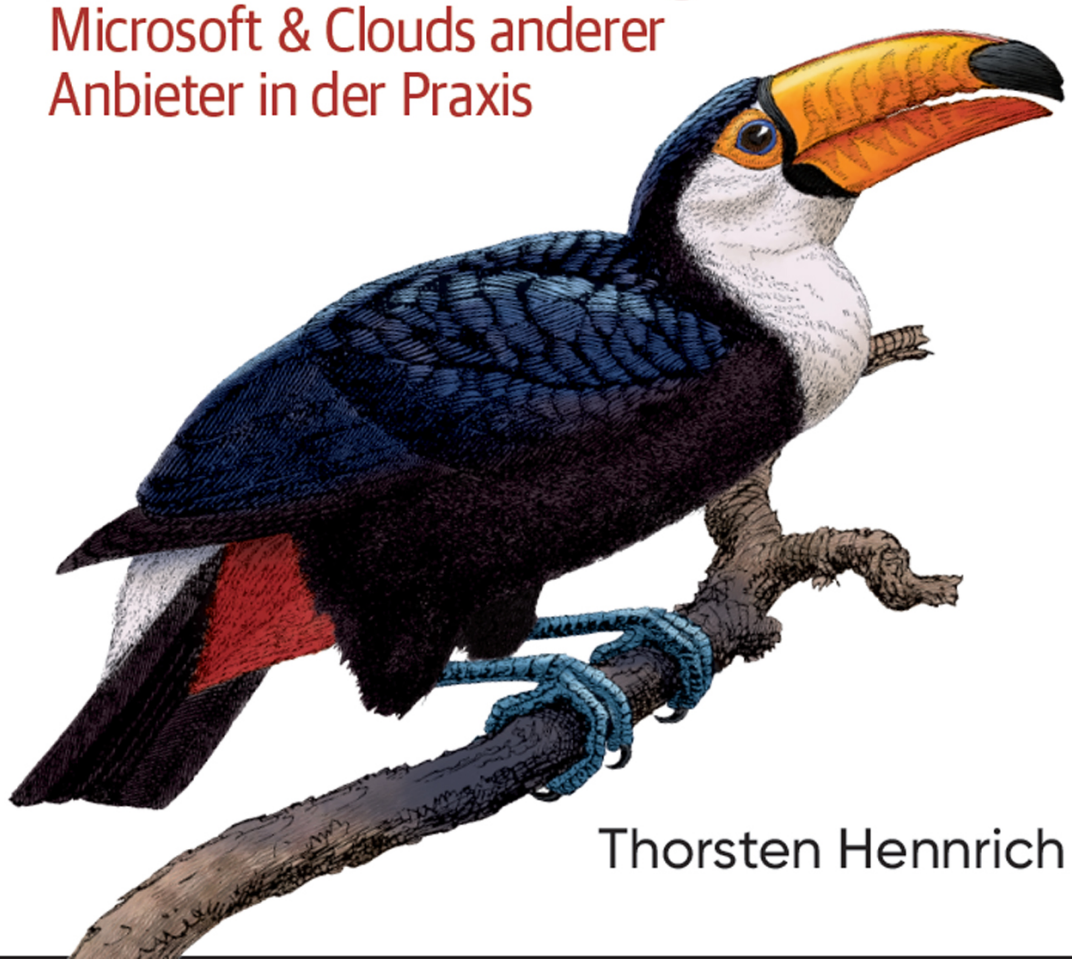
O'REILLY®

Cloud Computing nach der Datenschutz-Grundverordnung

Amazon Web Services, Google, Microsoft & Clouds anderer Anbieter in der Praxis



Thorsten Hennrich

Inhalt

KAPITEL 4

Wann ist die DSGVO im Cloud Computing überhaupt anzuwenden?

Jede datenschutzrechtliche Prüfung der DSGVO beginnt auch im Cloud Computing zunächst mit der grundlegenden Frage nach ihrer *Anwendbarkeit*. Es muss also geprüft werden, ob die DSGVO – sowie gegebenenfalls weitere Rechtsvorschriften – auf eine konkrete Datenverarbeitungstätigkeit *in sachlicher und räumlicher Hinsicht* überhaupt anzuwenden ist.

Die Klärung des sachlichen und räumlichen Anwendungsbereichs hat eine *Schlüsselfunktion* und öffnet quasi das Tor zur DSGVO. Denn möglicherweise ist der Sachverhalt ja so gelagert, dass gar nicht die DSGVO, sondern vielmehr Datenschutzregelungen aus einem komplett anderen Rechtsraum auf die zugrunde liegende Verarbeitungstätigkeit anzuwenden sind. Um zur besseren Veranschaulichung einmal ein etwas exotischeres Beispiel zu nehmen: Ist auf eine Datenverarbeitung in der Cloud die DSGVO anwendbar – oder unterfällt die Verarbeitung nicht etwa doch dem *Personal Data Protection Act* in Singapur oder dem brasilianischen *Lei Geral de Proteção de Dados Pessoais?*

Kurz erklärt: Anwendbarkeit der DSGVO

Im Rahmen der Anwendbarkeit ist zu prüfen, ob die DSGVO – sowie gegebenenfalls weitere Rechtsvorschriften – auf eine konkrete Datenverarbeitungstätigkeit in sachlicher und räumlicher Hinsicht überhaupt anzuwenden ist. Die Klärung des sachlichen und räumlichen Anwendungsbereichs hat eine Schlüsselfunktion und öffnet quasi das Tor zur DSGVO.

Für den Fall, dass es absolut unstrittig ist, dass die DSGVO anzuwenden und von einem Unternehmen zu beachten ist (wie bei den meisten Verarbeitungen von *personenbezogenen Daten* in der Cloud durch ein Unternehmen in der EU der

Fall), kann dieses Kapitel auch übersprungen werden. Ist es hingegen unklar, ob überhaupt personenbezogene Daten vorliegen oder die DSGVO auch räumlich anzuwenden ist (bzw. Ausnahmen vom Anwendungsbereich bestehen), dann ist dieses Kapitel genau richtig.

4.1 Sachlicher Anwendungsbereich: Werden personenbezogene Daten verarbeitet?

Im Rahmen des *sachlichen Anwendungsbereichs* geht es um die Frage, ob eine konkrete Datenverarbeitungstätigkeit *in sachlicher Hinsicht* in den Anwendungsbereich der DSGVO fällt. Um den Anwendungsbereich insoweit zu *eröffnen* (Schlüsselfunktion), muss die Datenverarbeitungstätigkeit vor allem die in Art. 2 DSGVO enthaltenen Anwendungsvoraussetzungen erfüllen:

- eine Verarbeitung personenbezogener Daten,
- ganz oder teilweise automatisiert bzw. nicht automatisiert mit Speicherung in einem Dateisystem und
- keine Ausnahme vom Anwendungsbereich (z. B. Verarbeitung für »private Zwecke«).

Kurz erklärt: Sachlicher Anwendungsbereich

Beim sachlichen Anwendungsbereich geht es um die Frage, ob eine Datenverarbeitungstätigkeit den Anwendungsvoraussetzungen der DSGVO in sachlicher Hinsicht unterfällt. Dies ist der Fall, wenn:

- eine Verarbeitung personenbezogener Daten vorliegt,
- die ganz oder teilweise automatisiert bzw. nicht automatisiert mit Speicherung in einem Dateisystem erfolgt und
- keine Ausnahme vom Anwendungsbereich einschlägig ist (z. B. für »private Zwecke«).

Die *Verarbeitung personenbezogener Daten* haben Sie bereits im Rahmen der wichtigen Begriffe in Abschnitt 3.5.1 kurz kennengelernt. Aufgrund ihrer Schlüsselfunktion für die DSGVO und der besonderen Bedeutung bei Auslagerungsszenarien in die Cloud schauen wir uns die Begriffe *personenbezogene Daten* und *Verarbeitung* im Folgenden etwas genauer an.

4.1.1 Personenbezogene Daten

Personenbezogene Daten sind der zentrale Schlüssel zur Anwendung des Datenschutzrechts. Aufgrund dieser Schlüsselfunktion ist es eine zentrale Grundfrage, ob überhaupt personenbezogene Daten vorliegen – oder nicht. Auch wenn dies in den meisten Cloud-Nutzungsszenarien von Unternehmen typischerweise der Fall sein wird, ist es wichtig, zu verstehen, was personenbezogene Daten überhaupt sind.

Die gesetzliche Definition zu *personenbezogenen Daten* (eine sogenannte *Legaldefinition*) ist in Art. 4 Nr. 1 DSGVO zu finden. Personenbezogene Daten sind hiernach alle Informationen, die sich auf eine *identifizierte oder identifizierbare* natürliche Person beziehen. Zu unterscheiden ist zwischen den Alternativen *identifiziert oder identifizierbar*.

Identifiziert Typische Beispiele für personenbezogene Daten, die eine Person im Sinne der ersten Alternative *direkt identifizieren* können, sind deren Name und Anschrift, Geburtsdatum, E-Mail-Adresse, biometrische Daten sowie Foto- und Videoaufnahmen. Hier lässt sich die Identifizierung der natürlichen Person unmittelbar anhand der Daten herstellen.

Identifizierbar Dagegen gestaltet sich das Vorliegen eines Personenbezugs im Rahmen der zweiten Alternative einer *Identifizierbarkeit* deutlich schwieriger. Eine natürliche Person wird als *identifizierbar* angesehen, wenn sie *direkt oder indirekt*, insbesondere mittels Zuordnung zu einer Kennung oder einer Kennnummer, zu Standortdaten, zu einer Online-Kennung zu besonderen Merkmalen ihrer Identität, identifiziert werden kann. Beispiele sind Telefonnummer, Kontonummer, Personalausweisnummer, Steuernummer, Versicherungsnummer, Kreditkartendaten, Kfz-Kennzeichen oder eine Religionszugehörigkeit. Auch Benutzernamen oder Nicknames (etwa für Twitter, Instagram oder Internetforen) machen eine Person indirekt identifizierbar und sind damit personenbezogene Daten. Von Bedeutung sind aber auch Zuordnungen zu Online-Kennungen. Hierzu zählen insbesondere IP-Adressen oder Browser-Fingerprints, die meist als personenbezogene Daten anzusehen sind. Aber auch Informationen über die Persönlichkeit, wie die Interessen oder Reiseziele eines Einzelnen, können die dahinterstehende natürliche Person direkt oder indirekt *identifizierbar* machen, insbesondere über diesbezügliche Informationen und Spuren in Social-Media-Plattformen.

Wissen Dritter Ob und in welchem Umfang im Rahmen der Identifizierbarkeit auch das Wissen Dritter einzubeziehen ist, ist eine viel diskutierte Frage. Es geht hierbei im Kern darum, ob es zur Bejahung eines Personenbezugs ausreicht, dass dazu irgendein Dritter weltweit die entsprechenden Kenntnisse und

Möglichkeiten hat oder ob hierfür allein das Wissen und die Möglichkeiten zu berücksichtigen sind, die dem Verantwortlichen selbst zur Verfügung stehen.

Wer sich schon etwas länger mit Datenschutz beschäftigt, wird sich daran erinnern, dass auch schon zu Zeiten des »alten« Bundesdatenschutzgesetzes im Rahmen der vergleichbaren Frage nach der *Bestimmbarkeit* einer natürlichen Person (§ 3 BDSG a. F.) hierzu verschiedene Ansichten vertreten wurden. So sollte auf der einen Seite bereits jede *objektiv* bestehende Möglichkeit bei irgendeinem Dritten ausreichen (so vor allem die Datenschutzbehörden). Auf der anderen Seite wurde für eine Bestimmbarkeit ein eher *relatives Verständnis* befürwortet, sodass gerade nicht jegliches Wissen Dritter, sondern die im konkreten Fall bei verhältnismäßigem Aufwand zur Verfügung stehenden Kenntnisse, Mittel und Möglichkeiten zu berücksichtigen sind.

Diese beiden Grundpositionen werden im Grundsatz auch im Rahmen der DSGVO diskutiert. Eine richtungsweisende Entscheidung hat der EuGH im Jahr 2016 in Bezug auf IP-Adressen getroffen. Hiernach ist eine Identifizierbarkeit – und damit ein Personenbezug – zu bejahen, wenn der Verantwortliche auch mit rechtlichen Mitteln (z. B. unter Einschaltung von Behörden) in der Lage ist, eine natürliche Person zu identifizieren. IP-Adressen sind daher personenbezogen, wenn beispielsweise ein Webseitenbetreiber rechtlich in der Lage ist, die für eine Identifikation erforderlichen Daten von dem Internetzugangsanbieter herauszuverlangen. Dagegen sind etwa die in der Praxis für Tracking-Zwecke beliebten Cookies für den Betreiber einer E-Commerce-Plattform oder eines Webshops schon allein dann personenbezogen, wenn er die Möglichkeit hat, diese einem Nutzer und den in einem Benutzerkonto hinterlegten Daten (wie Name, Rechnungs- und Lieferanschriften) zuzuordnen.

In Bezug auf *personenbezogene Daten* ist vor diesem Hintergrund festzuhalten, dass dieser Begriff aufgrund der Gleichstellung von *identifiziert* und *identifizierbar* in sachlicher Hinsicht weit zu verstehen ist. Denn der Sache nach sind praktisch alle Informationen personenbezogen, die mit einer natürlichen Person in Verbindung gebracht werden können. Erfasst sind also sämtliche Informationen, die sich unmittelbar auf natürliche Personen (also auf Menschen) beziehen oder eine solche Person identifizieren können. Dies können etwa persönliche Identifikationsmerkmale (wie Name, Anschrift, Telefonnummer, E-Mail-Adresse, Geburtsdatum, Personalausweisnummer, Steuernummer, IP-Adresse) oder sachliche Informationen (wie Beruf, Eigentumsverhältnisse) sein. Aber auch äußere Merkmale einer Person (wie biometrische Daten, Geschlecht, Größe, Foto- und Videoaufnahmen) oder innere Überzeugungen (wie Religionszugehörigkeit, politische Meinungen) können als personenbezogene Daten anzusehen sein. Übertragen auf das heutige Geschäftsleben und die

Datensätze, die von einem Unternehmen typischerweise in die Cloud ausgelagert werden, ist ein Personenbezug daher vor allem bei Kundendaten, Nutzerprofilen, elektronischen Adressbüchern, E-Mails, Lohn- und Gehaltsdaten, Sales-Leads, Marketinglisten für personalisierte Werbung, bei zahlreichen Web-Tracking-Anwendungen, Datensätzen in CRM-Lösungen und in aller Regel auch bei nicht gekürzten IP-Adressen anzunehmen.

Zur Wiederholung: Personenbezogene Daten

Personenbezogene Daten sind alle Informationen, die sich auf natürliche Personen beziehen oder eine solche Person identifizieren können. Beispiele für personenbezogene Daten sind Name, Anschrift, E-Mail-Adresse, Telefonnummer, Geburtsdatum, Personalausweisnummer, Steuernummer, IP-Adresse sowie Foto- und Videoaufnahmen.

Praxistipp: Weites Verständnis von »personenbezogenen Daten«

Personenbezogene Daten sind in sachlicher Hinsicht der zentrale Schlüssel zum Datenschutzrecht. Dem Begriff liegt ein weites Begriffsverständnis zugrunde, da praktisch alle Informationen, die mit einer natürlichen Person in Verbindung gebracht werden können, personenbezogen sind. Neben den Daten, die eine natürliche Person unmittelbar identifizieren (wie Name, Anschrift, E-Mail-Adresse) können auch Daten, die eine Person identifizierbar machen (wie Kennnummern, IP-Adressen oder Browser-Fingerprints) personenbezogene Daten darstellen.

Reine Sachdaten ohne Personenbezug (wie z. B. Ergebnisse der Fußballbundesliga) sind dagegen vom Schutzbereich des Datenschutzrechts ausgenommen und stellen keine personenbezogenen Daten dar.

Hinweis: Schutz von nicht personenbezogenen Daten

Die DSGVO ist nur auf personenbezogene Daten anwendbar. Nichtpersonenbezogene Daten sind jedoch nicht komplett schutzlos. Ihre

Sicherheit ist vielmehr nach den Grundsätzen der allgemeinen Daten- und Informationssicherheit zu bewerten.

Personen, deren personenbezogene Daten geschützt werden sollen, werden *betroffene Personen* oder *Betroffene* genannt.

Juristische Personen oder Personengruppen Juristische Personen oder bestimmte Gruppen von Personen sind aus dem Schutzbereich des Datenschutzrechts ausgenommen. Dies betrifft Daten, die ausschließlich Bezug auf juristische Personen (also Unternehmen wie eine GmbH oder eine AG), Personengruppen, Personenmehrheiten oder verstorbene Personen nehmen. Auch die Firma (Name einer Gesellschaft) oder andere Unternehmensdaten fallen nicht in den Schutzbereich der DSGVO. Dagegen sind der Name oder die Kontaktdaten eines Geschäftsführers oder Angestellten einer GmbH sehr wohl an der DSGVO zu messen.

Der Schutz der DSGVO endet grundsätzlich mit dem Tod einer betroffenen Person. Dies gilt ausnahmsweise nicht, soweit Daten nicht nur mit Verstorbenen, sondern auch mit lebenden Personen in Verbindung stehen.

Nicht-EU-Bürger können betroffene Personen sein, soweit ihre Daten durch Verantwortliche oder Auftragsverarbeiter verarbeitet werden, die in den räumlichen Anwendungsbereich der DSGVO fallen.

Das weite begriffliche Verständnis personenbezogener Daten führt zu einem weiten sachlichen Anwendungsbereich der DSGVO. In der Praxis hat dies zur Folge, dass in den allermeisten Datenverarbeitungsszenarien von Unternehmen oder der öffentlichen Hand von der Verarbeitung personenbezogener Daten auszugehen ist, da sich regelmäßig nur wenige Datensätze als reine Sachdaten (wie z. B. Bundesligaergebnisse ohne Torschützen, rein mathematische Berechnungen, Vermessungsdaten) ohne jeglichen Personenbezug eindeutig qualifizieren lassen.

Praxistipp: Im Zweifel von einem Personenbezug ausgehen

In der Praxis lassen sich in der Regel nur wenige Datensätze als reine Sachdaten ohne Unternehmensbezug qualifizieren. Im Zweifel sollte von einem Personenbezug ausgegangen werden.

Pseudonymisierung Im Kontext von personenbezogenen Daten ist immer auch an die *Pseudonymisierung* zu denken. Hierunter ist eine Verarbeitung personenbezogener Daten in einer Weise zu verstehen, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können (z.B. Kennnummern, Aliase etc.). Die zusätzlichen Informationen sind dabei gesondert aufzubewahren. Sie unterliegen technischen und organisatorischen Maßnahmen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden. Pseudonymisierte Daten sind eine zusätzliche Schutzmaßnahme, jedoch weiterhin als personenbeziehbar anzusehen, da ein Pseudonym anhand von zusätzlichen Informationen einer natürlichen Person zugeordnet werden kann.

Anonymisierung Durch eine Anonymisierung kann der Personenbezug dagegen unwiederbringlich entzogen werden. Es handelt sich hierbei um eine Verarbeitung personenbezogener Daten, die ebenfalls einer Rechtsgrundlage bedarf. Sind hiernach die ursprünglich personenbezogenen Daten derart verarbeitet, dass eine betroffene Person nicht oder nicht mehr identifiziert werden kann, sind die Daten anonymisiert, und es liegen keine personenbezogenen Daten mehr vor. Auf anonymisierte Daten ist die DSGVO ist nicht mehr anwendbar.

Wie begegnen mir personenbezogene Daten im Cloud Computing? Im Cloud Computing – etwa im Rahmen eines AV-Vertrags, dem Verarbeitungsverzeichnis oder allgemeinen Dokumentationspflichten (hierzu später mehr) – sind personenbezogene Daten meist weiter zu kategorisieren. Beispiele für eine solche Kategorisierung personenbezogener Daten sind: Stammdaten, Adressdaten, Mitarbeiter-/Personaldaten, Kontaktdaten, Bankverbindungsdaten, Daten von Videoaufzeichnungen von Überwachungskameras.

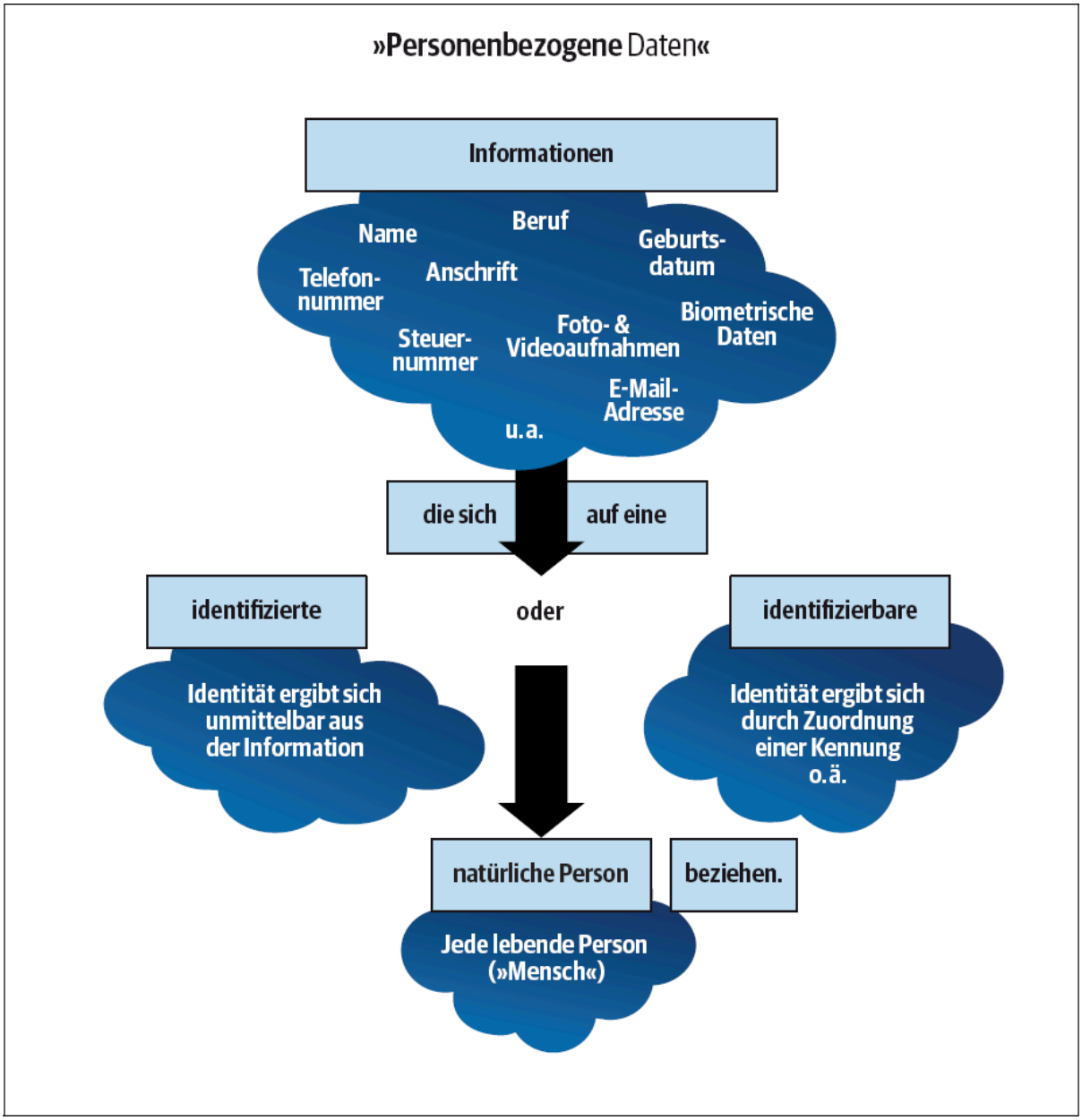


Abbildung 4-1: Personenbezogene Daten

4.1.2 Verarbeitung

Ein weiterer zentraler und umfassender Begriff der DSGVO ist die *Verarbeitung*. Nach Art. 4 Abs. 2 DSGVO ist *Verarbeitung* jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung. Diese – ebenfalls etwas kompliziert formulierte – Legaldefinition verdeutlicht, dass die DSGVO auch den Begriff der Verarbeitung weit fasst und jeden Vorgang, der unmittelbar oder mittelbar auf personenbezogene Daten einwirkt, als Verarbeitung ansieht.

Gerade für Einsteiger in den Datenschutz ist es daher erfahrungsgemäß einfacher, sich den Begriff der *Verarbeitung* als jeden Vorgang im Zusammenhang mit der *Verwendung* von Daten vorzustellen. Diese Verwendung umfasst quasi den gesamten Zyklus einer Datenverarbeitung und kann von der Erhebung der personenbezogenen Daten über die einzelnen Verarbeitungsschritte und die Nutzung bis hin zur Löschung dieser Daten reichen:

- Erhebung (jedes Beschaffen von Daten, z.B. über ein Kontaktformular auf einer Webseite),
- Verarbeitung (u.a. Speichern, Ändern, Sperren),
- Übermittlung (also Datenweitergabe an Datenempfänger)
- Nutzung und
- Löschung.

Zur Wiederholung: Verarbeitung

Verarbeitung ist quasi jeder Vorgang im Zusammenhang mit der Verwendung von Daten, insbesondere deren Speicherung, Veränderung, Übermittlung, Sperrung, Nutzung und Löschung.

4.1.3 Ganz oder teilweise automatisierte Verarbeitung

Die weitere Voraussetzung einer *ganz oder teilweise automatisierten Verarbeitung* ist grundsätzlich immer dann anzunehmen, wenn Datenverarbeitungsanlagen verwendet werden und eine Verarbeitung tatsächlich stattfindet. Eine konkrete Definition des Begriffs einer automatisierten Verarbeitung ist in der DSGVO jedoch nicht enthalten. Dies ist vor allem darauf zurückzuführen, dass auch zukünftige technologische Entwicklungen von dem Anwendungsbereich der DSGVO erfasst sein sollen (die sogenannte *Technologieneutralität* der DSGVO, wonach der Schutz der personenbezogenen Daten natürlicher Personen nicht von verwendeten Techniken abhängen soll). Es ist somit auch hier von einem grundsätzlich weiten Begriffsverständnis auszugehen. In der Praxis unterliegt damit quasi jede elektronische Datenverarbeitung der DSGVO.

Die Abgrenzung zwischen einer ganz oder teilweise automatisierten Verarbeitung erfolgt anhand der Möglichkeit, manuelle Zwischenschritte vornehmen zu können.

Nicht automatisierte Verarbeitung Art. 2 DSGVO erfasst auch die *nicht automatisierte Verarbeitung* personenbezogener Daten. Sie ist im Cloud Computing nicht von Relevanz, soll aber zur Vollständigkeit kurz erläutert werden. Denn der Schutz natürlicher Personen soll auch bei manuellen Verarbeitungen gewährleistet sein, wenn die personenbezogenen Daten in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Ein *Dateisystem* ist dabei jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich ist, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird. Daher kann das Festhalten personenbezogener Daten auf einem Blatt Papier als manuelle Verarbeitung dem Anwendungsbereich der DSGVO unterfallen, auch wenn die Daten erst später in eine Akte einsortiert werden sollen, die nach bestimmten Kriterien (wie Name oder Aktenzeichen) geordnet ist. Klassische Karteikarten in einem nach bestimmten Kriterien geordneten Karteisystem unterfallen demnach ebenfalls dem sachlichen Anwendungsbereich der DSGVO. Bei der nicht automatisierten Verarbeitung darf kein Zwischenschritt automatisiert sein, da andernfalls eine teilweise automatisierte Verarbeitung vorliegt.

4.1.4 Keine Ausnahme (z.B. für private Zwecke)

Ausnahmen vom sachlichen Anwendungsbereich sind in Art. 2 Abs. 2 und Abs. 3 DSGVO enthalten. Es handelt sich hierbei um Verarbeitungstätigkeiten, auf die die DSGVO keine Anwendung findet, wie zum Beispiel die Verarbeitung personenbezogener Daten außerhalb des EU-Rechts, im Rahmen der *Gemeinsamen Außen- und Sicherheitspolitik* (GASP) oder durch Organe, Einrichtungen, Ämter und Agenturen der EU.

Von Bedeutung ist vor allem die sogenannte *Haushaltsausnahme*, also die Verarbeitung personenbezogener Daten zu persönlichen oder familiären Zwecken (Art. 2 Abs. 2 lit. c DSGVO). Da auch im privaten Umfeld zahlreiche Clouds zum Einsatz gelangen, ist sie eine in der Praxis sehr wichtige und bedeutsame Ausnahme vom sachlichen Anwendungsbereich der DSGVO. Einem Nutzer, der zu rein privaten Zwecken auf die Leistungen eines Cloud-Anbieters zurückgreift, stellen sich typischerweise die folgenden Fragen:

- Gilt die DSGVO auch für mich, wenn ich die Bilder meiner Geburtstagsparty in eine Cloud hochlade und sie allen teilnehmenden Freunden über einen Link zur Verfügung stelle?
- Muss ich alle Freunde und Verwandten um ihre Einwilligung bitten, bevor ich Bilder in die Cloud hochlade?
- Stehen meinen Freunden Betroffenenrechte gegen mich zu?

Nach der *Haushaltsausnahme* findet die DSGVO keine Anwendung, wenn die Verarbeitung zu *rein persönlichen oder familiären Tätigkeiten* erfolgt. Aus Erwägungsgrund 18 DSGVO geht hervor, dass dies Tätigkeiten sind, die ohne Bezug zu einer beruflichen oder wirtschaftlichen Tätigkeit vorgenommen werden. Sobald eine wirtschaftliche oder geschäftliche Tätigkeit vorliegt, greift der Ausnahmetatbestand folglich nicht. Beispiele für *rein persönliche oder familiäre Tätigkeiten* sind private Namens- und Adressbücher (z. B. Kontaktlisten im Freundeskreis oder für gemeinsame Sportaktivitäten) oder Korrespondenzen zwischen Privatpersonen über SaaS-Anwendungen oder soziale Netzwerke.

Die Ausnahme greift jedoch gerade nicht für den Anbieter einer SaaS-Anwendung oder den Betreiber eines sozialen Netzwerks – im Gegenteil: Auf gewerblich tätige Verantwortliche und Auftragsverarbeiter, die mit ihren Anwendungen und Plattformen die Instrumente für die Verarbeitung personenbezogener Daten für persönliche oder familiäre Tätigkeiten bereitstellen, ist die DSGVO sehr wohl anwendbar.

Die Haushaltsausnahme ist grundsätzlich eng zu verstehen. Der Ausnahmetatbestand soll gerade nicht jeden Umgang mit familiären Daten erfassen. Die verdeutlicht auch der Wortlaut des Art. 2 Abs. 2 lit. c DSGVO. Die

Ausnahme soll hiernach nur dann greifen, wenn die Tätigkeit *ausschließlich* zu privaten oder familiären Zwecken erfolgt. Ausgenommen sind also alle Verarbeitungen, die lediglich »auch« privaten Zwecken dienen, zugleich aber andere, insbesondere wirtschaftliche Ziele verfolgen. In der heutigen Arbeitswelt, in der Clouds, Smartphones und Laptops oft tätigkeitsübergreifend sowohl zu privaten wie auch zu beruflichen Zwecken genutzt werden, ist eine solche Abgrenzung aber nicht immer einfach und wird daher auch häufig wegen fehlender Praktikabilität kritisiert. Sinnvoller sei vielmehr eine Schwerpunktbetrachtung, um den Herausforderungen der geräteübergreifenden Nutzung zu privaten und beruflichen Zwecken besser gerecht zu werden. Mit Blick auf Ziel und Zweck des Datenschutzes empfiehlt es sich, die Haushaltsausnahme gegenwärtig eher eng zu verstehen.

Praxistipp: Wo gilt die Haushaltsausnahme wirklich?

Die Haushaltsausnahme ist grundsätzlich eng zu verstehen. Der Ausnahmetatbestand soll gerade nicht jeden Umgang mit familiären Daten erfassen, sondern nur dann greifen, wenn die Tätigkeit *ausschließlich* zu privaten oder familiären Zwecken erfolgt.

Eine Abgrenzung zwischen *privat* und *familiär* ist in der DSGVO nicht enthalten. Der Begriff *familiär* ist aber nicht rein familienrechtlich auszulegen, wie ein vergleichender Blick auf andere Sprachfassungen der DSGVO verdeutlicht. So verwendet die englische Fassung der DSGVO den Begriff *household activity*, die französische Fassung das Wort *domestique*. Der in der deutschen Sprachfassung verwendete Begriff *familiär* ist daher etwas weiter zu verstehen und bezieht sich nicht nur auf die Familie, sondern auch auf den Haushalt.

Bei sozialen Netzwerken oder Anwendungen mit vergleichbaren Einstellungsmöglichkeiten ist vor allem zwischen der Verwendung von personenbezogenen Daten in einem *begrenzten* Personenkreis und in einem *unbestimmten* Personenkreis zu differenzieren. Im Rahmen eines begrenzten Personenkreises – z. B. in Form von Gruppennachrichten – greift die Ausnahme. Bei einem unbestimmten Personenkreis, wenn personenbezogene Daten quasi jedermann zugänglich sind, ist dies aber gerade nicht der Fall, und es greift stattdessen der Datenschutz, sprich: Der *sachliche Anwendungsbereich* der DSGVO ist eröffnet.

4.2 Räumlicher Anwendungsbereich: Wo und durch wen werden die Daten verarbeitet?

Beim *räumlichen Anwendungsbereich* geht es um die Frage, ob eine konkrete Datenverarbeitungstätigkeit auch *in räumlicher Hinsicht* in den Anwendungsbereich der DSGVO fällt. Gerade im Cloud Computing, wo quasi »mit wenigen Mausklicks« auch zahlreiche Datenverarbeitungsstandorte außerhalb der EU genutzt werden können, kommt es hier immer wieder zu Unklarheiten. Denn die DSGVO knüpft nicht am *Datenverarbeitungsstandort*, sondern vielmehr an der *Niederlassung* eines Verantwortlichen in der EU an. Im Ergebnis ist die DSGVO damit auf die Verarbeitung personenbezogener Daten durch ein deutsches Unternehmen mit festem Unternehmensstandort hierzulande in räumlicher Hinsicht quasi immer anwendbar. Leserinnen und Leser aufseiten von Unternehmen in Deutschland und in der EU können die folgenden Seiten zum räumlichen Anwendungsbereich daher auch überspringen.

Praxistipp: DSGVO ist auf die Datenverarbeitung durch ein deutsches bzw. europäisches Unternehmen quasi immer anwendbar

Die DSGVO ist auf die Verarbeitung personenbezogener Daten durch ein deutsches bzw. europäisches Unternehmen mit festem Unternehmensstandort in Deutschland bzw. in der EU in räumlicher Hinsicht quasi immer anwendbar. Leserinnen und Leser auf Seiten von Unternehmen in Deutschland und in der EU können die folgenden Seiten zum räumlichen Anwendungsbereich daher auch überspringen.

Mit Fragen des räumlichen Anwendungsbereichs haben sich vor allem Unternehmen auseinanderzusetzen, die nicht in der EU sitzen. Da die DSGVO auch ein *Marktortprinzip* verfolgt, kann sie in bestimmten Fällen ebenfalls von in den USA niedergelassenen Unternehmen zu beachten sein, wie wir im Folgenden noch sehen werden.

Die Regelungen zum räumlichen Anwendungsbereich sind in Art. 3 DSGVO wiederzufinden. Es sind drei Anwendungsfälle zu unterscheiden, wobei dem Begriff der *Niederlassung* eine zentrale Bedeutung zukommt:

- *Verarbeitung durch eine Niederlassung in der EU* (das sogenannte Niederlassungsprinzip): Die Verarbeitung erfolgt im Rahmen der Tätigkeit einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der EU, unabhängig davon, ob die Verarbeitung in der EU stattfindet (Art. 3 Abs. 1 DSGVO) – siehe dazu nachfolgend Abschnitt 4.2.1.
- *Verarbeitung durch eine Niederlassung außerhalb der EU* (das sogenannte Marktortprinzip): Die Verarbeitung personenbezogener Daten von betroffenen Personen, die sich in der Union befinden, erfolgt durch einen nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeiter und steht im Zusammenhang mit dem Anbieten von Waren oder Dienstleistungen in der EU oder der Beobachtung des Verhaltens der betroffenen Person (Art. 3 Abs. 2 DSGVO) – siehe dazu nachfolgend Abschnitt 4.2.2.
- Im Cloud Computing weniger relevant ist der Fall, dass personenbezogene Daten in diplomatischen oder konsularischen Vertretungen verarbeitet werden (Art. 3 Abs. 3 DSGVO).

4.2.1 Verarbeitung durch eine Niederlassung in der EU (Niederlassungsprinzip)

Nach dem sogenannten *Niederlassungsprinzip*, das auch schon vor der Datenschutzreform in Art. 4 der EU-Datenschutzrichtlinie sowie in § 1 Abs. 5 S. 1 BDSG a. F. wiederzufinden war, ist die DSGVO anwendbar, wenn ein Verantwortlicher oder ein Auftragsverarbeiter eine Niederlassung in der EU hat und im Zusammenhang mit der durch die Niederlassung ausgeübten Tätigkeit personenbezogene Daten verarbeitet. Entscheidend ist also allein das Vorhandensein einer *Niederlassung* in der EU, unabhängig davon, ob die Daten innerhalb oder außerhalb der EU verarbeitet werden.

Niederlassung Der Begriff der Niederlassung wird in der DSGVO nicht definiert. Erwägungsgrund 22 der DSGVO enthält jedoch Anhaltspunkte für die Anforderungen an eine Niederlassung. Diese setzt hiernach die effektive und tatsächliche Ausübung einer Tätigkeit durch eine feste Einrichtung voraus. Diese Anforderungen entsprechen im Wesentlichen dem Verständnis einer Niederlassung nach der alten EU-Datenschutzrichtlinie und sind daher auch im Rahmen der DSGVO grundsätzlich weit zu verstehen.

Kurz erklärt: Niederlassung

Eine Niederlassung setzt die effektive und tatsächliche Ausübung einer Tätigkeit durch eine feste Einrichtung voraus.

Feste Einrichtung Das Vorliegen einer *festen Einrichtung* ist anhand der tatsächlichen Umstände und Begebenheiten festzumachen. Rein vorübergehend installierte Einrichtungen (wie z. B. Messestände) reichen nicht zur Annahme einer festen Einrichtung aus. Gleiches gilt auch für reine Briefkastenfirmen mit lediglich einem Briefkasten in der EU. Die Rechtsform der Niederlassung oder die Einrichtung als Zweigstelle oder selbstständige Tochtergesellschaft ist ohne Bedeutung. Auch reine Produktionsstätten können deshalb eine Niederlassung darstellen.

Ein deutsches Unternehmen mit einem oder mehreren Unternehmensstandorten in Deutschland ist daher hierzulande niedergelassen. Die DSGVO ist auf das Unternehmen räumlich anwendbar – unabhängig davon, ob die Daten in einer Cloud innerhalb oder außerhalb der EU oder bei dem Unternehmen vor Ort (*on Premise*) verarbeitet werden.

Feste Einrichtung im Kontext von Cloud Computing Doch was ist, wenn ein Unternehmen keine *feste Einrichtung* in der EU hat? Hierzu schauen wir uns einmal zwei typische Konstellationen aus der Cloud-Computing-Praxis an, die einen Cloud-Anbieter betreffen:

- *1. Fall* (Eigenbetrieb von Rechenzentrum, Servern und Personal in der EU): Ein Cloud-Anbieter mit Sitz in den USA betreibt die seiner Cloud-Infrastruktur zugrunde liegenden Server in einem eigenen Rechenzentrum in der EU. Die Sicherheitsumgebung (Gebäude und Gelände) betreibt er selbst. Hierfür werden vor Ort unter anderem technisches Personal und weiteres Sicherheitspersonal »24/7« eingesetzt.
- *2. Fall* (Colocation in der EU): Ein Cloud-Anbieter mit Sitz in den USA betreibt die seinen Cloud-Infrastrukturen zugrunde liegenden Server in einem Rechenzentrum in der EU. Im Unterschied zum 1. Fall wird die Sicherheitsumgebung (Gebäude und Gelände) jedoch nicht von ihm selbst, sondern von einem spezialisierten Rechenzentrumsbetreiber bereitgestellt, in die er sich »einmietet«. Für den Betrieb seiner Server werden ihm auf den Rechenzentrumsflächen (den *Data Floors*) verschiedene Racks (gegebenenfalls in einem besonders gesicherten Bereich, dem *Cage*, oder verteilt auf mehrere Brandschutzabschnitte) vom Betreiber des Rechenzentrums zur Verfügung gestellt (sogenannte *Colocation*). Technisches Personal (insbesondere First- und Second-Level-Support) und weiteres Sicherheitspersonal sind im Leistungspaket enthalten. Der Cloud-Anbieter hat kein eigenes Personal oder sonstige Vertreter vor Ort, sondern wartet die Server und IT-Systeme remote durch eigene Techniker aus den USA.

Im 1. Fall ist von einer Niederlassung in der EU auszugehen. Eine feste Einrichtung wird durch die Errichtung bzw. durch den Betrieb eines eigenen Rechenzentrums in der EU (Gebäude und Gelände als Sicherheitsumgebung) begründet. Aufgrund des vor Ort vorhandenen Personals ist zudem von einer effektiven und tatsächlichen Ausübung einer Tätigkeit im Rahmen der Niederlassung auszugehen.

Unter einer effektiven und tatsächlich ausgeübten Tätigkeit sind jedoch nur menschliche Aktivitäten zu verstehen. Rein *technische Stützpunkte*, wie beim rein technischen Betrieb von Servern und IT-Systemen in Fall 2, begründen daher grundsätzlich keine Niederlassung in der EU.

Allerdings ist zu beachten, dass der EuGH eine flexible Konzeption des Niederlassungsbegriffs vertritt. In bestimmten Konstellationen kann daher auch bei einem rein technischen Stützpunkt eine Niederlassung anzunehmen sein, etwa wenn der Verantwortliche in dem EU-Mitgliedstaat einen Vertreter bestellt

hat oder wenn die Wartung im 2. Fall (*Colocation*) nicht vollständig remote, sondern ganz oder teilweise auch durch eigenes technisches Personal vor Ort erfolgt und hierfür beispielsweise in dem Rechenzentrumsgebäude ein Büro oder eine sonstige betriebliche Basis eingerichtet wird. Insofern wird das Vorliegen einer Niederlassung immer auch von den besonderen Charakteristika des jeweiligen Einzelfalls abhängen. Darüber hinaus sind noch nicht alle Konstellationen endgültig geklärt, sodass aktuelle Entwicklungen zu beachten sind, insbesondere Stellungnahmen vonseiten der Aufsichtsbehörden für den Datenschutz.

Hinweis: Rein technische Stützpunkte in der EU begründen im Regelfall keine Niederlassung

Rein technische Stützpunkte in der EU, wie sie dem Betrieb von Servern oder sonstigen IT-Systemen im Rahmen von Colocation sowie der gerade im Cloud Computing äußerst praxisrelevanten Nutzung von IT-Infrastruktur im Wege des IaaS oder Hostings zugrunde liegen, begründen im Regelfall keine Niederlassung.

Auftragsverarbeiter in der EU Das Einschalten eines Auftragsverarbeiters in der EU – wie zum Beispiel die Nutzung der Infrastruktur eines Cloud-Anbieters mit Rechenzentrum in der EU durch einen Cloud-Nutzer in Kanada – begründet im Regelfall keine Niederlassung in der EU. Verarbeitet ein Unternehmen außerhalb der EU daher personenbezogene Daten durch einen Auftragsverarbeiter in der EU, ist der Auftragsverarbeiter nicht als Niederlassung des Verantwortlichen in der EU anzusehen. Gerade in Bezug auf Auftragsverarbeiter und weitere Unterauftragsverarbeiter sind aber ebenfalls noch nicht alle Konstellationen endgültig geklärt, sodass auch hier aktuelle Entwicklungen im Blick zu behalten sind.

Hinweis: Auftragsverarbeiter in der EU ist keine Niederlassung

Verarbeitet ein Unternehmen außerhalb der EU personenbezogene Daten durch einen Auftragsverarbeiter in der EU, ist der Auftragsverarbeiter grundsätzlich nicht als Niederlassung des Verantwortlichen in der EU anzusehen.

Datenverarbeitung »im Rahmen der Tätigkeiten« der Niederlassung Bei großen internationalen Konzernen mit Hauptsitz in den USA und mehreren Niederlassungen in der EU stellt sich die weitere Frage, ob die Datenverarbeitung *im Rahmen der Tätigkeit* der Niederlassung erfolgt und damit ein Zusammenhang zwischen der Datenverarbeitung und der in der Niederlassung ausgeübten Tätigkeit besteht. Seit dem *Google-Spain-Urteil* des EuGH (Urt. v. 13. Mai 2014 – C-131/12) ist auch hier ein weiterer Maßstab anzulegen. Bereits Werbe- und Marketingaktivitäten können zur Bejahung eines solchen Zusammenhangs ausreichen. Im konkreten Fall hatte die Niederlassung von Google die Aufgabe, den Verkauf von Werbeflächen in der Suchmaschine zu fördern und hierzu Werbe- und Marketingaktivitäten in Spanien ausgeführt, um die Rentabilität der Suchmaschine zu steigern. Der EuGH zog zur Bejahung einer datenverarbeitenden Niederlassung in modernen Datenverarbeitungsszenarien damit auch das konzernweite Geschäftsmodell von Google als Suchmaschinenanbieter heran. Er weitete also schon im Jahr 2014 den räumlichen Anwendungsbereich des Datenschutzrechts aus, selbst wenn die eigentliche Datenverarbeitung nicht in der EU stattfand. Der EuGH hat damit dem heute in Art. 3 Abs. 2 DSGVO enthaltenen *Marktortprinzip* vorgegriffen.

Hinweis: Datenverarbeitungen »im Rahmen der Tätigkeit« einer Niederlassung auch bei Werbe- und Marketingaktivitäten (Google-Spain-Urteil des EuGH)

Datenverarbeitungen im Rahmen der Tätigkeit einer Niederlassung liegen nach dem *Google-Spain-Urteil* des EuGH auch dann vor, wenn die Datenverarbeitung zwar nicht in der EU stattfindet, die Niederlassung in der EU jedoch die Aufgabe hat, Werbe- und Marketingaktivitäten der Suchmaschine zu fördern.

4.2.2 Verarbeitung durch eine Niederlassung außerhalb der EU (Marktortprinzip)

Der räumliche Anwendungsbereich der DSGVO wird durch Art. 3 Abs. 2 DSGVO auch auf außerhalb der EU niedergelassene Verantwortliche und Auftragsverarbeiter ausgedehnt, die keine Niederlassung in der EU haben. Die DSGVO erfasst damit vor allem das sogenannte *Targeting* von Personen in der EU durch außerhalb der EU niedergelassene Anbieter, sofern die Datenverarbeitung im Zusammenhang steht mit:

- dem *Angebot von Waren oder Dienstleistungen* an betroffene Personen in der EU (Art. 3 Abs. 2 lit. a DSGVO) oder
- der *Beobachtung des Verhaltens* von betroffenen Personen in der EU (Art. 3 Abs. 2 lit. b DSGVO).

Es reicht aus, dass sich die betroffene Person in der EU befindet. Es kommt also auf den tatsächlichen, physischen Aufenthaltsort in der EU an. Der registrierte Wohnsitz oder Lebensmittelpunkt ist ohne Bedeutung. Der Schutz ist auch nicht an die Staatsangehörigkeit der betroffenen Person geknüpft. Es sind alle Personen geschützt, die sich – ungeachtet ihres gewöhnlichen Wohnsitzes oder Lebensmittelpunkts – in der EU befinden.

Angebot von Waren oder Dienstleistungen in der EU Sehen wir uns zunächst die erste Alternative des *Angebots von Waren oder Dienstleistungen* an betroffene Personen in der EU an. In der DSGVO ist hierzu keine weitergehende Präzisierung zu finden. Ein *Angebot* ist aber nicht rein zivilrechtlich, sondern weit zu verstehen. Auch Aufforderungen zur Abgabe eines Angebots (*invitatio ad offerendum*) oder mittelbare Zwecke für die Angebotsabgabe können erfasst sein. Zudem ist es unerheblich, ob tatsächlich ein Vertragsschluss stattfindet.

Des Weiteren muss der Verantwortliche oder Auftragsverarbeiter es *offensichtlich beabsichtigen*, das Angebot an Personen in der EU auszurichten (vgl. Erwägungsgrund 23 DSGVO). Hierfür reicht es nicht aus, dass eine Webseite lediglich allgemein über das Internet zugänglich ist. Auch die Verwendung einer allgemein gebräuchlichen Sprache im Drittland ist meist kein ausreichender Anhaltspunkt (gerade bei der in vielen Ländern und im weltweiten Geschäftsleben gebräuchlichen englischen Sprache). Erforderlich ist vielmehr eine deutlich erkennbare Ausrichtung auf die EU. Diese ist etwa gegeben, wenn eine Sprache verwendet wird, die in einem oder in mehreren EU-Mitgliedstaaten gebräuchlich ist, in Verbindung mit der Möglichkeit, Waren und Dienstleistungen in dieser Sprache zu bestellen. Auch die Erwähnung von Kunden oder Nutzern in der EU (etwa Verweise auf europäische Referenzkunden) kann ein Indiz für ein Anbieten von Waren oder Dienstleistungen in der EU sein. Es können aber auch

weitere Kriterien für eine Ausrichtung an Personen in der EU herangezogen werden, etwa die Verwendung länderspezifischer *Country-Code-Top-Level-Domains* (ccTLD), wie ».de« für Deutschland, ».at« für Österreich oder ».fr« für Frankreich. Weitere Indizien können auf E-Commerce-Plattformen enthaltene Angaben zu Versandmöglichkeiten von Waren in die EU sein, Preisauszeichnungen in Euro oder in einer anderen Währung eines EU-Mitgliedstaats oder Werbeaktivitäten in der EU.

Besonderheiten im Cloud Computing – IaaS-Ebene Im Cloud Computing können auch Cloud-typische Leistungsmerkmale auf IaaS-, PaaS- oder SaaS-Ebene für eine Leistungsausrichtung an Personen in der EU herangezogen werden. Auf *IaaS-Ebene* können etwa EU-spezifische Beschreibungen eines Cloud-Anbieters zu dem (Hoch-)Verfügbarkeitskonzept – wie in Bezug auf Regionen und Verfügbarkeitszonen oder die Trassierung von Datenleitungen zur Anbindung der Rechenzentren an die Backbones und Netzwerke von Telekommunikationsnetzbetreibern (auch *Carrier* genannt) – von Bedeutung sein, wenn beispielsweise niedrige Latenzen bei den Paketlaufzeiten aus und nach Europa als besonderes Merkmal herausgestellt werden.

Auch technische Beschreibungen von Public- oder Private-Cloud-Infrastrukturen, die auf die Einhaltung von Compliance-Anforderungen in einem oder in mehreren EU-Mitgliedstaaten ausgerichtet sind, können auf eine EU-Ausrichtung hindeuten (z. B. Private Cloud mit Verweis auf europäische Datenschutz- und Datensicherheitsanforderungen). Dies gilt insbesondere auch für die Bewerbung europäischer Zertifizierungen, Gütesiegel, Prüfstandards sowie technischer Standards und Normen aus Gesichtspunkten einer Interoperabilität.

Verweise auf direkte Leitungsverbindungen zu europäischen Netzknoten und Peering-Points (wie DE-CIX in Frankfurt oder AMS-IX in Amsterdam) können ebenfalls ein Indiz für eine EU-Ausrichtung sein. Allerdings sind bei den großen Netzknoten nicht nur nationale Carrier aus der EU angeschlossen, die kurze Übertragungswege zu Personen in der EU ermöglichen, sondern auch viele außereuropäische Carrier, die zu Peering-Zwecken Daten miteinander austauschen. Insofern wird immer eine konkrete Einzelfallbetrachtung erforderlich sein.

Wird ein Cloud-Service eines außereuropäischen Anbieters dahin gehend beworben, dass durch niedrige Strompreise in dem Drittland der Betrieb von IT-Systemen günstiger und vorteilhafter ist gegenüber dem Strommarkt in der EU (in Deutschland insbesondere mit Blick auf Strompreisanpassungen durch die EEG-Umlage oder durch die massiven Strompreiserhöhungen infolge des Kriegs

in der Ukraine, die gerade im Rechenzentrumsumfeld ein zentrales Thema sind), wird auch hier von einer EU-Ausrichtung auszugehen sein.

SaaS-Ebene Auf *SaaS-Ebene* wird eine Leistungsausrichtung an Personen in der EU etwa bei Software mit eindeutigem Bezug zur EU und spezifischen Add-ins, Schnittstellen oder Spracheinstellungsoptionen (z. B. Fachanwendungen für die Buchführung oder Lohn- und Gehaltsabrechnung nach den gesetzlichen Vorgaben eines EU-Mitgliedstaats) anzunehmen sein.

Waren und Dienstleistungen Den Begriffen *Waren* und *Dienstleistungen* liegt ganz im Sinne einer europarechtlichen Auslegung ebenfalls ein weites Begriffsverständnis zugrunde. Als *Waren* sind alle beweglichen körperlichen Gegenstände zu verstehen. Im Cloud Computing ist aber vor allem der Begriff der *Dienstleistung* von Bedeutung. Zahlreiche Cloud-Services, Social-Media-Dienste und Streaming-Plattformen sind als Dienstleistung zu verstehen. Die DSGVO ist daher anzuwenden, wenn die Leistung von natürlichen Personen in der EU als jeweils betroffene Person genutzt wird. Wird die Leistung dagegen von einem Unternehmen und mithin von einer juristischen Person genutzt, ist die DSGVO nicht nach Art. 3 Abs. 2 DSGVO anwendbar, da die Datenverarbeitung nicht im Zusammenhang mit dem Angebot von Waren oder Dienstleistungen an eine betroffene Person steht. In diesem Fall kann ein außereuropäischer Anbieter aber durch entsprechende vertragliche Verpflichtungen an die DSGVO und die darin enthaltenen europäischen Datenschutzgrundsätze gebunden werden.

Hinweis: Cloud Computing als Dienstleistung im Sinne von Art. 3 Abs. 2 DSGVO

Zahlreiche Cloud-Services, Social-Media-Dienste und Streaming-Plattformen außereuropäischer Anbieter sind als *Dienstleistung* an eine natürliche Person als betroffene Person in der EU zu verstehen, auf die die DSGVO Anwendung findet.

Aus Sicht eines außereuropäischen Unternehmens, dessen Verarbeitungstätigkeiten an der DSGVO zu messen sind, kann es sich als problematisch erweisen, wenn Anforderungen der DSGVO im Widerspruch zum nationalen Recht seines Heimatstaats oder anderer Rechtsordnungen stehen (gerade bei US-amerikanischen Hyperscalern wie AWS, Google und Microsoft gibt es möglicherweise Konflikte mit US-Recht). Im Cloud Computing war der Konflikt zwischen den unterschiedlichen Verpflichtungen aus nationalen

Rechtsordnungen schon im Jahr 2011 Gegenstand einer lebhaften Debatte, als Microsoft bei einer Vorstellung von Office 365 die Frage gestellt wurde, ob man garantieren könne, dass in Rechenzentren in der EU gespeicherte Daten die EU unter keinen Umständen verlassen. In diesem Kontext stehen vor allem Verpflichtungen nach *CLOUD Act*, dem *US Patriot Act* und dem *Foreign Intelligence Surveillance Act* (FISA) im Fokus der Debatte, zuletzt insbesondere nach dem Schrems-II-Urteil des EuGH aus dem Juli 2020 (ausführlich zu diesen Themen und dem Verfahren »Microsoft Corp. v. United States« siehe Kapitel 13).

Praxishinweis: Konflikt mit nationalem Recht anderer Staaten

Aus Sicht eines außereuropäischen Unternehmens kann es sich in der Praxis in einigen Konstellationen als problematisch erweisen, dass die Anforderungen der DSGVO im Widerspruch zum Recht einer anderen Rechtsordnung stehen (wie dem nationalen Recht seines Heimatstaats).

Beobachtung des Verhaltens Nach der zweiten Alternative erstreckt sich die räumliche Anwendbarkeit auch auf die Beobachtung des Verhaltens von betroffenen Personen in der EU (Art. 3 Abs. 2 lit. b, Erwägungsgrund 24 DSGVO). Eine derartige Verhaltensbeobachtung liegt vor, wenn durch Datenverarbeitungstechniken die Internetaktivitäten einer Person derart nachvollzogen werden können, dass für diese Person ein Profil mit ihren persönlichen Vorlieben, Verhaltensweisen und Gepflogenheiten erstellt werden kann, mit dessen Hilfe zukünftige Verhaltensweisen dieser Person vorausgesagt werden können. Die Regelung zielt ausdrücklich auf Internetsachverhalte ab. Eine solche Verhaltensbeobachtung wird daher insbesondere bei einem Tracking im Internet durch Analysetools, Cookies, Social-Media-Plug-ins und anderen Formen der systematischen Auswertung von Onlineaktivitäten gegeben sein, hierbei insbesondere auch mit Blick auf die Bedienung von Administrations- und Verwaltungsportalen von Cloud-Anbietern.

Kurz erklärt: Räumlicher Anwendungsbereich

Im Rahmen des *räumlichen Anwendungsbereichs* stellt sich die Frage, ob eine konkrete Datenverarbeitungstätigkeit in räumlicher Hinsicht den Anwendungsvoraussetzungen der DSGVO unterfällt. Dies ist insbesondere der Fall, wenn:

- die Verarbeitung im Rahmen der Tätigkeit einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der EU erfolgt (*Niederlassungsprinzip*),
- die Verarbeitung durch eine Niederlassung außerhalb der EU im Zusammenhang mit dem Angebot von *Waren oder Dienstleistungen* an betroffene Personen in der EU oder im Zusammenhang mit ihrer Verhaltensbeobachtung (*Marktortprinzip*) erfolgt.

4.3 Andere Rechtsgebiete

Fragen in Bezug auf das *anwendbare Recht* stellen sich aber nicht nur im Zusammenhang mit der DSGVO. Sie sind im Cloud Computing grundsätzlich mit sämtlichen Rechtsordnungen und Rechtsgebieten verbunden, die durch die grenzüberschreitende Nutzung eines Cloud-Service berührt werden. Denn während Cloud-Infrastrukturen in technischer Hinsicht von globaler Dimension sein können und an Landesgrenzen nicht haltmachen, sind Rechtsfragen stets auf territorial begrenzte Rechtsräume zurückzuführen. Nutzt ein deutsches Unternehmen daher Cloud-Services eines ausländischen Anbieters, wirft diese Nutzung nicht nur datenschutzrechtliche Fragen auf. Auch andere Rechtsgebiete können hiervon betroffen sein. So können in zivilrechtlicher Hinsicht etwa die allgemeinen Kollisionsregelungen des internationalen Privatrechts anzuwenden sein, um das auf vertragliche Schuldverhältnisse anzuwendende Recht (*Rom I-VO*) oder das Deliktsstatut (*Rom II-VO*) zu bestimmen.

4.4 FAQs

Mein Unternehmen sitzt in Deutschland und möchte eine Cloud mit Datenverarbeitungsstandorten in der EU nutzen. Ist die DSGVO anwendbar?

Dieses Cloud-Nutzungsszenario ist bei vielen deutschen Unternehmen quasi der Standard. Die DSGVO ist anwendbar, da die Verarbeitungen im Rahmen der Tätigkeit einer *Niederlassung* des Verantwortlichen mit Sitz in Deutschland erfolgt.

Mein Unternehmen sitzt in Deutschland. Kann es die DSGVO »umgehen«, indem nur noch Server in Drittländern (z.B. in den AWS-Regionen Ohio/USA und Singapur) genutzt werden?

Nein, nach dem Niederlassungsprinzip ist allein das Vorhandensein einer *Niederlassung* in der EU entscheidend. Die DSGVO ist demnach auf alle in einem Mitgliedstaat der EU niedergelassene Unternehmen räumlich anwendbar, unabhängig davon, ob die Daten innerhalb oder außerhalb der EU oder beim Unternehmen vor Ort (*on Premise*) verarbeitet werden.

Mein Unternehmen sitzt in Deutschland und plant ein Multi-Cloud-Szenario mit US-amerikanischen Hyperscalern (u.a. AWS-Dienste, Microsoft 365) und europäischen Cloud-Anbietern. Die personenbezogenen Daten sollen sowohl an Standorten in den USA als auch in Europa verarbeitet werden, aufgrund besonderer Geschäftsbeziehungen mit Asien darüber hinaus auch in der AWS-Region Asien-Pazifik (Singapur). Ist die DSGVO anwendbar, bzw. sind daneben auch andere Datenschutzgesetze zu berücksichtigen?

Die DSGVO ist auch hier anwendbar, da die Verarbeitungen im Rahmen der Tätigkeit einer *Niederlassung* eines Verantwortlichen mit Sitz in Deutschland erfolgt. Daneben können aber auch Vorschriften des US-amerikanischen Rechts und des Rechts in Singapur zu berücksichtigen sein, soweit Daten an den dortigen Standorten verarbeitet werden (zu internationalen Datentransfers und einem sogenannten TIA bzw. zu einem Datenzugriff nach US-Recht mehr in den Kapiteln Kapitel 12 und Kapitel 13).

Mein Unternehmen sitzt in den USA und hat keine Niederlassung in der EU. Die Datenverarbeitung erfolgt in den USA. Jedoch bietet es auch Personen in der EU entgeltlich Cloud-Services an. Ist die DSGVO anwendbar?

Es liegt ein Fall des Angebots von Dienstleistungen an EU-Bürger (Art. 3 Abs. 2 lit. a DSGVO, *Marktortprinzip*) vor. Auf hiermit im Zusammenhang stehende Datenverarbeitungen ist die DSGVO anzuwenden.

4.5 Checkliste zum Anwendungsbereich der DSGVO

Sachlicher Anwendungsbereich:

- ☑ Handelt es sich um *personenbezogene Daten?*
- ☑ Liegt eine *Verarbeitung* vor?
- ☑ Ist keine *Ausnahme* einschlägig (etwa die sogenannte Haushaltsausnahme)?

Räumlicher Anwendungsbereich:

- ☑ Erfolgt die Verarbeitung im Rahmen der Tätigkeit einer *Niederlassung* eines Verantwortlichen oder eines Auftragsverarbeiters in der EU? Auf Unternehmen in Deutschland und der EU ist die DSGVO in aller Regel bereits hiernach anwendbar.
- ☑ Werden *Waren oder Dienstleistungen* in Deutschland oder in der EU angeboten?
- ☑ Liegt eine *Beobachtung des Verhaltens* von betroffenen Personen in Deutschland oder in der EU vor?