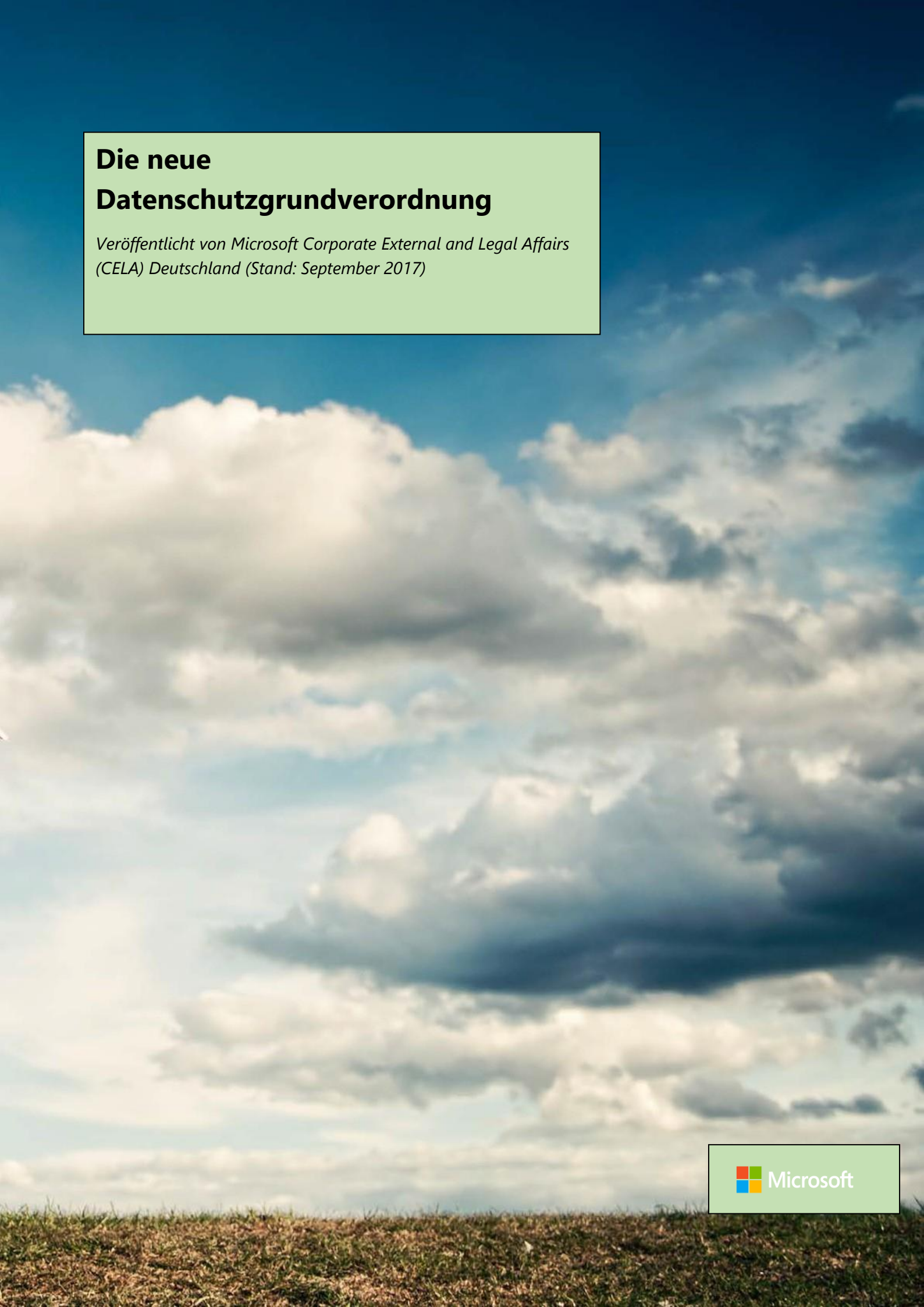

# Die neue Datenschutzgrundverordnung

*Veröffentlicht von Microsoft Corporate External and Legal Affairs (CELA) Deutschland (Stand: September 2017)*

Microsoft

Ab 25. Mai 2018 gilt die neue Datenschutzgrundverordnung ("DSGVO") in der Europäischen Union. Damit wird ein europaweit einheitlich geltender datenschutzrechtlicher Rahmen geschaffen und das bestehende Datenschutzniveau weiter erhöht. Die DSGVO ersetzt grundsätzlich die bestehenden Gesetze in den einzelnen Ländern, jedoch können für bestimmte Bereiche zusätzliche oder abweichende Regelungen in den einzelnen Ländern getroffen werden (sog. „Öffnungsklauseln"). So bleibt beispielsweise der hohe Standard im Arbeitnehmerdatenschutz nach deutschem Recht erhalten.

Für Cloud-Angebote führt das neue Recht zu keinen grundlegenden Umwälzungen, insbesondere was Auftragsdatenverarbeitungsverträge und internationale Datentransfers angeht. Jedoch gibt es einige Punkte, die die Rechte der Kunden und der betroffenen natürlichen Personen („Datensubjekten") weiter stärken, beispielsweise bei IT-Sicherheit und Datenpannen sowie der Unterstützung von Kunden in ihren Transparenzpflichten gegenüber den Datensubjekten. Eine weitere wesentliche Neuerung ist, dass die DSGVO in viel weiterem Umfang als bisher direkte Ansprüche der Datensubjekte gegenüber den Auftragsverarbeitern (also den Cloud-Anbietern) zulässt. Auch wird die Bedeutung des Datenschutzes durch eine Verstärkung der möglichen Strafen betont und somit die Cloud-Anbieter noch weiter in die Pflicht genommen.

## 1. Microsoft und die DSGVO

Microsoft begrüßt diese Änderungen im Interesse der Kunden und der betroffenen Personen. Microsoft bietet seinen Kunden bereits jetzt Vereinbarungen, die DSGVO-konforme Bedingungen enthalten
Im Folgenden möchten wir kurz die wesentlichen für Cloud-Angebote relevanten Punkte der DSGVO, insbesondere relevante Änderungen, darstellen und Sie über Microsofts Herangehensweise hinsichtlich dieser Punkte informieren.

## 2. Wesentliche neue Regelungen nach der DSVGO

Zunächst kurz zu den Kernprinzipien, die sich nicht verändert haben:

Der Cloud-Anbieter verarbeitet regelmäßig als Auftragsverarbeiter personenbezogene Daten auf Weisung des Kunden. Dies bleibt auch nach der DSGVO so. Dementsprechend können und müssen auch in Zukunft Speicherungen personenbezogener Daten im Rahmen von Cloud-Angeboten über Auftragsverarbeitungsverträge geregelt werden. Beim Thema Auftragsverarbeitungsvertrag folgt die DSGVO weitgehend dem bestehenden deutschen Recht. Dies führt dazu, dass der Anpassungsbedarf in Deutschland gering ist, jedoch durchaus zu einem erheblichen Anpassungsbedarf in einigen anderen EU-Ländern führt. Insbesondere folgt die DSGVO dem deutschen Vorbild, was die Darstellung der technischen und organisatorischen Maßnahmen in den Verträgen angeht. Im internationalen Kontext bleiben die bestehenden Mechanismen, insbesondere die Standardvertragsklauseln, in Kraft.

Erwähnenswert sind folgende neue bzw. geänderte Punkte:

**a. Unterstützung der Kunden bezüglich ihrer Rechte gegenüber Datensubjekten**

Die DSGVO gewährt Datensubjekten weitergehende Rechte als bisher, insbesondere was Informations-, Datenlöschungs- und Datenmigrationsansprüche angeht. Microsoft unterstützt seine Kunden hier gerne und hat sich in seinen Vereinbarungen zur DSGVO ausdrücklich dazu verpflichtet, derartige Unterstützungsleistungen zu erbringen, damit die Kunden in der Lage sind, Informationsanfragen, Löschungspflichten und Datenmigrationsansprüchen nachzukommen. Dazu gehört auch das Führen eines entsprechenden Verfahrensverzeichnisses durch Microsoft.

**b. Unterstützung der Kunden bei „Privacy by Design"**

Die DSGVO nimmt alle Unternehmen, die personenbezogene Daten verarbeiten und kontrollieren, in die Pflicht, bei ihren Produkten und Prozessen eine datenschutzfreundliche Nutzung zu ermöglichen. Dies hat Microsoft nicht nur selbstverständlich für sich selbst umgesetzt, sondern strukturiert seine Cloud-Angebote auch so, dass die Kunden ihren eigenen „Privacy by Design" Verpflichtungen nachkommen können. Dazu gehören Verschlüsselungs- und Pseudonymisierungsmöglichkeiten in den Fällen, in denen dies sinnvoll und nach dem Stand der Technik machbar ist, Wiederherstellungstechniken und regelmäßige Bewertung der eigenen Prozesse. Zu all diesen und weiteren Punkten verpflichtet sich Microsoft gegenüber Kunden in den entsprechenden Vereinbarungen ausdrücklich.

**c. Bestellung von Unterauftragnehmern**

Die DSGVO stellt in Artikel 28 (2) klar, dass Unterauftragnehmer nur mit Zustimmung des Kunden eingeschaltet werden können, wobei aus Praktikabilitätsgründen eine solche Zustimmung auch pauschal vorab erteilt werden kann, wenn der Kunde über einen neuen Unterauftragsnehmer informiert wird und ein Widerspruchsrecht bekommt. Microsoft hat dies bereits in seinen bestehenden Bedingungen umgesetzt und bietet den Kunden an, ihr Widerspruchsrecht durch eine Kündigung auszuüben.

**d. Haftung für Unterauftragsnehmer**

Soweit Microsoft – wie oben beschrieben – Unterauftragsnehmer zulässigerweise verwendet, verpflichtet sich Microsoft ausdrücklich in seinem DSGVO Bestimmungen für diese einzustehen und übernimmt die Haftung für diese. Dies schließt auch die Verpflichtung ein, dass ausreichende technische und organisatorische Maßnahmen bei den Unterauftragnehmern getroffen werden. Der Kunde muss sich hierum also nicht kümmern. Selbstverständlich bleiben ihm aber seine bestehenden Rechte erhalten.

**e. IT-Sicherheit**

Die Verhinderung von IT-Sicherheitslücken und Datenpannen bzw. die Vermeidung von Schäden, wenn IT-Sicherheitslücken und Datenpannen auftauchen, ist ein Kernbestandteil der DSGVO. Hierzu gehören nicht nur klassische Hackingangriffe oder

Verluste von Datenträgern, sondern alle Datenschutzverletzungen, die dazu führen, dass Daten von Unberechtigten genutzt werden können. Eine Datenpanne kann sowohl auf Seiten des Cloud-Anbieters als auch auf Seiten des Kunden vorkommen. Für Microsoft ist es selbstverständlich, sich gegenüber den Kunden in den DSGVO-Bestimmungen dazu zu verpflichten, Maßnahmen zu ergreifen, um die IT-Sicherheit zu gewährleisten (und wenn doch etwas passiert, den Kunden unverzüglich über mögliche Risiken für ihn zu informieren). Microsoft verpflichtet sich auch, den Kunden zu unterstützen, wenn in seinem Umfeld Sicherheitsvorkehrungen nicht eingehalten wurden (beispielsweise wenn der Kunde Passwörter zu Cloud-Anwendungen von Microsoft verloren hat). Insbesondere stellt Microsoft den Kunden alle notwendigen Informationen im Zusammenhang von Datenpannen zur Verfügung.

### f. Sensitive Daten (insbesondere Gesundheitsdaten)

Eine wesentliche Änderung der DSGVO ist, dass es in Zukunft auch nach deutschem Recht ohne jeden Zweifel möglich sein wird, besondere Arten personenbezogener Daten (sogenannte „sensible Daten"), inklusive Gesundheitsdaten, im internationalen Umfeld zu speichern. Die diesbezügliche deutsche Sonderregel (deren Vereinbarkeit mit EU-Recht ohnehin fraglich war) fällt weg. Das bedeutet, dass internationale Cloud-Angebote auch benutzt werden können, soweit Gesundheitsdaten oder andere sensible Daten betroffen sind. Unabhängig davon bietet Microsoft natürlich nach wie vor wahlweise Kunden an, die das möchten, Daten nur in der EU zu speichern oder die Microsoft Cloud Deutschland zu wählen. Die Microsoft Cloud Deutschland sieht ein Treuhändermodell mit der T-Systems International GmbH vor. Nach dem Treuhändermodell hat Microsoft technisch selbst keinen Zugriff auf die Daten, sondern nur die T-Systems International GmbH.

## 3. Zusammenfassung

Auch beim Thema DSGVO möchte Microsoft seiner Vorreiterrolle unter den Cloud-Anbietern im Bereich Datenschutz gerecht werden und freut sich daher, seinen Kunden bereits jetzt mit den DSGVO-Vereinbarungen die notwendigen Mittel an die Hand geben zu können. Bei Fragen zur DSGVO stehen Ihnen die weiteren nützlichen Informationen zur Verfügung:

Das Microsoft Trustcenter hat Informationen zur DSGVO hier zusammengefasst. Hier finden Sie ein 30 Minuten Webinar zur DSGVO.