



# DSGVO-Evaluierung – Cloud-Dienste rechtssicher gestalten

## Positionspapier

### Auf einen Blick

Aktuell herrscht erhebliche rechtliche Unsicherheit beim Einsatz von Cloud-Dienstleistern. Der Beschluss der Datenschutzkonferenz (DSK) zu Microsoft 365 vom 25.11.2022 verdeutlicht den Handlungsbedarf. Die laufende Evaluierung der DSGVO muss genutzt werden, um aktuell besonders relevante Rechtssicherheiten und praxisfremde, branchenspezifische Auswirkungen zu beheben. Im Mittelpunkt müssen stehen:

- Implementierung einer Herstellerhaftung für große Cloud-Dienstleister statt einer Weisungspflicht für Kunden zu Sicherheitsmaßnahmen
- EU-weit einheitliche Rechtsvorgaben, kein deutsches Goldplating
- Datenschutzerklärungen mit Augenmaß und Praktikabilität
- Sichere Rechtsgrundlagen für vom Vertrag ausgelöste Datenverarbeitung eines Cloud-Dienstleisters

### Praxistaugliche Vorgaben für Cloud-Dienstleister – Evaluierung der DSGVO –

#### Implementierung einer Herstellerhaftung für große Cloud-Dienstleister, statt einer Weisungspflicht für Kunden zu Sicherheitsmaßnahmen

Die Verwendung von Cloud-Lösungen inklusive Software-Updates großer Cloud-Dienstleister sind praxisfern geregelt. Undifferenziert schreibt die DSGVO für alle Arten von Auftragsverarbeitungen vor, dass der Kunde als Auftraggeber Weisungen zur technischen Ausgestaltung und zu Anpassungen an den jeweiligen Stand der Technik geben muss. Dies gilt auch für große Cloud-Anbieter und deren komplexe Dienste und Systeme. Insbesondere für kleine Unternehmen ist dies nicht händelbar. Denn sie verfügen weder über ausreichendes Wissen noch über eine entsprechende Marktmacht gegenüber großen Anbietern. Bei rechtlich korrektem Handeln müssten sie beispielsweise im Falle eines Einsatzes von cloud-basierten Multi-Tenant-Lösungen notwendige technische und organisatorische Vorgaben für jedes einzelne Update machen und diese gegenüber industriellen Cloud-Dienstleistern vertraglich verankern. Die Implementierung in Form einer Herstellerhaftung, welche die EU bereits beim Cyber Resilience Act sowie bei den Produkthaftungs- und Produktsicherheits-Richtlinien vorsieht, wäre auch für industrielle Cloud-Dienstleister eine Lösung und sollte für diese in der DSGVO verankert werden.

#### EU-weit einheitliche Rechtsvorgaben, kein deutsches Goldplating

EU-weit tätige Anbieter und Nutzer von Cloud-Lösungen haben aktuell keine einheitliche Vertragsgestaltungs- und Umsetzungsmöglichkeit, weil Rechtsfragen in den Mitgliedsstaaten unterschiedlich ausgelegt werden. Im Rahmen der Evaluierung muss auf EU-weit einheitliche und praktikable Rechtsvorgaben in der DSGVO, zumindest in deren Erwägungsgründen, hingearbeitet werden.

Die Einführung von Verwaltungsvorschriften zur effizienteren Durchführung von Abstimmungen (sog. Kohärenzverfahren) unter den Datenschutzaufsichtsbehörden in Europa sind hier ein wichtiger Schritt. Dies könnte die Bürokratiebelastung sowohl für Anbieter als auch Nachfrager erheblich reduzieren, welche aus unterschiedlichen Auslegungen und Umsetzungen durch nationale Datenschutzaufsichtsbehörden resultieren. EU-weit müssen Rechtsfragen und Auslegungen abgestimmt und praxisnah erfolgen.

#### Datenschutzerklärungen mit Augenmaß und Praktikabilität

Die Anforderungen an die Datenschutzerklärungen sind zu detailliert und erfordern permanente Anpassungen bei Produktentwicklungen (bspw. Updates). Für eine rechtssichere Dokumentation müssen Kunden aktuell die technischen Funktionsweisen kennen und sie verstehen. Dies


überfordert insbesondere kleine Unternehmen. Im Rahmen der Evaluierung muss der Umfang von Datenschutzdokumentationen auf ein vernünftiges Maß reduziert werden. Mit einer Möglichkeit der Verweisung auf Online-Dokumentationen des Cloud-Dienstleisters bzw. umgekehrt auf die Verfahrensdokumentation der Kunden zur Beschreibung von Geschäftsgegenstand, Arten und Kategorien von Daten könnten die Dokumentationsanforderungen bereits erheblich vereinfacht werden.

#### Sichere Rechtsgrundlagen für vom Vertrag ausgelöste Datenverarbeitung eines Cloud-Dienstleisters

Aktuell herrscht Unsicherheit bei vom Vertrag ausgelösten Datenverarbeitungen eines Cloud-Dienstleisters. Beispiele sind Abrechnungen und Provisionsberechnungen, Verbesserung von Kernfunktionen, Bekämpfung von Cyberangriffen / Betrug oder Financial Reporting. Um diese Dienstleistungen rechtsicher vornehmen zu können, müssen die Datenschutzaufsichtsbehörden sich auf EU-weit einheitliche Rechtsgrundlagen verständigen. Praxiskonforme Sichtweisen zu dieser Rechtsfrage vertreten insbesondere die Niederlande, welche derartige Datenverarbeitungen als rechtskonform ansehen, wenn diese in einem Standarddatenschutzvertrag dokumentiert sind. In Deutschland fordern hingegen die Datenschutzaufsichtsbehörden für jeden Verarbeitungsschritt eine gesonderte Rechtsgrundlage.

#### Ansprechpartnerin

Rita Bottler

 089 5116-0

 @bottler@muenchen.ihk.de



[ihk-muenchen.de](https://www.ihk-muenchen.de)



[/ihk.muenchen.oberbayern](https://www.facebook.com/ihk.muenchen.oberbayern)



[@IHK\\_MUC](https://twitter.com/IHK_MUC)



[ihk-muenchen.de/newsletter](https://www.ihk-muenchen.de/newsletter)



[/company/ihk-muenchen](https://www.linkedin.com/company/ihk-muenchen)



[/company/ihk-muenchen](https://www.linkedin.com/company/ihk-muenchen)