

# Datenschutz-Checkliste für den Brexit



Anfang des Jahres 2020 ist das Vereinigte Königreich offiziell aus der Europäischen Union ausgetreten. Am 1. Januar 2021 trat der Handels- und Kooperationsvertrag zwischen der EU und dem Vereinigten Königreich vorläufig in Kraft. Dieser enthält auch eine Übergangsregelung in Bezug auf den Schutz personenbezogener Daten, welche gültig ist, bis ein Angemessenheitsbeschluss durch die Kommission erfolgt. Gemäß dieser Regelung soll der Transfer personenbezogener Daten in das Vereinigte Königreich nicht als Datentransfer in ein Drittland im Sinne des Art. 44 EU-DSGVO gelten. Diese Übergangsfrist beträgt zunächst vier Monate und kann einmalig um zwei weitere Monate verlängert werden.

Die EU-DSGVO gilt für Mitgliedstaaten der EU unmittelbar, sodass sie einheitliche Anforderungen an die Erhebung und Verarbeitung personenbezogener Daten in den Mitgliedstaaten zwingend vorschreibt. Bisher sind die rechtlichen Anforderungen im Vereinigten Königreich daher auf einem ebenso hohen Niveau wie in allen anderen europäischen Mitgliedstaaten, sodass personenbezogene Daten einen gleichwertigen Schutz genießen. Dies kann sich jedoch mit dem Ende der Übergangsphase spätestens am 30. Juni 2021 ändern, da das Vereinigte Königreich dann an die rechtlichen Anforderungen der EU-DSGVO nicht mehr gebunden sein wird.

Diese Tatsache stellt viele europäische

Unternehmen im Rahmen der Zusammenarbeit mit Organisationen und Datenzentren aus dem Vereinigten Königreich vor neue Herausforderungen. Um Sie dabei zu unterstützen, haben wir eine Checkliste mit allen wichtigen Punkten erstellt.

Am 19. Februar 2021 hat die EU-Kommission in einer offiziellen Pressemitteilung verlauten lassen, dass ein Verfahren zur Annahme von zwei Angemessenheitsbeschlüssen eingeleitet wurde. Um das Verfahren erfolgreich abschließen zu können, bedarf es jedoch noch einer Stellungnahme des Europäischen Datenschutzausschusses (EDSA) und der Zustimmung der einzelnen EU-Mitgliedstaaten.

Deshalb empfehlen wir, dass sich Unternehmen darauf vorbereiten, dass das Vereinigte Königreich zu einem Drittland wird.

Was Sie unbedingt beachten sollten, wenn Sie **personenbezogene Daten aus dem Europäischen Wirtschaftsraum** an einen **Datenverantwortlichen oder Auftragsverarbeiter mit Sitz im Vereinigten Königreich** übermitteln:

- Überprüfen Sie, ob Sie schriftlich einen Vertreter innerhalb der Union gemäß Art. 27 EU-DSGVO benennen müssen.
- Ergänzen Sie gegebenenfalls die Datenschutzrichtlinien auf Ihrer Website um den festgelegten Vertreter.

- Erweitern Sie Ihre Datenschutzbestimmungen auf der Website, alle weiteren Datenschutzbestimmungen sowie Ihre internen Richtlinien um korrekte Verweise auf das britische Datenschutzrecht, den Data Protection Act 2018 und die EU-DSGVO, um Missverständnisse zu vermeiden.
- Vergewissern Sie sich, ob der zuständige Datenschutzbeauftragte oder die zuständige Aufsichtsbehörde über die Datenübermittlung entsprechend unterrichtet werden müssen.
- Überprüfen Sie, ob Datenübermittlungsverträge oder Weitervermittlungsverträge mit verbundenen Unternehmen oder Dritten hinsichtlich der Tatsache besprochen werden müssen, dass das Vereinigte Königreich nun nicht länger Mitgliedsstaat der EU, sondern stattdessen als Drittland im Sinne der EU-DSGVO zu betrachten ist und somit kein adäquater Schutz der personenbezogenen Daten gewährleistet werden kann.
- Gegebenenfalls müssen Sie Ihr Verzeichnis aller Verarbeitungstätigkeiten (VVT) ergänzen und gemäß Art. 30 I e) EU-DSGVO darin angeben, dass Sie personenbezogene Daten an ein Drittland übermitteln.

## Kontakt

KPMG AG  
Wirtschaftsprüfungsgesellschaft  
Erthalstraße 1  
55118 Mainz

**Prof. Dr. Dirk Loomans**  
Partner, Consulting –  
Cyber Security  
T +49 6131 37-0248  
dloomans@kpmg.com

[www.kpmg.de](http://www.kpmg.de)

[www.kpmg.de/socialmedia](http://www.kpmg.de/socialmedia)

