/ Brexit und DS-GVO

29.01.2019

Brexit | Datenschutz | Regulierung & Governmental Affairs

Die Datenschutzgrundverordnung (DS-GVO) gilt seit noch nicht einmal einem Jahr. Jüngsten Umfragen zur Folge haben längt nicht alle Unternehmen in der EU die Umsetzung der neuen Datenschutzanforderungen abgeschlossen. Und schon droht durch den bevorstehenden Brexit am 29.03.2019 neues Ungemach. Seit 25.05.2018 ist die DS-GVO unmittelbar auch im Vereinigten Königreich (UK) anwendbar. Mit dem drohenden Austritt aus der Europäischen Union (EU) wird UK aller Voraussicht nach nun zum im datenschutzrechtlichen Sinne unsicheren „Drittland" - mit gravierenden Auswirkungen auf das Datenschutzmanagement betroffener Unternehmen.

Wer ist betroffen?

Von den datenschutzrechtlichen Auswirkungen eines Brexit sind insbesondere folgende Unternehmen betroffen:

- Unternehmen mit Sitz in UK
- Unternehmen mit Sitz in der EU, die personenbezogene Daten in UK verarbeiten, nach UK transferieren und/oder aus UK erhalten

Ausgangslage und mögliche Szenarien

Aller Voraussicht nach möchte die UK-Regierung die DS-GVO nach einem Brexit im Wesentlichen in nationales UK-Recht übernehmen.

Für Unternehmen mit Sitz in UK dürften die Datenschutzanforderungen damit im Großen und Ganzen gleich bleiben. UK-Unternehmen müssten jedoch gegebenenfalls bedenken, einen Vertreter in der EU zu benennen. Auch der in der DS-GVO für die Zuständigkeit von Aufsichtsbehörden vorgesehene „One-Stop-Shop"-Mechanismus dürfte für UK entfallen.

Im Übrigen unterscheiden sich die erwarteten Folgen im Wesentlichen abhängig davon, welches der beiden folgenden Austrittsszenarien eintritt:

„Deal"

Das jüngst im Britischen Unterhaus abgelehnte Austrittsabkommen sah für den Datenschutz folgendes vor: Die DS-GVO sollte in UK in großen Teilen - vorerst für eine Übergangsphase bis zum 31.12.2020 - anwendbar bleiben. Dies sollte jedoch nur solange gelten, bis die EU-Kommission ein „angemessenes Schutzniveau" beschließen würde. Mit einer diesbezüglichen Prüfung wollte die EU nach dem Austritt beginnen und sich bemühen, diese innerhalb der Übergangsphase abzuschließen. Außerdem enthält das abgelehnte Abkommen eine ausdrückliche Verpflichtung der EU, personenbezogene Daten aus UK nicht anders zu behandeln als solche aus den verbleibenden EU-Mitgliedstaaten.

Ob und in mit welchem Inhalt nach der jüngsten Ablehnung ein Austrittsabkommen zustande kommt, steht derzeit weiterhin in den Sternen. Auch Details zu den datenschutzrechtlichen Aspekten eines derzeit diskutierten „Plan B" sind noch nicht bekannt.

„No Deal"

Sofern UK tatsächlich ohne Deal aus der EU austritt, wird UK aller Voraussicht nach zum unsicheren „Drittland" im Sinne der DS-GVO. Ein Angemessenheitsbeschluss der EU-Kommission, der grenzüberschreitende Datentransfers aus der EU nach UK ermöglichen könnte, ist derzeit jedenfalls nicht in Sicht. Deshalb wären andere Maßnahmen erforderlich, um Datenübermittlungen nach UK rechtmäßig durchzuführen, beispielsweise die Implementierung von EU-Standardvertragsklauseln oder Binding Corporate Rules (BCR).

Bei Verstoß gegen diese strengen Bedingungen für den Datentransfer in Drittländer drohen drastische Bußgelder.

Was ist nun zu tun?

Bestandsaufnahme

Zuerst sollten Unternehmen sorgfältig prüfen, inwiefern sie in datenschutzrechtlicher Sicht durch den Brexit überhaupt betroffen sind.

Dabei sind vor allem etwaige Geschäftsprozesse und Datenflüsse mit UK-Bezug zu betrachten, in die Niederlassungen des Unternehmens, Kunden, Geschäftspartner, Dienstleister oder andere Beteiligte in UK involviert sind.

Vorbereitung

Betroffene Unternehmen sollten im nächsten Schritt ermitteln, welche Maßnahmen – insbesondere für die „No Deal"-Variante – in Betracht kommen, um etablierte Geschäftsprozesse und Datenflüsse möglichst wenig zu beeinträchtigen.

Die erforderlichen Maßnahmen, beispielsweise EU-Standardvertragsklauseln oder BCR, lassen sich nicht ad hoc „über Nacht" umsetzen, sondern bedürfen einer sorgfältigen Vorbereitung, ggf. in Abstimmung mit den beteiligten Datenempfängern in UK.

Höchstvorsorglich sollten betroffene Unternehmen schon jetzt vorbereitende Umsetzungsmaßnahmen ergreifen, beispielsweise die „unterschriftsreife" Vorbereitung von EU-Standardvertragsklauseln, um im Falle eines „No Deals" bestmöglich gerüstet zu sein.

Beobachtung

Zudem sollten Unternehmen sollten die weitere Entwicklung zum Brexit und dessen datenschutzrechtlichen Auswirkungen aufmerksam verfolgen, um geplante Abläufe und Maßnahmen gegebenenfalls möglichst schnell und reibungslos anpassen zu können.

Umsetzung der DS-GVO

In jedem Fall gilt es aber, die Anforderungen der DS-GVO auch weiterhin wirksam umzusetzen und bereits getroffene Umsetzungsmaßnahmen im Sinne eines kontinuierlichen und effektiven Datenschutz-Managements zu prüfen, zu bewerten und ggfs. zu verbessern. Schließlich werden sich die die hohen datenschutzrechtlichen Anforderungen der DS-GVO – abgesehen von den Auswirkungen auf den Datentransfer nach UK – durch einen Brexit im Vergleich zur jetzigen Rechtslage nicht ändern.

Weiterführende Links:

- Mittelung der EU Kommission am 30. März 2019: Ein Aktionsplan für den Notfall
- Mitteilung der EU Kommission zum Austritt des Vereinigten Königreichs und der EU-Vorschriften im Bereich Datenschutz

Im Fokus: Brexit

Verfolgen Sie aktuellen Entwicklungen und News in unserem News-Channel zum Brexit

Haben Sie Fragen? Kontaktieren Sie gern: Daniel Rücker , Sebastian Dienst

Practice Groups: Datenschutz , Regulatory & Governmental Affairs

Contact Person

Dr. Daniel Rücker, LL.M.
Leiter Datenschutz
Mitglied der Practice Group Digital Business
Rechtsanwalt

T +49 89 28628457

Sebastian Dienst
Mitglied der Practice Group Datenschutz
Mitglied der Practice Group Digital Business
Rechtsanwalt

T +49 89 28628457