

Cloud Dienstleister

Die Auswahl ist groß – Aber welche entsprechen der DSGVO?

Einleitung

In der heutigen digitalen Ära, in der Daten das neue Gold darstellen, ist die Wahl eines Cloud-Dienstleisters von entscheidender Bedeutung für den Schutz und die Verwaltung wertvoller Unternehmensressourcen. Die Dominanz US-amerikanischer Anbieter auf dem globalen Cloud-Markt wirft jedoch zunehmend Fragen hinsichtlich des Datenschutzes, der Datensouveränität und Abhängigkeit auf. Diese Bedenken sind insbesondere in Europa vor dem Hintergrund der strengen Datenschutzgesetze, wie der Datenschutz-Grundverordnung (DSGVO), von großer Bedeutung.

Vor diesem Hintergrund zielt dieses Whitepaper darauf ab, die komplexen Herausforderungen zu beleuchten, die sich aus der Nutzung US-amerikanischer Cloud-Dienstleister ergeben, und gleichzeitig den Blick auf alternative Lösungen innerhalb Europas zu lenken.

Um Entscheidungsträgern in Unternehmen eine fundierte Grundlage für die Auswahl eines Cloud-Dienstleisters zu bieten, findet sich in diesem Whitepaper zudem eine sorgfältig zusammengestellte Tabelle mit verschiedenen europäischen Cloud-Anbietern.

Problemstellung

Im Kontext des Cloud Act haben US-Behörden die Befugnis, von in den USA ansässigen Unternehmen die Herausgabe personenbezogener Daten zu verlangen. Diese Anforderung kann ohne die Notwendigkeit eines Gerichtsbeschlusses oder eines Rechtshilfeabkommens erfolgen. Diese Regelung wirft bedeutsame Fragen hinsichtlich des Datenschutzniveaus für EU-Bürger auf, insbesondere wenn es um die Nutzung von Cloud-Diensten amerikanischer Anbieter geht. Im Vergleich zu Dienstleistern, die ihren Sitz und ihre Datenverarbeitungsinfrastruktur innerhalb der Europäischen Union haben, erscheint das Schutzniveau bei US-Anbietern als weniger robust.

Die Europäische Union und die Vereinigten Staaten haben in der Vergangenheit versucht, durch Abkommen wie dem »Privacy Shield« ein angemessenes Datenschutzniveau zu gewährleisten. Jedoch wurde dieses Abkommen vom Europäischen Gerichtshof (EuGH) für ungültig erklärt. Als Reaktion darauf erließ die EU-Kommission einen neuen Angemessenheitsbeschluss, das »EU-US Data Privacy Framework«, welches jedoch ebenfalls auf Kritik stößt. Insbesondere die Datenschutzorganisation noyb, unter der Leitung von Max Schrems, die bereits maßgeblich zur Anfechtung der Vorgängerabkommen beigetragen hat, sieht in dem neuen Framework lediglich eine Neuauflage des gescheiterten Privacy Shield und hat angekündigt, auch gegen dieses Abkommen vor dem EuGH vorzugehen.

Sollte das EU-US Data Privacy Framework ebenfalls vom EuGH für ungültig erklärt werden und keine anderen Garantien gemäß Artikel 46 der Datenschutz-Grundverordnung (DSGVO) bestehen, wäre eine Datenübertragung in die USA nur noch unter den strengen Voraussetzungen des Artikels 49 DSGVO möglich. Dies unterstreicht

die Notwendigkeit für Unternehmen, die Nutzung von Cloud-Diensten sorgfältig zu prüfen und dabei mögliche rechtliche und datenschutzrechtliche Risiken zu berücksichtigen.

Vor diesem Hintergrund empfiehlt es sich für Unternehmen, die Implementierung von Cloud-Diensten zu evaluieren, insbesondere hinsichtlich der Auswahl des Anbieters. Es kann ratsam sein, Anbieter zu bevorzugen, die ihren Sitz sowie ihre Datenverarbeitungsinfrastruktur innerhalb Deutschlands oder zumindest der Europäischen Union haben. Solche Anbieter unterliegen nicht der US-Gerichtsbarkeit und bieten daher eine höhere Wahrscheinlichkeit, dass die Daten ihrer Kunden vor unberechtigtem Zugriff geschützt sind. Durch die Wahl eines solchen Anbieters können Unternehmen nicht nur die Einhaltung der DSGVO sicherstellen, sondern auch das Vertrauen ihrer Kunden in den Schutz ihrer persönlichen Daten stärken.

Die beigefügte Tabelle bietet eine Auswahl an Cloud-Diensten, die für die Evaluierung in Betracht kommen. Diese Empfehlungen werden von Trusted Cloud mit Unterstützung des Bundesministeriums für Wirtschaft und Klimaschutz bereitgestellt.

Anbieter	Plattform	Anmerkung
1 & 1 Internet AG Hauptsitz: Montabaur, Rheinland-Pfalz	IONOS Cloud (IaaS)	<ul style="list-style-type: none"> » Serverstandorte: Berlin, Karlsruhe (Nutzung der Strato AG Rechenzentren) » C5-zertifizierte Services: Compute Engine, Cloud Cubes, Object Storage » Zertifizierungen: DSNW ISO/IEC 27001:2013 » Rechenzentrum ebenfalls zertifiziert
Mitteldeutsche IT-GmbH Hauptsitz: Leipzig	Cloud Dienstleister & Cloud Service (IaaS, PaaS, SaaS)	<ul style="list-style-type: none"> » Serverstandort: Markkleeberg, Sachsen » Zertifizierungen: Subunternehmen/Rechenzentren ISO27001, ISO 9001, EN50600 » Kein Zertifikat für Anbieter/Service » Fokus: Mittelständische Unternehmen in Deutschland
YourSecureCloud GmbH Hauptsitz: Neumarkt, Oberpfalz, Bayern	Your Secure Cloud (SaaS)	<ul style="list-style-type: none"> » Serverstandort: Nürnberg » Zertifizierungen: Subunternehmen/Rechenzentren ISO 27001, ISO 9001, ISO/IEC 27001
Strato AG Hauptsitz: Berlin	HiDrive Strato (SaaS)	<ul style="list-style-type: none"> » Serverstandorte: Berlin, Karlsruhe » Zertifizierungen: Anbieter/Service und Rechenzentren ISO 27001
Deutsche Telekom AG Hauptsitz: Bonn	OpenTelekom Cloud based on OpenStack (IaaS)	<ul style="list-style-type: none"> » Serverstandorte: Deutschland, Niederlande, Schweiz » Zertifizierungen: Anbieter/Service und Rechenzentrum BSI C5 -ISAE 3000, ISO 9001:2015, ISO/IEC 27001:2017 » Weitere Zertifikate verfügbar
e.pilot GmbH Hauptsitz: Köln	Epilot Cloud (SaaS)	<ul style="list-style-type: none"> » Serverstandort: Hessen » Zertifizierungen: Subunternehmen/Rechenzentren C5, CSA Star Level 2, ISO/IEC 27001:2013, ISO/IEC 27018:2015, ISO/IEC 9001:2015 » Anbieter/Service Zertifizierung: VdS 10010



Legende	
IaaS	INFRASTRUCTURE AS A SERVICE Sie verwalten die Infrastruktur als Nutzer teilweise selbstständig (z. B. Betriebssystem, Middleware, Daten und Anwendungen), wobei der Dienstanbieter die Infrastruktur im Bereich Computing, Speicher, Netzwerke und Virtualisierung betreibt.
SaaS	SOFTWARE AS A SERVICE Der Dienstanbieter stellt hier Software zur Verfügung, die auf Ihrer Infrastruktur genutzt werden kann. Die Wartung/ Funktionalität der Software spielt für Sie keine Rolle, das übernimmt der Dienstanbieter.
PaaS	PLATFORM AS A SERVICE Der Dienstanbieter stellt Ihnen Hardware- und Software-Tools über das Internet bereit. I.d.R. werden diese Tools für die Softwareentwicklung benötigt. Der Host läuft über die Hardware und Software des Dienstanbieters auf seiner Infrastruktur.
BSI C5	Der Kriterienkatalog C5 (Cloud Computing Compliance Criteria Catalogue) des Bundesamts für Sicherheit in der Informationstechnik spezifiziert Mindestanforderungen an sicheres Cloud Computing und richtet sich in erster Linie an professionelle Cloud-Anbieter, deren Prüfer und Kunden.
ISO / IEC 27001	Eine Internationale Norm, die Anforderungen für Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines dokumentierten Informationssicherheits-Managementsystems spezifiziert.
ISO 27001	Es handelt sich um eine Zertifizierung auf Basis von IT-Grundschutz des BSI. Testate dürfen nur von einem beim BSI zertifizierten Auditor vergeben werden.
ISO 9001	Es handelt sich um eine Norm für Qualitätsmanagementsysteme. Die DIN legt Mindestanforderungen fest, die umzusetzen sind, um die Kundenanforderungen sowie weitere Anforderungen an Ihre Produkt- bzw. Dienstleistungsqualität zu erfüllen.
ISO / IEC 27018	Ein seit August 2014 bestehender internationaler Standard für den Datenschutz in der Cloud.
Vds Zertifikat	Richtlinien zur Umsetzung der DSGVO. Sie enthalten Vorgaben und Hilfestellungen für die Implementierung eines Datenschutzmanagementsystems sowie konkrete Maßnahmen für die organisatorische und technische Umsetzung der DSGVO. Bei Umsetzung der Richtlinie kann ein VdS-Zertifikat erworben werden.

Sollten Sie nähere Informationen zu den einzelnen Zertifikaten, zu den Kosten, zum Support oder zu der Größe der Unternehmen benötigen, informieren Sie sich auf der Webseite der Trusted Cloud.

Trusted Cloud



Entscheiden Sie sich für uns, ist es plötzlich ganz einfach.

WIR KÜMMERN UNS UM DATENSCHUTZ UND
INFORMATIONSSICHERHEIT IN IHREM UNTERNEHMEN:

SO KONFORM WIE NÖTIG - SO PROZESSORIENTIERT WIE MÖGLICH!



glende-consulting.de



» BESUCHEN SIE UNS

GLENDE.CONSULTING GmbH & Co. KG
Friedrich-Barnewitz-Str. 7
18119 Rostock-Warnemünde

» SPRECHEN SIE MIT UNS

Tel.: 0381.7787 468-0

» SCHREIBEN SIE UNS

info@glende-consulting.de

HAFTUNGSAUSSCHLUSS Dieses Whitepaper behandelt verschiedene datenschutzrechtliche Fragestellungen. Es dient ausschließlich Informationszwecken und stellt keine Rechtsberatung dar. Trotz großer Sorgfalt bei der Erstellung können wir keine Haftung für die Eignung der Dokumente für Ihren Anwendungsbereich übernehmen. Beachten Sie, dass aufgrund neuer Rechtsprechungen und Gesetzesänderungen Aktualisierungen notwendig sein können. Dieses Dokument kann Links zu externen Websites enthalten, die nicht unter unserer Kontrolle stehen. Wir übernehmen keine Verantwortung für den Inhalt, Datenschutzpraktiken oder andere Aspekte dieser externen Websites. Die Bereitstellung von Links zu diesen Seiten bedeutet nicht, dass wir deren Inhalte befürworten. Nutzer folgen diesen Links auf eigenes Risiko.

Weitere Informationen entnehmen Sie bitte unserem **IMPRESSUM** unter <https://www.glende-consulting.de/impressum.html>

HINWEIS ZUR SPRACHREGELUNG Aus Gründen der besseren Lesbarkeit verwenden wir in diesem Dokument das generische Maskulin.