Mittelstand | 4.0
Agentur Cloud

LEITFADEN

Cloud Computing aus Sicht der Datenschutz-Grundverordnung (DS-GVO)

Leitfaden DS-GVO-konforme Auftragsverarbeitung in der Cloud

Mittelstand-Digital

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

Überblick

Zielsetzung

Der vorliegende Leitfaden behandelt das Thema Cloud Computing aus der Sicht der DS-GVO. Seit dem 25. Mai 2018 gilt die neue Verordnung zur Verarbeitung personenbezogener Daten. Was genau das für Cloud-Nutzer und Anbieter bedeutet und auf welche Aspekte man bei einem Cloud-Dienst achten muss, damit dieser DS-GVO konform ist, wird nachfolgend erläutert.

Was ist Cloud Computing?

Um den Zusammenhang zwischen Cloud Computing und der DS-GVO richtig einordnen zu können, ist unter anderem entscheidend, was wir in dieser Broschüre unter Cloud Computing verstehen. Es existieren verschiedene Beschreibungen und Definitionen, was Cloud Computing ist (z.B. NIST).

Wir zielen hier nicht auf eine allgemeingültige Definition ab, sondern nennen nachfolgend die zentralen und für die DS-GVO wichtige Aspekte bzw. Eigenschaften von Cloud Computing.

Vereinfacht gesprochen ist Cloud Computing die Bereitstellung von IT-Leistung über das Internet. IT-Leistung kann dabei in “Rohform” etwa als Rechenleistung, Speicherplatz, Netzwerkleistung, etc. angeboten werden, oder auch “veredelt” etwa in Form von Datenverarbeitung (Verwaltung, Auswertung von Daten) oder kompletten Anwendungen. Der Anbieter hält die von ihm bereit gestellte cloud-basierte IT-Leistung i.d.R. für unterschiedliche (zeitgleiche) Abnehmer (Kunden) bereit und stellt sie bedarfsorientiert zur Verfügung. Schnelle Bereitstellung, flexible Verfügbarkeit oder verbrauchsabhängige Bezahlmodelle sind einige der Argumente, die positiv mit Cloud Computing verbunden sind.

Was ist die Mittelstand 4.0: Agentur Cloud

Die Mittelstand 4.0-Agentur Cloud ist Teil der Förderinitiative Mittelstand Digital.Mittelstand-Digital informiert kleine und mittlere Unternehmen über die Chancen und Herausforderungen der Digitalisierung. In der Initiative hat die Mittelstand 4.0 Agentur Cloud den Auftrag, das Thema Cloud Computing für unterschiedliche Akteure der Wirtschaft besser verständlich zu machen, um die Besonderheiten und Chancen von Cloud Computing für das eigene Unternehmen bewerten zu können und schließlich Entscheidungen treffen zu können, ob und in welcher Form die Nutzung von Cloud-Diensten für das eigene Unternehmen vorteilhaft ist.

Über die Autoren

Erden Yücel ist Jurist, Finanzbetriebswirt und GDD zertifizierter Datenschutzbeauftragter. Nach seiner Zeit als Ansprechpartner in einem international tätigten Unternehmen für Fragen rund um das IT-Recht, ist er heute geschäftsführender Gesellschafter der FYNE Consulting GmbH und betreut national & international tätige Unternehmen als externer Datenschutzbeauftragter.MichaelSchnaider ist Informatiker, Geschäftsführer der IT-DienstleistungsGmbH Emslandund Leiter des Mittelstand4.0-Kompetenzzentrums Lingen. In seiner Funktion unterstützt er mittelständische Unternehmen beistrategischen und operativen Entscheidungen zu IT-Nutzung und digitaler Fortentwicklung.

Einleitung

Seit einigen Jahren nimmt das Geschäft mit der „Wolke“ stetig zu. Immer mehr Unternehmen, Vereine und Organisationen greifen auf Cloud-Dienste zurück, wie aus einschlägigen Studien zur Cloud-Nutzung abzulesen ist [z.B. Cloud Monitor2018].

Auch bisher galten Verpflichtungen, die die Nutzung von Cloud-Diensten reglementiert haben, insbesondere aus der Perspektive des Schutzes von personenbezogenen Daten. Allerdings werden Cloud-Anbieter mit der Datenschutz-Grundverordnung (DS-GVO) weitaus stärker in die Pflicht genommen als bisher. Daraus ergeben sich eine Reihe entscheidender Fragestellungen:

- Was ist der Cloud-Anbieter aus der Sicht der DS-GVO?
- Wofür wird ein Auftragsverarbeitungs-Vertrag (AV-Vertrag) benötigt und was muss er beinhalten?
- Wer trägt die Verantwortung bei der Verarbeitung von personenbezogenen Daten?
- Darf man einen Cloud-Anbieter aus dem EU-Ausland beauftragen?
- Wie wähle ich den richtigen Cloud-Anbieter aus der Sicht der DS-GVO?
- Wie kann der Cloud-Anbieter das Bestehen von technisch organisatorischen Maßnahmen nachweisen?

Bei der Anwendung von Cloud-Diensten und der Bereitstellung von IT-Dienstleistungen werden regelmäßig mehrere Beteiligte tätig. Hier ist es von Bedeutung, wie deren Beziehungen datenschutzrechtlich zu bewerten sind und wie die Beteiligten Ihren Verpflichtungen nachkommen. Was ist der Cloud-Anbieter aus der Sicht der DS-GVO?

Frage 1:

Was ist der Cloud-Anbieter aus der Sicht der DS-GVO?

Der Verantwortliche

Der **Verantwortliche** kann eine Person, ein Unternehmen, eine Organisation oder eine Behörde sein, welche über die Mittel und Zwecke der Verarbeitung personenbezogener Daten entscheidet. Der Verantwortliche ist somit die Stelle, welche personenbezogene Daten verarbeitet. Während eines Bewerbungsprozesses ist es z.B. die Personalabteilung, welche die Bewerbung prüft.

In der Regel ist der Verantwortliche also das Unternehmen, das einen Cloud-Dienst oder eine in der Cloud bereitgestellte IT-Dienstleistung nutzt. Dabei ist es unerheblich, ob für die Nutzung ein Entgelt geleistet wird.

Die DS-GVO definiert den Begriff der **personenbezogenen Daten** in Art. 4 Nr. 1 wie folgt:

„Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (betroffene Person) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser Person sind, identifiziert werden kann…“

Bei personenbezogenen Daten handelt es sich also um Informationen, die sich auf einem Menschen beziehen, wie z.B. der Name einer Person, das Fahrzeugnummernschild eines Fahrzeugs, welches wiederum auf den Fahrer schließt oder die Steuer-Identifikationsnummer des Steuerzahlers.

Der Auftragsdatenverarbeiter

Ein Auftragsverarbeiter ist nach Art. 4 Nr. 8 DS-GVO eine Stelle, die personenbezogene Daten im Auftrag seines Auftraggebers (also des Verantwortlichen) verarbeitet. Dabei spielt es keine Rolle, ob es sich bei dem Auftragsverarbeiter um eine Person handelt oder es ein Unternehmen, Verein oder Behörde ist. Jedoch ist für die Einstufung eines Dienstleisters als Auftragsverarbeiter ein weiterer Faktor von entscheidender Bedeutung und zwar die Weisungsgebundenheit. Der Auftragsverarbeiter muss den Weisungen seines Auftraggebers folgeleisten und darf personenbezogene Daten nicht nach eigenem Willen verarbeiten. Des Weiteren ist es wichtig zu verstehen, dass die Auftragsverarbeitung auf Grundlage eines Vertrages erfolgen muss (Art. 28 Abs. 3 DS-GVO – dazu später mehr).

Die Verarbeitung

Der Begriff der „Verarbeitung“ ist sehr weit gefasst. Die DS-GVO versteht unter der Verarbeitung z.B. das Erheben, Speichern, Verändern, Ordnen,…, von personenbezogenen Daten. Wenn man sich die Begrifflichkeiten vor Augen führt, ist die Frage, ob der Cloud-Dienst-Anbieter ein Auftragsverarbeiter ist, leicht mit „ja“ zu beantworten. Ein Cloud-Anbieter verarbeitet, etwa in Form der Speicherung, Daten seines Anwenders, also des Verantwortlichen – dabei darf man nicht vergessen, dass es sich um personenbezogene Daten handeln muss. Handelt es sich nicht um personenbezogene Daten, sind die Datenschutzgesetze nicht anwendbar.

Praxisbeispiel: (File-Sync & Share)

Die FYNE Consulting GmbH möchte gewährleisten, dass Bewerbungsunterlagen zwischen den jeweiligen Ansprechpartnern der Fachabteilungen und der Personalabteilung geteilt werden können. Sie beschließt daher die Bewerbungen mithilfe eines Cloud-Ordners zwischen den jeweiligen Fachabteilungen und der Personalabteilungen zu teilen und gemeinsam zu bearbeiten.

Die FYNE Consulting GmbH als Verantwortliche beauftragt somit einen Cloud-Anbieter mit der Verarbeitung personenbezogener Daten in Form der Speicherung von Bewerbungsunterlagen.

Frage 2:

Wofür wird ein Auftragsverarbeitungs-Vertrag benötigt und was muss er beinhalten?

Weitergabe an Dritte nur mit AV-Vertrag

Verantwortliche dürfen personenbezogene Daten grundsätzlich nicht an „Dritte“ weitergeben. Bereits die Übertragung von Daten auf einen anderen Server als den Unternehmensserver ist grundsätzlich nicht erlaubt. Doch wie kann es dann sein, dass man auf Cloud-Anbieter zurückgreifen kann?

Die Lösung: ein Vertrag zur Auftragsverarbeitung. Durch diesen Vertrag wird der Auftragsverarbeiter, also der Cloud Anbieter, rechtlich wie ein Teil des verantwortlichen Unternehmens eingestuft – und nicht als Dritter. Der AV-Vertrag ist also ein effizientes Mittel und gem. Art. 28 Abs. 3 DS-GVO Pflicht, um die Auftragsverarbeitung gesetzeskonform zu gestalten.

Folgende Punkte sollten in dem AV-Vertrag mit dem Cloud-Anbieter geregelt sein:

- Gegenstand und Dauer des Auftrages
- Art und Zweck der Verarbeitung personenbezogener Daten
- Art der personenbezogenen Daten
- Kategorien betroffener Personen (also der Personen, deren Daten verarbeitet werden sollen)
- Technisch organisatorische Maßnahmen, um den Zugriff Unbefugter auf die personenbezogenen Daten zu verwehren
- Unterauftragsverhältnisse
- Kontrollrechte des Auftraggebers
- Mitteilungspflichten des Auftragnehmers bei relevanten Ereignissen
- Weisungsbefugnisse des Auftraggebers
- Löschung und Rückgabe der personenbezogenen Daten

Wann liegt eine Auftragsverarbeitung vor?

IIn der Praxis ist die Bewertung, ob es sich bei einer Dienstleistung um eine Auftragsverarbeitung oder eine sonstige ausgelagerte Leistung handelt, nicht leicht zu treffen. Es sind aber Kriterien benannt, die eine Einordnung präziser ermöglichen. Ist der Dienstleister gegenüber dem Auftraggeber weisungsabhängig, ist dies ein Indikator für eine Auftragsverarbeitung. Besteht ein wirtschaftliches Interesse an den verarbeiteten Daten bzw. am Ergebnis der Verarbeitung seitens des Dienstleisters oder haftet der er für die Richtigkeit und* Rechtmäßigkeit der Verarbeitung spricht dies dafür, dass eine Übermittlung vorliegt.

Eine Reihe von Kriterien zur Bewertung von Verarbeitungsdienstleistungen im Hinblick auf Auftragsdatenverarbeitung finden Sie unter:

https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_12.pdf

Praxisbeispiel: (File-Sync & Share)

Für die Umsetzung des zuvor genannten Vorhabens, Bewerbungs-unterlagen über einen Cloud-Dienst (File Sync & Share) zu teilen, benötigt die FYNE Consulting GmbH einen Vertrag zur Auftragsverarbeitung, um ihrer Verantwortung als „Verantwortlicher“ gem. der DS-GVO gerecht zu werden. Durch den Abschluss eines Auftragsverarbeitungs-vertrages wird sichergestellt, dass der Auftragsverarbeiter (hier der Betreiber des Cloud-Dienstes) alle technisch-organisatorischen Maßnahmen sowie alle weiteren Anforderungen der DS-GVO erfüllt.

Praxistipp

Recherchieren Sie auf den Seiten der Aufsichtsbehörden der jeweiligen Bundesländer, die für Sie in Frage kommen. Diese stellen in der Regel Musterverträge zur Verfügung

Frage 3:

Wer trägt die Verantwortung bei der Verarbeitung von personenbezogenen Daten?

Die Gesamtverantwortung für Datenverarbeitung und Nachweispflicht trägt nach Art. 5 Abs. 2 DS-GVO der Verantwortliche – die Verantwortung umfasst auch die Verarbeitung durch den Cloud-Anbieter. Verstößt aber ein Cloud-Anbieter gegen die Pflicht zur weisungsgebundenen Verarbeitung, indem er die Daten des Auftraggebers verordnungswidrig für eigene Zwecke oder Zwecke Dritter verarbeitet, gilt er nach Art. 28 Abs. 10 DS-GVO insoweit selbst als Verantwortlicher – mit allen rechtlichen Folgen, z.B. der Haftung, aber auch der Pflicht zur Erfüllung der Betroffenenrechte.

Dennoch ist es für Verantwortliche enorm wichtig, den Auftragsverarbeiter vor Abschluss eines Vertrages bezüglich getroffener Maßnahmen zur Vermeidung von Datenpannen zu prüfen und die getroffenen Maßnahmen, insbesondere die technisch organisatorischen Maßnahmen, schriftlich festzuhalten.

Praxistipp

Eine Liste der erforderlichen technisch-organisatorischen Maßnahmen sollte in jedem Anhang eines Auftragsverarbeitungsvertrages vorhanden sein. Der Auftragsverarbeiter ist dafür zuständig die jeweiligen Punkte, wie z.B. Zugangskontrolle, Übermittlungskontrolle, etc. durch präzise Angaben, wie diese erfüllt werden, einzutragen.

Frage 4:

Darf man einen Cloud-Anbieter aus dem EU-Ausland beauftragen?

Auch Auftragsverarbeiter, die Ihren Sitz im EU-Ausland (also nicht in der EU) haben, müssen sich an die Pflichten der DS-GVO halten, denn es gilt das Marktortprinzip. Das Markortprinzip stellt eine Neuerung, der ab Mai 2018 geltenden DS-GVO dar. Die Regelung betrifft vor allem Unternehmen, die sich außerhalb der Union befinden. Danach findet die DS-GVO *„Anwendung auf die Verarbeitung personenbezogener Daten von betroffenen Personen, die sich in der Union befinden, durch einen nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeiter, wenn die Datenverarbeitung im Zusammenhang damit steht“.*
Vorliegend bedeutet es, dass auch Cloud-Anbieter aus dem EU-Ausland, die personenbezogene Daten aus der EU verarbeiten, unter den Anwendungsbereich der DS-GVO fallen.

Im EU-Ausland ansässige Cloud-Anbieter müssen ein zur EU-DS-GVO gleichwertiges Datenschutzniveau nachweisen. Das kann z.B. entweder geschehen indem es über eine offizielle Stelle des Staates bestätigt wird (z.B. EU-U.S. Privacy Shield) oder durch die Verwendung von Standardvertragsklauseln. Standardvertragsklauseln sind von der Europäischen Kommission verabschiedete Vertragsentwürfe mit deren Unterzeichnung ein Cloud-Anbieter sich dazu verpflichtet die Europäischen Datenschutzstandards einzuhalten. Ist dies nicht der Fall, dürfen die Dienste des Cloud-Anbieters für die Verarbeitung personenbezogener Daten nicht genutzt werden. Dabei ist es unerheblich, ob diese Daten (z.B. durch Verschlüsselung) gegen Fremdzugriffe geschützt werden.

Praxistipp

Soll ein Cloud-Anbieter außerhalb der EU in Anspruch genommen werden, kann man für US-amerikanische Unternehmen unter folgendem Link: https://www.privacyshield.gov/list recherchieren, ob sich das angesprochene Unternehmen dem EU-U.S. Privacy Shield verpflichtet hat.

Frage 5:

Wie wähle ich den richtigen Cloud-Anbieter aus Sicht der DS-GVO?

Cloud-Anbieter müssen technisch organisatorische Maßnahmen ergreifen und einhalten, die den Schutz personenbezogener Daten vor Unbefugten gewährleisten. Einige dieser Maßnahmen sind:

Verfügbarkeit
Personenbezogene Daten stehen zeitgerecht zur Verfügung und können ordnungsgemäß von autorisierten Benutzern verarbeitet werden.

Vertraulichkeit
Nur Befugte können personenbezogene Daten zur Kenntnis nehmen.

Zugriffskontrolle
Die Daten müssen mithilfe von Firewalls und Viren-Software vor Beschädigung und Diebstahl geschützt sein.

Integrität
Personenbezogene Daten bleiben während der Verarbeitung unversehrt, vollständig und aktuell.

Authentizität
Der Ursprung von personenbezogenen Daten kann eindeutig festgestellt werden.

Datensparsamkeit
Datensparsamkeit konkretisiert den Grundsatz der Erforderlichkeit, der vom Verarbeitungsprozess insgesamt verlangt, nicht mehr personenbezogene Daten zu erheben und zu verarbeiten, als zur Erreichen des Verarbeitungszwecks erforderlich sind. Hierzu gehört auch das Löschen von personenbezogenen Daten, die nicht mehr benötigt werden.

Transparenz
Die Verarbeitung personenbezogener Daten kann mit zumutbarem Aufwand nachvollzogen, überprüft und bewertet werden, z.B. wer wann welche personenbezogenen Daten wie verarbeitet hat.

Kommunikationskonzept:
Die Kommunikation zu den Verantwortlichen für verschiedene Szenarien sollte klar organisiert und definiert sein.

Intervenierbarkeit:
Verfahren sind so zu gestalten, dass sie den Betroffenen die Ausübung der ihnen zustehenden Rechte wirksam ermöglichen und entsprechende Funktionalitäten für die Daten verarbeitende Stelle zur Verfügung stehen.

Frage 6:

Wie kann der Cloud-Anbieter das Bestehen von technisch organisatorischen Maßnahmen nachweisen?

Cloud-Anwendern ist es in der Regel nicht oder nur selten möglich, sich direkt bei den Cloud-Anbietern von der vertragsgemäßen Verarbeitung der Daten zu überzeugen. Die Daten und Anwendungen können zeitgleich über eine Vielzahl von geografisch getrennten Standorten verteilt sein. Eine Vor-Ort-Kontrolle wird dadurch unmöglich. Es ist daher zwingend notwendig und vertraglich zu regeln, dass der Cloud-Anbieter alle möglichen Unter-Anbieter sowie alle Standorte bekannt gibt, an denen die Verarbeitung stattfindet bzw. im Rahmen des Vertragsverhältnisses stattfinden könnte. Dazu gehören insbesondere auch die Standorte der Unter-Anbieter.

In diesem Zusammenhang ist darauf hinzuweisen, dass der Cloud-Anbieter für die Datenverarbeitung der Unter-Anbieter haftet, aber mit zunehmender Anzahl von eingebundenen Unter- Anbietern selbst das Problem hat, die Kontrolle über die Daten zu verlieren.

Dem Problem schwieriger Überprüfbarkeit der vertragsgemäßen Verarbeitung der Daten kann unter Umständen dadurch begegnet werden, dass lediglich Angebote von Cloud-Anbietern genutzt werden, die regelmäßig von unabhängigen Stellen auditiert und zertifiziert werden.

Unabhängige Stellen (z.B. anerkannte Zertifizierungsstellen) können die Korrektheit der entsprechenden Verfahren zu einem Prüfzeitpunkt bestätigen. Bislang ist zwar noch kein genehmigtes Zertifikat vorhanden, doch speziell auf die Anforderungen der DS-GVO ausgerichtete Zertifikate können trotzdem schon als Nachweis der DS-GVO-Konformität genutzt werden (z.B. 27001 = IT-Grundschutz). Zusätzlich ist es für die Transparenz gegenüber dem Anwender von Vorteil, wenn der Anbieter von Cloud-Diensten regelmäßig Berichte über das Sicherheitsumfeld zu den Diensten veröffentlicht. Bei akuten Vorfällen ist ein unverzügliches und aussagekräftiges direktes Informieren der Cloud-Anwender erforderlich.

Ein den deutschen Datenschutzanforderungen gleichwertiges Datenschutzniveau ist lediglich dann gewährleistet, wenn die Verarbeitung personenbezogener Daten ausschließlich innerhalb der EU oder EWR-Vertragsstaaten stattfindet und die personenbezogenen Daten bei Unternehmen gespeichert und verarbeitet werden, die keinen EU/EWR-fremden staatlichen Kontrollen unterstehen.

Exkurs:

Datenübermittlung ins Ausland

Erhebt ein Unternehmen Daten im Inland, dürfen sie ohne Zustimmung der betroffenen Personen oder eine gesetzliche Erlaubnis nur dann ins Ausland abgeführt werden, wenn es sich um Mitgliedstaaten der EU oder des Europäischen Wirtschaftsraums handelt.

Bei einer Auftragsverarbeitung in Drittländern, also Staaten außerhalb der Europäischen Union (EU) und des Europäischen Wirtschaftsraums (EWR), hat die DS-GVO bedeutsame Neuerungen vorgenommen. Bislang waren nach BDSG nur Auftragsverarbeitungen innerhalb der EU von den privilegierenden Regelungen gedeckt. Sobald im Rahmen einer Auftragsverarbeitung die EU/EWR-Grenzen überschritten wurden, weil der Dienstleister sich in einem Drittland befand, galt dieser nicht mehr als Auftragsverarbeiter, sondern als Dritter. Dritter ist jede Person oder Stelle, die nicht in den Kreis des verantwortlichen Auftraggebers fällt. Gegenüber einem Dritten war und ist auch nach der DS-GVO die Datenverarbeitung unter den vereinfachten Bedingungen der Auftragsverarbeitung nicht möglich.

Eine Übermittlung personenbezogener Daten in ein Drittland ist nach Art. 44 DS-GVO nur zulässig, wenn die weitere Verarbeitung nach den Regeln der DS-GVO erfolgt und vergleichbare Schutzmechanismen dafür sorgen, dass die vorgesehenen Rechte der Betroffenen nicht ausgehebelt werden.

Eine Datenübermittlung in ein Drittland kann beispielsweise durch Angemessenheitsbeschlüsse der EU-Kommission gemäß Art. 45 DS-GVO zulässig sein. Hiernach beschließt die Kommission, dass ein bestimmtes Drittland ein angemessenes Datenschutzniveau bietet.

Drittländer mit angemessenem Datenschutzniveau:

- Andorra,
- Argentinien,
- Kanada (nur kommerzielle Organisationen),
- Färöer,
- Guernsey,
- Israel,
- Isle of Man,
- Jersey,
- Neuseeland,
- Schweiz,
- Uruguay
- USA (wenn der Empfänger dem Privacy Shield angehört).

Eine Übertragung in ein Drittland, in dem der Schutz der personenbezogenen Daten nicht sichergestellt werden kann, ist dann möglich, wenn eine Einwilligung des Betroffenen vorliegt. Hier ist jedoch insbesondere die Anforderung der Freiwilligkeit zu beachten. Ausnahmen sind die Übermittlung zur Vertragserfüllung, wichtige Gründe des öffentlichen Interesses und die Geltendmachung von Rechtsansprüchen.

Die Folge

Soll eine Marketing-Firma in den USA, welche sich nicht dem EU-U.S. Privacy-Shield unterworfen hat, mit der Erstellung eines Newsletters (etwa durch die Bereitstellung eines Newsletter-Dienstes in der Cloud) beauftragt werden und erhält diese dafür Zugriff auf die Kundendaten (hier typischerweise mindestens die E-Mailadressen der Newsletter-Adressaten), benötigt sie dafür die Einwilligung sämtlicher Personen, denen die Daten gehören.

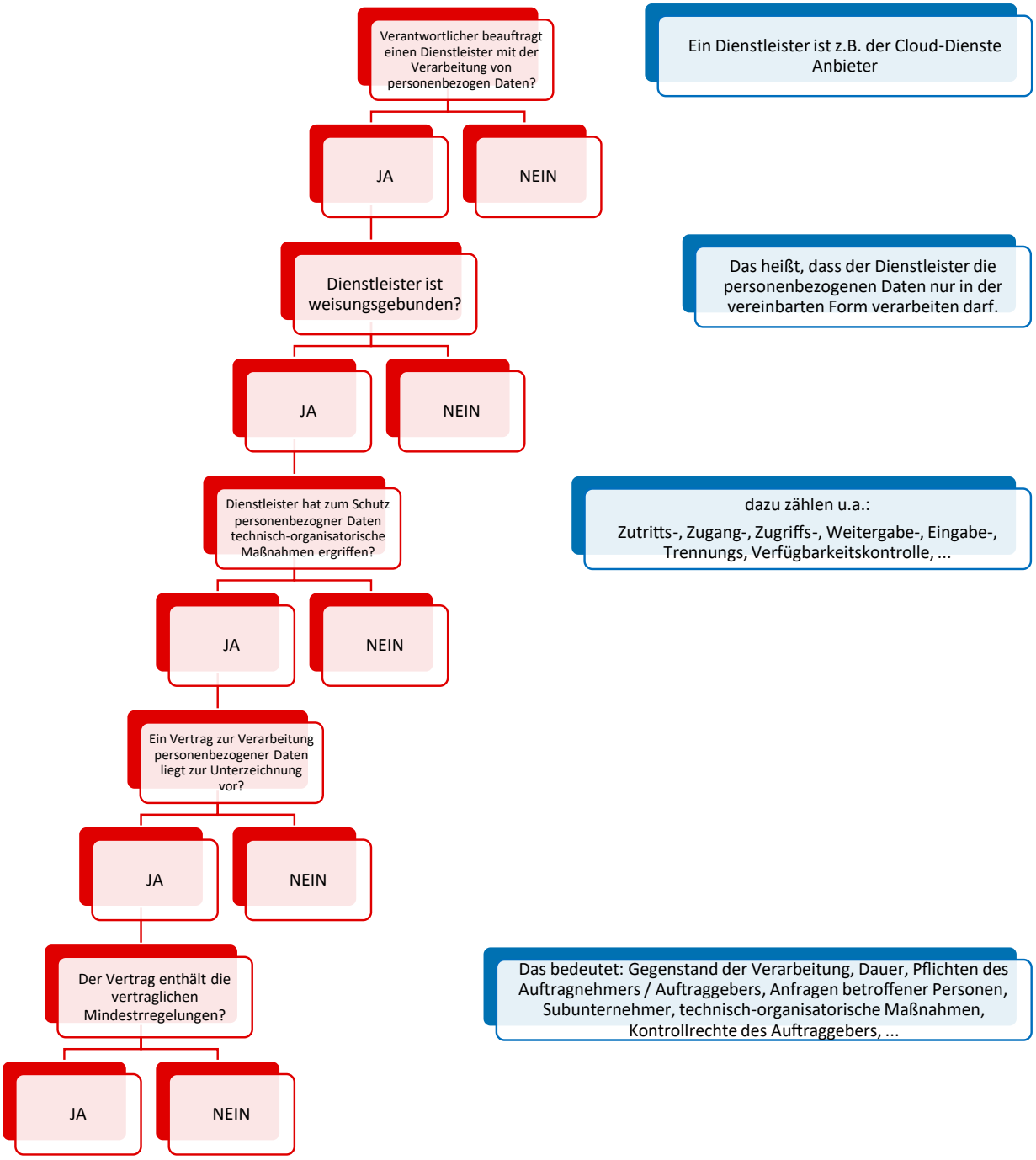
Zusammenfassung

Die Nutzung von Cloud Computing und die DS-GVO stehen nicht im Widerspruch zueinander. Die Regelungen der DS-GVO beschränken also nicht die Nutzung von Cloud-Diensten. Faktisch werden Anwender von Cloud-Diensten sogar besser geschützt, da sie durch die Verwendung von Auftragsverarbeitungsverträgen in die Pflicht genommen werden, ihre Cloud-Dienste genauer zu prüfen.

Auch für die Cloud-Anbieter kann die DS-GVO eine Chance sein. Die gesetzliche Pflicht die technisch-organisatorischen Maßnahmen zu ergreifen, können Marketinginstrumente darstellen. Durch den cleveren Einsatz von Maßnahmen können sich Cloud-Anbieter zukünftig von ihren Mitbewerbern absetzen, indem Sie mit der Datenschutzkonformität der DS-GVO werben.

Ablaufschema

Auswahl eines DS-GVO-konformen Cloud-Anbieters



Mittelstand | 4.0 Agentur Cloud

Über die Mittelstand 4.0-Agentur Cloud

Die Mittelstand 4.0-Agentur Cloud besteht aus den Projektpartnern Fraunhofer IAO, der Hoch- schule Osnabrück und der IT-Dienstleistungs¬gesellschaft mbH Emsland (kurz: it.emsland). Sie unterstützt durch ihre Arbeit Multiplikatoren wie beispielsweise Kammern oder Verbände, die Unternehmen auf ihrem Weg in die Digitalisierung begleiten. Die Mittelstand 4.0-Agentur Cloud ist Teil der Förderinitiative “Mittelstand-Digital – Strategien zur digitalen Transformation der Unternehmensprozesse”.

Was ist Mittelstand-Digital?

Mittelstand-Digital informiert kleine und mittlere Unternehmen über die Chancen und Herausforderungen der Digitalisierung. Die geförderten Kompetenzzentren helfen mit Expertenwissen, Demonstrationszentren, Best-Practice-Beispielen sowie Netzwerken, die dem Erfahrungsaustausch dienen. Das Bundesministerium für Wirtschaft und Energie (BMWi) ermöglicht die kostenfreie Nutzung aller Angebote von Mittelstand-Digital.

Der DLR Projektträger begleitet im Auftrag des BMWi die Projekte fachlich und sorgt für eine bedarfs- und mittelstandsgerechte Umsetzung der Angebote. Das Wissenschaftliche Institut für Infrastruktur und Kommunikationsdienste (WIK) unterstützt mit wissenschaftlicher Begleitung, Vernetzung und Öffentlichkeitsarbeit.

Weitere Informationen finden Sie unter www.mittelstand.digital

Impressum

Verleger
Mittelstand 4.0-Agentur Cloud
c/o IT-DienstleistungsGmbH Emsland
Geschäftsführer:
Dipl.-Inform. Michael Schnaider
Kaiserstraße 10B
49809 Lingen (Ems)

T 0049/ 591/ 8076 980
F 0049/ 591/ 8076 989
E info@it-emsland.de

Sitz: Lingen (Ems)
Reg.-G: Amtgericht Osnabrück, HBR 100772
USt-IdNr. Gem. §27a UStG.: 220043875

Für den Inhalt Verantwortliche gem. § 55 II RStV
IT-Dienstleistungsgesellschaft mbH Emsland
Michael Schnaider
Kaiserstr. 10b
49809 Lingen (Ems)

FYNE Consulting GmbH
Nicole Fedder, Erden Yücel
Kaiserstr. 10b
49809 Lingen (Ems)

T 0049/ 591/ 8076 980
F 0049/ 591/ 8076 989
E schnaider@it-emsland.de

Grafik und Layout
Rolf Andreas Kraß-Westerink

Druck
Flyeralarm GmbH, Alfred-Nobel-Str. 18, 97080 Würzburg

Auflage
250 Exemplare

Stand
September 2018

Fraunhofer IAO

HOCHSCHULE OSNABRÜCK
UNIVERSITY OF APPLIED SCIENCES

it.emsland
IT-Dienstleistungsgesellschaft mbH Emsland