der Digitalen Wirtschaft.

Ressort Recht

Aufgabe unseres Ressorts Recht ist es, die einzelnen Gremien des Verbandes und die Mitgliedsunternehmen in Projekten im Zusammenhang mit ihrer Arbeit im BVDW rechtlich zu beraten und sie bei der Anwendung des geltenden Rechts zu unterstützen.

Das Ressort fungiert als Expertengremium für Mitglieder und die Branche. Die Mitglieder des Ressorts sind Rechtsanwälte, die unter anderem im Recht der neuen Medien tätig sind und auf langjährige Erfahrung sowie eine fundierte berufliche Praxis zurückgreifen.

Mehr zum Thema Recht im BVDW unter

www.bvdw.org

Impressum

Brexit – Checkliste für Digitalunternehmen

Erscheinungsort und -datum	Berlin, September 2019
Herausgeber	Bundesverband Digitale Wirtschaft (BVDW) e.V. Schumannstraße 2, 10117 Berlin, +49 30 2062186 - 0, info@bvdw.org, www.bvdw.org
Geschäftsführer	Marco Junk
Präsident	Matthias Wahl
Vizepräsidenten	Thomas Duhr, Anke Herbener, Achim Himmelreich, Alexander Kiock, Stephan Noller, Marco Zingler
Kontakt	RA Michael Neuber, Justiziar/ Bereichsleiter Politik und Recht, neuber@bvdw.org
Vereinsregisternummer	Vereinsregister Düsseldorf VR 8358