Thorsten Hennrich: Cloud Computing nach der Datenschutz-Grundverordnung

Zusammenfassung

Patrick Bucher

24.08.2023

Inhaltsverzeichnis

1 Einleitung

Die drei führenden Hyperscaler – Amazon Web Services (AWS), Microsoft Azure und Google Cloud – sind in den USA beheimatet. Die Verarbeitung von Daten in der Cloud geschieht oft länderübergreifend. Datenschutz ist jedoch oftmals national geregelt. Auch kann eine Datenverarbeitung mehrere Hersteller betreffen, mit denen man unterschiedliche vertragliche Regelungen getroffen hat.

Die DSGVO wurde am 25. Mai 2018 eingeführt und sieht hohe Bussgelder bei Verstössen gegen den Datenschutz vor.

2 Cloud Computing: Einführung, Basics und wichtigste Begriffe

Cloud Computing ist im Grunde eine Auslagerung von Tätigkeiten mit IT-Bezug zu einem externen Dienstleister; eine flexible und nutzungsorientierte Form von IT-Outsourcing. "Cloud" wird oftmals als Synonym für Online-Datenspeicher oder Internet verwendet. (Siehe auch "NIST Definition of Cloud Computing" für eine genauere Definition.) Das BSI versteht unter "Cloud Computing" ein dynamisch an den Bedarf angepasstes Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen.

Zur Bereitstellung von IT-Ressourcen als Cloud benötigt es breitbandige Datennetzte mit tiefer Latenz (zwischen den Datenzentren, aber auch zu den Endverbrauchern, z.B. via Glasfaser), leistungsfähige Standardhardware (die zu homogenen Pools zusammengeschlossen werden kann), vielfältige Zugangsgeräte (PCs, Notebooks, Smartphones, IoT-Geräte) und Thin Clients, die mittels Browser bedienbar sind.

Cloud Computing kann verstanden werden als Weiterentwicklung und Kombination von Basistechnologieen wie dem Grid Computing (z.B. SETI@home), von Application Service Providers (ASPs), die eine Anwendung zentral auf Servern zur Verfügung stellen, der serviceorientierten Architektur (SOA), wobei Anwendungen durch standardisierte Schnittstellen angeboten werden und der Virtualisierung, welche die Hardware abstrahiert, in Pools zusammenfasst und dadurch flexibel anbieten und optimal ausnutzen kann. Anwendungen können werden mitsamt benötigten Programmbibliotheken in unveränderlichen Containern gebündelt und können so unabhängig von einer bestimmten Umgebung ausgeführt werden. Container werden oftmals mit Docker gebaut und mit Kubernetes orchestriert.

Cloud-Angebote können in drei Schichten eingeteilt werden:

- Infrastructure as a Service (IaaS): Die Infrastruktur wird gemietet statt angeschafft, wodurch Investitionskosten (etwa für Server) wegfallen bzw. in laufende Kosten umgewandelt werden. Durch die Auslagerung der IT-Infrastruktur ergeben sich Risiken im Datenschutz und in der Anbieterabhängigkeit. Beispiel: virtuelle Maschinen.

- Platform as a Service (PaaS): Laufzeit- und Entwicklungsplattformen (mitsamt zugrundeliegender Hardware) werden gemietet statt selber entwickelt. Diese Ebene richtet sich v.a. an Kunden, die ihre eigene Software entwickeln und betreiben wollen. Der PaaS-Markt ist kleiner als der IaaS- und der SaaS-Markt, weswegen sich die Risiken eines Vendor Lock-Ins erhöhen. Beispiel: Google App Engine.
- Software as a Service (SaaS): Software wird nicht angeschafft und selber betrieben, sondern von einem Anbieter (meist in einem Abo-Modell) meist als Web-Anwendung bezogen. Die Kosten für den eigenen Betrieb fallen weg, dafür steigt die Abhängigkeit von einem bestimmten Anbieter. Beispiele: Microsoft 365, Salesforce.

Cloud-Angebote werden in verschiedenen Formen bereitgestellt:

- Public Cloud: Diese Angebote sind für jedermann, d.h. öffentlich auf gemeinsam genutzter Hardware verfügbar. Die gemeinsame Verarbeitung von Daten verschiedener Nutzer ist für diese transparent. Anbieter mit sehr umfangreichen Ressourcen, die massiv skalieren können, werden als *Hyperscaler* bezeichnet.
- Private Cloud: Eine Cloud-Umgebung wird von einer Organisation zur eigenen Verwendung oder zur Verwendung eines eingeschränkten Nutzerkreises aufgebaut. Die Skalierbarkeit ist zumeist geringer als bei einer Public Cloud, dafür können Risiken im Datenschutz und in der Datensicherheit besser kontrolliert werden. Es gibt Anbieter, die ihre vermeintliche Private Cloud selber auf einer Public Cloud hosten.
- Hybrid Cloud: Hierbei werden Public Cloud und Private Cloud (und, optional, Legacy-Hardware) zu einer hybriden Cloud kombiniert. Daten können gemäss ihrem Schutzbedarf verarbeitet werden. Diese Mischform erschwert jedoch den Betrieb.
- Multi Cloud: Angebote verschiedener Anbieter werden zusammengeschlossen und können über eine einheitliche Managementoberfläche oder Orchestrierungswerkzeuge einheitlich genutzt werden. Hierdurch reduziert sich die Abhängigkeit von einzelnen Anbietern. Im Gegenzug erhöht sich die Komplexität, und den unterschiedlichen Standorten der Anbieter muss Rechnung getragen werden (bezogen auf Datenschutz und Datensicherheit).
- Community Cloud: Mehrere Organisationen mit vergleichbaren Anforderungen (regulatorisch, technisch) betreiben eine gemeinsame Cloud-Infrastruktur für ihren eigenen Bedarf.

Die wichtigsten Cloud-Anbieter sind:

- Amazon Web Services (AWS): Der weltweit grösste Cloud-Anbieter wurde 2006 gegründet und bietet Hosting von Kleinkunden bis zu Grosskonzernen an, wobei Netflix einer der prominentesten Kunden ist. Wichtige Services sind die *Elastic Compute Cloud* (EC2, virtuelle Server) und der *Simple Storage Service* (S3, Datenspeicher). Die Infrastruktur ist unterteilt in Regionen und Availability Zones. Eine Region ist der Standort eines Rechenzentrumsclusters in einem bestimmten Land oder geografischen Gebiet. Pro Region gibt es mindestens eine Availability Zone bestehend aus einem oder mehreren Rechenzentren. Availability Zones sind voneinander isoliert und physisch getrennt, d.h. Ausfälle einer Zone können andere Zonen nicht beeinflussen. Die Datenverarbeitung kann auf bestimmte

Regionen eingeschränkt werden. Mit *AWS Outposts* kann On-Premise-Hardware in AWS eingebracht werden.
- Google Cloud Platform (GCP): Der Suchmaschinenanbieter Google rief seine Cloud im Jahr 2008 ins Leben und stellte die PaaS-Plattform *App Engine* zur Verfügung. Seit 2013 verfügt die GCP mit der *Compute Engine* über ein IaaS-Anegbot. Google unterschweidet (wie bei AWS) zwischen Regionen und (voneinander isolierten) Zonen. Nicht alle Angebote stehen in jeder Region zur Verfügung.
- Microsoft Azure: Der derzeit zweitgrösste Cloud-Anbieter wurde 2010 gegründet und verfügt über ein vergleichbares Angebot wie AWS und Google, wobei Microsoft 365 eines der wichtigsten SaaS-Angebote ist. Die Infrastruktur ist in Regionen und Verfügbarkeitszonen gegliedert. Mithilfe sogenannter *Azure-Geografien* können Daten und Dienste unter Wahrung von Compliance-Anforderungen innerhalb einer geografischen Region verschoben werden. Bei Microsoft 365 hängt das Land der Datenspeicherung hängt von der Rechnungsadresse des Kunden ab.

3 Datenschutz nach der DSGVO: Einführung und wichtigste Basics für die Cloud-Computing-Praxis

Datenschutz bewahrt die Freiheit natürlicher Personen, selbst über den Umgang ihrer personenbezogenen Daten zu entscheiden und schützt das Recht auf informationelle Selbstbestimmung. Die DSGVO ist das Ergebnis einer Datenschutzreform, welche die Regeln EU-weit vereinheitlicht. Sie ist eine Verordnung und nicht nur eine blosse Richtlinie und damit direkt in den EU-Mitgliedsstaaten gültig. In den jeweiligen Ländern wird sie durch Anpassungs- und Umsetzungsvorschriften ergänzt. Ziel der DSGVO war es auch, Europa “cloud-friendly” und “cloud-active” zu machen, wobei Hindernisse im grenzüberschreitenden Cloud Computing beseitigt worden sind. Die DSGVO ist technologieneutral formuliert und schafft einen europaweiten einheitlichen Rahmen für Datenschutz. Den wirtschaftlichen Vorteilen des Cloud Computings stehen Sicherheits- und Datenschutzbedenken bei potentiellen Kunden gegenüber. Wichtige Fragestellungen hierbei sind u.a.:

1. Wann lieft eine Verarbeitung personenbezogener Daten vor?
2. Was ist bei der Auswahl eines Cloud-Anbieters zu berücksichtigen?
3. Wo befinden sich die Daten, und wie sicher ist die Cloud-Infrastruktur?
4. Wann und wie muss ein Auftragsverarbeitungsvertrag (AV-Vertrag) abgeschlossen werden?
5. Wie ist die Datenübertragung in andere Länder geregelt?

Personenbezogene Daten sind geschützt; deren Verarbeitung unterliegt einem Verbot mit Erlaubnisvorbehalt. (Was nicht explizit erlaubt worden ist, ist verboten.) Wird eine Datenverarbeitung erlaubt, bezeichnet man dies als *Erlaubnistatbestand.* Als personenbezogene Daten versteht man u.a. Informationen, die sich auf eine Person beziehen, und mithilfe derer eine Person identifiziert werden kann (Name, Adresse, Geburtsdatum, E-Mail-Adresse, IP-Adresse

usw.). Eine Person, deren Daten verarbeitet werden, wird als *betroffene Person* bezeichnet. Unter einer Datenverarbeitung versteht man den ganzen Zyklus von Erhebung über Speicherung, Übermittlung, Nutzung bis zur Löschung der Daten. Die Datenverarbeitung ist rechtmässig, wenn ein Erlaubnisvorbehalt vorliegt und sie im Einklang mit gesetzlichen Vorgaben (DSGVO, weitere) erfolgt.

Die wichtigsten Akteure im Datenschutz sind:

- Die betroffene Person (*Data Subject*) ist eine natürliche Person, welche über schützenswerte personenbezogene Daten zur Datenverarbeitung verfügt.
- Der Verantwortliche (*Controller*) ist eine natürliche oder juristische Person, welche mit anderen über Zweck und Mittel einer Datenverarbeitung entscheidet; d.h. im Cloud Computing ist es der Nutzer eines Angebots. Im Rahmen der DSGVO ist jedes Unternehmen als Verantwortlicher anzusehen.
- Der gemeinsam Verantwortliche (*Joint Controller*) ist jemand, der die Zwecke und Mittel zur personenbezogenen Datenverarbeitung mit einem anderen Verantwortlichen zusammen festlegt. So können Kundendaten von mehreren Unternehmen gemeinsam genutzt werden, wobei die jeweiligen Aufgaben und Verpflichtungen in einer transparenten Vereinbarung festzulegen sind.
- Der Auftragsverarbeiter (*Processor*) ist ein Dienstleister, der personenbezogene Daten im Auftrag eines Verantwortlichen im Rahmen eines Auftragverhältnis übernimmt. Er muss die vom Verantwortlichen festgelegten Zwecke und Mittel einhalten, wozu diese Pflichten im Rahmen eines AV-Vertrags an den Dienstleister weitergegeben werden.
- Der Unterauftragsverarbeiter (*Sub-Processor*) ist ein Dienstleister, der für andere Auftragsverarbeiter arbeitet, und für den wiederum die gleichen Pflichten gelten, und diese auch an andere Auftragsverarbeiter weitergeben kann.
- Der Dritte (*Third Party*) ist ein Aussenstehender, der nicht wie eine der oben erwähnten Akteure in eine personenbezogene Datenverarbeitung eingebunden ist.
- Der Empfänger (*Recipient*) ist jeder, dem personenbezogene Daten offengelegt werden, unabhängig davon, ob er eine dritte Person ist oder nicht.
- Der Datenschutzbeauftragte (*Data Protection Officer*) kümmert sich als Ansprechpartner und Anlaufstelle um die Einhaltung von Datenschutzvorschriften in einem Unternehmen und ist dabei weisungsfrei. Er sollte bei entsprechenden Fragen eingebunden werden.
- Die Aufsichtsbehörde (*Supervisory Authority*) ist eine unabhängige staatliche Stelle, welche für die Einhaltung und Durchsetzung der DSGVO verantwortlich ist.

Die DSGVO unterscheidet zwischen folgenden Ländern:

- EU-Mitglieds- und EWR-Vertragsstaaten (Island, Norwegen, Liechtenstein), die direkt an die DSGVO gebunden sind.
- Drittstaaten, die nicht an die DSGVO gebunden sind, und deren Datenschutzniveau von der EU-Kommission eingeschätzt wird:
  - Sichere Drittländer, die über ein mit der DSGVO vergleichbares Datenschutzniveau verfügen (z.B. die Schweiz und das Vereinigte Königreich).

– Unsichere Drittländer, deren Datenschutzniveau unter demjenigen der DSGVO liegen.

Man unterscheidet zwischen einer Datenübermittlung *1. Stufe* innerhalb der direkt an die DSGVO gebundenen Länder und einer Datenübermittlung *2. Stufe* bei einer Datenübermittlung mit Drittstaaten.

4 Wann ist die DSGVO im Cloud Computing überhaupt anzuwenden?

Bei der DSGVO stellt sich die Frage, ob diese auf einen bestimmten Fall überhaupt anwendbar ist. In sachlicher Sicht muss hierzu eine Verarbeitung personenbezogener Daten mit Speicherung vorliegen, für die keine Ausnahme gilt.

Personenbezogene Daten sind alle Informationen, mit der eine Person direkt identifiziert (z.B. Name, Adresse) oder identifizierbar (z.B. Kundennummer, Benutzername, IP-Adresse) ist. Hierbei stellt sich die Frage, inwiefern das Wissen Dritter zur Identifikation notwendig ist (z.B. Auskunft durch eine Behörde). Für reine Sachdaten (z.B. mathematische Formeln) oder Daten juristischer Personen sowie Daten verstorbener natürlicher Personen findet die DSGVO keine Anwendung.

Pseudonymisierte Daten sind weiterhin personenbezogene Daten, wenn die Informationen zur Identifikation der natürlichen Person weiterhin vorhanden sind, wenn auch getrennt aufbewahrt werden. Auf anonymisierte Daten, aufgrund derer nicht mehr auf eine natürliche Person geschlossen werden kann, findet die DSGVO hingegen keine Anwendung.

Eine Verarbeitung kann manuell oder (teilweise) automatisch erfolgen und betrifft alle Vorgänge, die sich auf personenbezogene Daten beziehen. Erfolgt eine Verarbeitung rein zu persönlichen oder familiären Zwecken, gilt die Haushaltsausnahme, nach der die DSGVO keine Anwendung findet. (Das Hochladen von Geburtstagsfotos in einen Cloud-Speicher oder das Teilen solcher Bilder in einem begrenzten Personenkreis fällt dadurch nicht unter die DSGVO.) Geschieht die Verarbeitung jedoch für wirtschaftliche Zwecke, ist die DSGVO hingegen anwendbar.

Für die Anwendbarkeit der DSGVO ist nicht der Datenverarbeitungsstandort sondern eine Niederlassung im EU-Raum ausschlaggebend. Nach dem Marktortprinzip unterliegt eine Verarbeitung der DSGVO, wenn diese durch eine Niederlassung innerhalb der EU erfolgt oder Personen betrifft, die sich im EU-Raum aufhalten.

Ein Cloud-Anbieter, der sein eigenes Rechenzentrum als feste Einrichtung betreibt, gilt als in der EU niedergelassen. Gehören ihm jedoch nur einige Server in einem Rechenzenter, das nicht von seinen Angestellten betreten wird, liegt keine Niederlassung vor (Colocation). Bei der Auftragsverarbeitung durch einen Cloud-Anbieter innerhalb des EU-Raums liegt keine Niederlassung vor.

Werden Angebote für Waren und Dienstleistungen an Personen im EU-Raum angeboten, oder wird deren Verhalten (zwecks Profilbildung) beobachtet, findet die DSGVO Anwendung (siehe Google-Spain-Urteil). Ob sich beispielsweise ein Online-Shop an Personen in der EU richtet, kann von verschiedenen Faktoren abhängen (z.B. die verwendete TLD, Preisangaben in EU-Währungen, Verwendung europäischer Sprachen usw.)

5 Wann ist die Datenverarbeitung erlaubt? – Zulässigkeit (1. Stufe): Erlaubnistatbestände als Rechtsgrundlage

Ob personenbezogene Daten verarbeiten werden dürfen, ist zunächst eine Zulässigkeitsprüfung erforderlich. Eine Verarbeitung ist grundsätzlich verboten, sofern nicht ein Erlaubnistatbestand vorliegt (Verbot mit Erlaubnisvorbehalt). Es gibt u.a. folgende Erlaubnistatbestände:

- Einwilligung: Die betroffene Person stimmt einer Datenverarbeitung explizit zu. Diese Einwilligung ist mit Wirkung auf die Zukunft widerrufbar und bedarf keiner besonderen Form. Sie ist nur wirksam, wenn folgende Voraussetzungen gegeben sind:
    1. Freiwilligkeit: Es liegt keine Zwangssituation vor.
    2. Bestimmtheit: Die Verarbeitung erfolgt auf einen klar bestimmten Zweck; es liegt keine pauschale Einwilligung vor.
    3. Informiertheit: Die betroffene Person wurde in klarer und verständlicher Sprache über die Verarbeitung informiert.
    4. Einwilligungsbewusstsein: Die Einwilligung muss explizit erfolgen (Opt-In, z.B. durch Betätigung einer Schaltfläche oder Aktivierung einer Checkbox), eine Stillschweigende Einwilligung (Opt-Out) ist nichtig.
- Verarbeitung zur Erfüllung eines Vertrags: Zur Auslieferung einer bestellten Ware muss beispielsweise die Anschrift verarbeitet werden können; ein Vermieter muss die Kontaktdaten eines Mieters beispielsweise an den Hausmeister oder an einen Elektriker weitergeben können.
- Verarbeitung zur Erfüllung rechtlicher Verpflichtungen: Eine Firma muss beispielsweise aufgrund einer Aufbewahrungspflicht die Lohnabrechnungen ehemaliger Mitarbeiter für einige Zeit nach Beendigung des Beschäftigungsverhältnisses aufbewahren.
- Verarbeitung zur Wahrung berechtigter Interessen: Ein berechtigtes Interesse liegt etwa dann vor, wenn personenbezogene Daten innerhalb einer Unternehmensgruppe weitergeleitet werden, oder eine Datenverarbeitung zwecks IT-Sicherheit nötig ist. Hierzu müssen folgende Kriterien erfüllt sein:
    1. Der Verantwortliche muss ein berechtigtes Interesse an der Datenverarbeitung haben.
    2. Die Datenverarbeitung muss erforderlich sein, d.h. es gibt keine milderen Alternativen zur Durchsetzung des gleichen Interesses.
    3. Die Interessen des Berechtigten überwiegen das Schutzbedürfnis des Betroffenen.

- Auftragsverarbeitung: Ein Cloud-Anbieter verarbeitet Daten im Auftrag einer anderen Person.

Für besonders sensible Daten (z.B. genetische, biometrische oder Gesundheitsdaten) gibt es spezielle Regelungen, die im jeweiligen Fall zu prüfen sind.

6 Auftragsverarbeitung

Wird die Verarbeitung personenbezogener Daten an einen Cloud-Provider ausgelagert, spricht man von einer Auftragsverarbeitung. Diese liegt sowohl bei der Auslagerung einzelner IT-Ressourcen (z.B. Server) und Anwendungen (z.B. Microsoft 365) als auch bei einer vollständigen Auslagerung von Geschäftsprozessen (z.B. Lohnbuchhaltung) vor.

Der im Rahmen der Auftragsverarbeitung herbeigezogene Dienstleister entscheidet dabei nicht über Zwecke und Mittel der Datenverarbeitung, sondern muss sich dabei nach dem Verantwortlichen richten, der die Datenverarbeitung in Auftrag gibt. Hat der Verantwortliche beim Betroffenen eine Erlaubnis zur Datenverarbeitung eingeholt, darf er diese Verarbeitung ohne weitere Absprache mit dem Betroffenen an einen Auftragsverarbeiter (d.h. an einen Cloud-Anbieter) weitergeben. Die Verantwortung für den Schutz der Daten des Betroffenen geht dabei nicht an den Auftragsverarbeiter weiter, sondern verbleibt beim Verantwortlichen.

Der Auftragsverarbeiter gilt dabei nicht als Dritter, aber als Empfänger der Daten, der vom Verantwortlichen gegenüber dem Betroffenen auch als solcher in der Datenschutzerklärung zu benennen, bei Datenschutzauskünften mitzuteilen und im Verarbeitungsverzeichnis anzugeben ist. Typsische Beispiele für eine Auftragsverarbeitung sind:

- IT-Outsourcing oder Betreuung der IT-Infrastruktur durch einen Dienstleister (z.B. mit Fernzugriff auf personenbezogene Daten).
- Betreuung von Webseiten, Webshops und Analyse der entsprechenden Interaktionen durch Agenturen.
- Auslagerung von Datensicherung und -archivierung sowie die Vernichtung entsprechender Datenträger.
- Verarbeitung von Kundendaten durch Callcenter aus Marketing- oder zu Supportzwecken.
- Scan und Druck von Dokumenten, die personenbezogene Informationen enthalten.

Verarbeitet ein Cloud-Anbieter oder ein sonstiger Dienstleister Daten zu eigenen Zwecken, liegt keine Auftragsverarbeitung vor. (In diesem Fall ist ein Erlaubnistatbestand mit dem Betroffenen erforderlich.) Erlangt ein Sicherheitsdienst, ein Reinigungsunternehmen oder ein Berufsgeheimisträger (Anwalt, Steuerberater) im Rahmen einer Dienstleistung Zugriff auf personenbezogene Daten, liegt keine Auftragsverarbeitung vor. Mietet sich ein Unternehmen in einem Rechenzentrum ein (Colocation), ohne dem Anbieter dabei Zugriff auf personenbezogene Daten zu gewähren, liegt ebenfalls keine Auftragsverarbeitung vor.

Ein Auftragsverarbeitungsvertrag (AV-Vertrag) setzt eine sorgfältige Auswahl eines Auftragsverarbeiters voraus. Dieser muss fachlich geeignet sein und hinreichende Garantien bieten, dass technische und organisatorische ergriffen werden, um den Anforderungen der DSGVO zu genügen. (Diese werden vom Anbieter in einer Liste der technischen und organisatorischen Massnahmen – TOMs – ausgewiesen.) Der AV-Vertrag (Data Processing Agreement, DPA) wird zwischen dem Verantwortlichen und dem Auftragsverarbeiter abgeschlossen. Bei grossen Cloud-Anbieter sind das weitgehend standardisierte Verträge, die praktisch keinen Spielraum für besondere Regelungen bieten, und meist als Zusätze zu den allgemeinen Geschäftsbedingungen akzeptiert werden:

- Amazon: AWS GDPR Data Processing Addendum
- Google: Data Processing and Security Terms
- Microsoft: Nachtrag zum Datenschutz für Microsoft-Produkte und -Services

Bei kleineren Cloud-Anbietern besteht oftmals mehr Spielraum um den AV-Vertrag an die jeweiligen Anforderungen der jeweiligen Datenverarbeitung anzupassen.

Im Rahmen eines AV-Vertrags kann auch die Auftragsverarbeitung vonseiten des Auftragsverarbeiters zu einem Unterauftragnehmer (Subunternehmer) geregelt sein. Diese Auftragsverarbeitung hat unter den gleichen Bedingungen wie diejenige zwischen dem Verantwortlichen und dessen Auftragsverarbeiter zu erfolgen.

Grundsätzlich ist der Einsatz von einem Subunternehmer vom Verantwortlichen zu genehmigen, da eine Einzelgenehmigung jedoch in der Praxis kaum praktikabel ist (gerade bei grossen Cloud-Anbietern mit sehr vielen Kunden), müssen diesen oft allgemeine Genehmigungen erteilt werden. Es besteht jedoch die Möglichkeit, gegen den Einsatz bestimmter Subunternehmer Einspruch zu erheben, wenn hierzu ein wichtiger Grund vorliegt (z.B. wenn ein Subunternehmer als Konkurrent des Verantwortlichen Zugriff auf dessen personenbezogene Daten erhält). Grosse Cloud-Anbieter bieten jedoch oft keine solche Wiederspruchsmöglichkeit.

Bei der Auftragsverarbeitung im Ausland ist der Standort der Datenverarbeitung relevant. Hier ist zwischen zwei Fällen zu unterscheiden:

1. Innerhalb vom EU-/EWR-Ausland gibt es keine zusätzlichen Anforderungen, da diese Weitergaben der DSGVO unterstehen.
2. Beim Austausch mit Drittstaaten gelten besondere Anforderungen an internationale Datentransfers; hierbei ist die Einschätzung der EU-Kommission an das Datenschutzniveau des jeweiligen Ziellandes ausschlaggebend. (Die Schweiz gilt beispielsweise als sicheres Drittland.)

Sind bei einer Datenverarbeitung mehrere Staaten als Standorte involviert, ist die rechtliche Situation in allen Standorten zu berücksichtigen.

7 Gemeinsame Verantwortlichkeit (Joint Control)

Werden personenbezogene Daten von zwei oder mehreren Parteien gemeinsam verarbeitet, und legen diese (im Gegensatz zur Auftragsverarbeitung) Zwecke und Mittel dieser Datenverarbeitung gemeinsam fest, spricht man von einer gemeinsamen Verantwortlichkeit (Joint Control).

Die Abgrenzung gegenüber der Auftragsverarbeitung ist nicht immer klar, da ein vermeintlicher Auftragsverarbeiter oftmals eigene Zwecke und Mittel zur Datenverarbeitung hat, wie es beispielsweise bei Google Analytics der Fall ist. (Google fungiert hier als eigener Verantwortlicher, da es mit der Datenverarbeitung eigene Ziele verfolgt.)

Die gemeinsamen Verantwortlichen legen neben Mittel und Zwecken auch die Verteilung der Pflichten untereinander in einer Vereinbarung zwischen den gemeinsamen Verantwortlichen fest. Diese Vereinbarung orientiert sich inhaltlich an einer Auftragsverarbeitungsvereinbarung.

8 Allgemeine Grundsätze für die Verarbeitung personenbezogener Daten

Im Falle einer zulässigen Verarbeitung personenbezogener Daten ist dabei auf die folgenden Grundsätze zu achten:

- *Rechtmässigkeit*: Es muss die Erlaubnis des Betroffenen (oder ein sonstiger Erlaubnistatbestand) für die Verarbeitung vorliegen.
- *Verarbeitung nach Treu und Glauben*: Die betroffene Person muss Kenntnis von einer Verarbeitung haben und über deren Bedingungen informiert werden.
- *Transparenz*: Es muss für den Betroffenen nachvollziehbar sein (z.B. über eine Datenschutzerklärung), welche Daten von wem für welche Zwecke verarbeitet werden.
- *Zweckbindung*: Die Verarbeitung darf nur für festgelegte, eindeutige und legitime Zwecke erfolgen. Ändert sich der Zweck der Verarbeitung, muss der Betroffene auf diese einwilligen. (Eine Datenerhebung "auf Vorrat" ist nicht zulässig.)
- *Datenminimierung*: Die Verarbeitung soll auf das für den Zweck notwendige Mass minimiert sein. Es gilt der Grundsatz der Verhältnismässigkeit, sodass nicht das absolute Minimum der Verarbeitung zwingend ist. Hingegen ist zu prüfen, ob die Daten zum jeweiligen Zweck auch anonymisiert verarbeitet werden könnten.
- *Richtigkeit*: Daten sind auf dem neuesten Stand zu halten; alte Daten sind zu berichtigen oder zu löschen.
- *Speicherbegrenzung*: Daten sollen nur so lange gespeichert werden, wie es für den jeweiligen Zweck nötig ist.

- *Integrität und Vertraulichkeit*: Eine angemessene Datensicherheit soll durch dazu geeignete Massnahmen (Zugangssicherung, verschlüsselte Übertragung, periodische Datensicherung) gewährleistet werden. (Da Datensicherungen ein legitimes Mittel zur Gewährleistung von Integrität und Vertraulichkeit sind, steht ihre Anfertigung nicht im Konflikt zu Datenminimierung und Speicherbegrenzung.)
- *Rechenschaftspflicht*: Die Verarbeitungsgrundsätze sind nicht nur einzuhalten, sondern auch zu dokumentieren, etwa um die Einhaltung gegenüber Aufsichtsbehörden nachweisen zu können. Kann die Einhaltung der DSGVO im Schadensfall nicht nachgewiesen werden, werden die Verantwortlichen nicht aus der Haftung befreit; Bussgelder drohen.

9 Verarbeitungsverzeichnis

Verantwortliche, gemeinsame Verantwortliche und Auftragsverarbeiter müssen die von ihnen vorgenommenen Verarbeitungen personenbezogener Daten im der *Dokumentation aller Verarbeitungstätigkeiten* (kurz: im *Verarbeitungsverzeichnis*) dokumentieren. Bis auf wenige Ausnahmen (Unternehmen mit weniger als 250 Beschäftigten, deren Datenverarbeitung keine Risiken birgt, nur gelegentlich erfolgt und keine besonderen personenbezogenen Daten betrifft) müssen alle Unternehmen ein solches Verarbeitungsverzeichnis führen.

Das Verarbeitungsverzeichnis dient u.a. zum Nachweis der Einhaltung der DSGVO gegenüber Aufsichtsbehörden, zum Festhalten der konkreten Rechtsgrundlage und bildet die Grundlage für die Arbeit des Datenschutzbeauftragten. Das Verarbeitungsverzeichnis ist nicht öffentlich und muss betroffenen Personen nicht offengelegt werden. Es muss aber bei Bedarf den Aufsichtsbehörden zur Verfügung gestellt werden, wobei bei Nichtvorlegung (oder Nichtvorhandensein) Strafen drohen.

Im Verarbeitungsverzeichnis werden *Verarbeitungstätigkeiten* – eine Reihe von Verarbeitungsschritten zur Erfüllung eines gemeinsamen Zwecks (z.B. der Newsletterversand an Kunden oder die Personalverwaltung) – des Verantwortlichen abstrakt dokumentiert. Der Detailgrad der Beschreibung ist so zu wählen, dass das Verarbeitungsverzeichnis für Aussenstehende nachvollziehbar ist. Beim Aufbau dieser Dokumentation orientiert man sich oftmals anhand konkreter Anwendungen und Systeme, welche bei der Verarbeitung zum Einsatz kommen.

Für das Verarbeitungsverzeichnis ist die Geschäftsleitung verantwortlich; diese Verantwortung wird meist jedoch an den Datenschutzbeauftragten weitergereicht, welcher das Verzeichnis mit den involvierten Fachabteilungen erstellt und pflegt.

Im Verarbeitungsverzeichnis sind folgende Informationen festzuhalten:

- Name und Kontaktdaten der/des Verantwortlichen und des Datenschutzbeauftragen (zwecks Kontaktaufnahme)
- Zwecke der Verarbeitung (z.B. Betrieb eines Online-Shops)
- Kateogrien betroffener Personen (z.B. Webseitenbesucher, Kunden, Interessenten)
- Kategorien personenbezogener Daten (z.B. Kundenstammdaten, Zahlungsinformationen)

- Kategorien von – internen und externen – Empfängern (Abteilungen, Dienstleister, Hoster, Cloud-Anbieter)
- Datenübermittlungen in ein Drittland (z.B. in die USA)
- Löschfristen (falls möglich)
- Beschreibung der technischen und organisatorischen Massnahmen (hilfreich ist oft der Bezug auf die TOMs der Auftragsverarbeiter)
- optional: Ergänzende Beschreibung der Verarbeitugnstätigkeit
- optional: Festhalten der Rechtsgrundlage (z.B. Einwilligung des Kunden bei der Registrierung im Webshop)
- optional: Dokumentation des Ergebnisses einer Datenschutz-Folgeabschätzung

Es empfiehlt sich bei der Erstellung eines Verarbeitungsverzeichnis auf Mustervorlagen der jeweiligen Aufsichtsbehörde zurückzugreifen.

Bei gemeinsamen Verantwortlichen müssen nicht beide ein Verarbeitungsverzeichnis führen. Es empfiehlt sich, diese Verantwortlichkeit unter den gemeinsam Verantwortlichen zu regeln.

Das Verarbeitungsverzeichnis von Auftragsverarbeitern ist weniger ausführlich und muss u.a. die Kategorien der Empfänger nicht aufführen, was gerade bei grossen Cloud-Anbietern kaum praktikabel wäre.

10 Datensicherheit

Ein häufiger Vorbehalt gegenüber Cloud Computing sind Unsicherheiten im Bezug auf die Datensicherheit, welche folgende Ziele hat:

- *Vertraulichkeit*: Unbefugter Zugriff auf Daten soll mithilfe von Zugriffs- und Berechtigungskontrollen sowie mit dem Einsatz von Verschlüsselungstechnologien ausgeschlossen werden.
- *Integrität*: Die Unversehrtheit von Daten soll sichergestellt werden indem unbefugtes Modifizieren an Daten und Metadaten (u.a. Autor, Änderungszeitpunkt) verhindert wird. Hierzu kommen neben Zugriffs- und Berechtigungsmechanismen auch zusätzliche Schutzmassnahmen wie Firewalls zum Einsatz.
- *Verfügbarkeit*: Dem Nutzer sollen die Daten jederzeit zur Verfügung stehen, was mittels redundanten Setups von Hardware und Schutz vor DDoS-Attacken gewährleistet werden soll.

Diese Schutzziele werden mithilfe geeigneter technischer und organisatorischer Massnahmen (TOMs) gewährleistet.

Die Datensicherheit beschäftigt sich mit dem Schutz sämtlicher Systeme, Anwendungen und Daten und bildet die Voraussetzung für den *Datenschutz*, welcher das Recht natürlicher Personen im Umgang mit ihren Daten regelt.

Im Rahmen der DSGVO hat der Verantwortliche entsprechende Massnahmen zu ergreifen, diese zum Nachweis zu dokumentieren und auch von eingeschalteten Auftragsverarbeitern einzufordern.

Ein angemessenes Schutzniveau kann auf Basis eines risikobasierten Ansatzes gewählt werden, wobei Eintretenswahrscheinlichkeit und Schadensausmass bei einem sicherheitsrelevanten Vorfall zu berücksichtigen sind.

Beim Cloud Computing sind dabei neben den bekannten Sicherheitsrisiken auch cloudspezifische Risiken wie beispielsweise die folgenden zu beobachten:

- ungenügende Isolation der Mandanten bei gemeinsam genutzten IT-Ressourcen
- Fehler in der Bedienung einer Cloud-Verwaltungsoberfläche
- grenzüberschreitende Datenverarbeitung
- Anbieterabhängigkeit (*Vendor-Lock-in*)

Bei der Auswahl eines Cloud-Anbieters empfiehlt sich ein Blick der erlangten Zertifizierungen, wie beispielsweise:

- der C5-Kriterienkatalog (*Cloud Computing Compliance Criteria Catalogue*) vom BSI, der Mindestanforderungen an sicheres Cloud Computing enthält
- ISO/IEC 27001, der die Abbildung eines *Informationssicherheits-Managementsystems* (*ISMS*) beschreibt
- ISO 9001 zum Qualitätsmanagement und ISO 9004 zur kontinuierlichen Verbesserung desselben
- das IT-Grundschutz-Kompendium des BSI
- der *EuroCloud Star Audit*
- der Trusted-Cloud-Kriterienkatalog

Für den Nachweis einer DSGVO-Konformität kann bisher keine offizielle Zertifizierung erlangt werden, entsprechende Programme sind jedoch in Erarbeitung.

Weiter empfiehlt es sich, Notfallpläne zu erstellen und ein entsprechendes Notfallmanagement zu etablieren.

11 Datenschutz-Folgeabschätzung

Bei der *Datenschutz-Folgeabschätzung* (*Data Protection Impact Assessment*, DPIA) handelt es sich um eine präventive Prüfung für besonders risikobehaftete Verarbeitungsvorgänge, die aufgrund ihrer Art, ihres Umfangs, ihrer Umstände oder ihrer Zwecke ein hohes Risiko für die Betroffenen zur Folge haben.

Bei bestimmten Verarbeitungen (z.B. Einsatz von Profiling- oder Scoring-Verfahren, bei der umfangreichen Überwachung öffentlich zugänglicher Bereiche sowie bei weiteren von Aufsichtsbehörden aufgelisteter Vorgänge) ist eine DSFA zwingend durchzuführen. Diese muss Folgendes enthalten:

- eine systematische Beschreibung der Verarbeitungsvorgänge mitsamt Zweck
- eine Bewertung der Notwendigkeit und Verhältnismässigkeit der Verarbeitung bezogen auf den Zweck
- eine Bewertung der Risiken für die Rechte und Freiheit der Betroffenen
- geplante Abhilfemassnahmen zum Schutz personenbezogener Daten im Einklang mit der DSGVO

Bei der Nutzung von Cloud-Angeboten ist der Nutzer als Verantwortlicher für die Ausarbeitung einer DSFA verantwortlich.

Ein prominentes Beispiel ist der Einsatz von Microsoft 365, bei dem in der Regel eine DSFA durchzuführen ist. (Als Abhilfemassnahme ist etwa die Deaktivierung der Übertragung von Telemetrie- und Diagnosedaten an Microsoft verbreitet.)

12 Wann dürfen Daten in Länder ausserhalb der EU übermittelt werden? – Zulässigkeit (2. Stufe): Internationale Datntransfers

Da in verschiedenen Ländern unterschiedliche Datenschutzniveaus gewährleistet sind, muss sichergestellt werden, dass die DSGVO nicht durch einen Datentransfer über Landesgrenzen unterlaufen wird. Die Anforderungen an den Datenschutz müssen quasi mit den übertragenen Daten "mitreisen". Oftmals ist es die einfachste Lösung, Daten nur innerhalb des EU/EWR-Raumes zu übermitteln, wo die DSGVO verbindlich gilt.

Als Datenübermittlung gilt ein Vorgang bei dem Daten an andere Empfänger weitergegeben bzw. zu deren Abruf bereitgestellt werden (etwa über Download-Plattformen). Bei einer internationalen Datenübermittlung stellt ein *Datenexporteur* einem *Datenimporteur* jenseits der Landesgränze Daten zur Verfügung. Hierbei ist zwischen zwei Grundkonstellationen zu unterscheiden:

1. Eine Datenübertragung innerhalb der EU sowie zu den EWR-Staaten Island, Norwegen und Liechtenstein, die nicht EU-Mitglieder sind. Diese sind datenschutzrechtlich gleichgestellt; die DSGVO ist in diesen Ländern verbindlich.
2. Eine Datenübertragung in ein sogenanntes Drittland, wobei zwischen *sicheren Drittländern* mit angemessenem Datenschutzniveau (z.B. Schweiz, UK, Japan) und *unsicheren Drittländern* ohne angemessenem Datenniveau (z.B. USA) unterschieden wird. (Ein angemessenes Datenschutzniveau wird von der EU-Kommission in einem *Angemessenheitsbeschluss* festgestellt.)

Diese Unterscheidung macht es nötig, dass ein Verantwortlicher den genauen Standort der Datenverarbeitung kennt. Viele Cloud-Anbieter ermöglichen es, Daten ausschliesslich im EU-Raum zu verarbeiten, das für die Nutzer der jeweiligen Angebote datenschutztechnisch eine grosse Vereinfachung darstellt. Gewährt ein Anbieter jedoch technischem Personal aus einem

Drittland Zugriff auf personenbezogene Daten, liegt wiederum eine Datenübertragung vor, wobei das technische Personal als Empfänger fungiert.

Ein Sonderfall bilden Datenübertragungen in die USA, welche traditionell einen schwächer ausgeprägten bzw. nur branchenspezifischen Datenschutz kennen. Daher gelten die USA als unsicheres Drittland. Um Handelshemmnisse zwischen EU-Ländern und den USA abzubauen, wurden die *Safe-Harbor-Vereinbarung* zwischen der EU und den USA abgeschlossen, die auf einer *freiwilligen Selbstregulierung* basieren. Ein Anbieter in den USA verpflichtet sich dabei dazu, ein der EU vergleichbares Datenschutzniveau einzuhalten (Selbstzertifizierungsmechanismus). Dieses Abkommen bildete von 2000 bis 2015 die Grundlage für Datenübermittlungen in die USA, bis der Europäische Gerichtshof (EuGH) Safe Harbor für ungültig erklärte, da das Abkommen keinen genügenden Datenschutz gewähre.

Mit dem *EU-U.S. Privacy Shield* wurde 2016 ein weiteres Abkommen geschlossen, das wiederum auf einer freiwilligen Selbstzertifizierung der US-Unternehmen basierte. Die Enthüllungen von Edward Snowden zeigten jedoch, dass auch dieses Abkommen kein genügendes Schutzniveau bietet, zumal US-Behörden umfassenden Zugriff auf Daten von EU-Bürgern erhielten. Das *Privacy Shield* wurde 2020 vom EuGH für ungültig erklärt, wodurch entsprechende Datentransfers über Nacht rechtswidrig wurden. Mit dem *Trans-Atlantic Data Privacy and Security Framework* ist jedoch eine Nachfolgeregelung bereits in Arbeit.

Eine Datenübertragung in die USA ist nur aufgrund besonderer Vereinbarungen möglich, bei der sich ein US-Unternehmen verpflichtet, ein angemessenes Datenschutzniveau zu gewährleisten, und hierzu entsprechende Massnahmen ergreift. Diese Vereinbarungen basieren entweder auf *verbindlichen internen Datenschutzvorschriften* (*Binding Corporate Rules*, BCR) oder auf *Standardvertragsklauseln* (*Standard Contractual Clauses*, SCC). Bei letzteren handelt es sich um einen modular aufgebauten Mustervertrag, der von beiden Parteien – Datenexporteur und Datenimporteur – zu ergänzen und zu unterschreiben ist. Diese sind ohne weitere Genehmigung einer Aufsichtsbehörde gültig, sofern der Standardvertrag nicht modifiziert wird. (Ergänzungen und zusätzliche Garantien sind jedoch möglich, sofern die DSGVO dadurch nicht unterlaufen wird.) Die neuen Standardvertragsklauseln von 2021 erfüllen gleichzeitig die Anforderungen an einen Auftragsverarbeitungsvertrag.

13 Datenzugriff durch Behörden nach dem Recht der USA

US-Behörden können unter bestimmten Voraussetzungen nicht nur auf Daten zugreifen, die an einen Empfänger in die USA übermittelt worden sind, sondern auch auf solche, die ein US-Unternehmen ausserhalb von US-Territorium gespeichert hat. Wichtige Gesetze in diesem Zusammenhang sind:

- Der *Foreign Intelligence Surveillance Act* aus dem Jahr 1978 dient zur Spionageabwehr und ermöglicht die Herausgabe von Geschäftsunterlagen an US-Sicherheitsbehörden auf dem Wege gerichtlicher Anordnungen.

- Die *Executive Order 12333*, 1981 von Ronald Reagan erlassen, ermöglicht Überwachungsmassnahmen und Informationssammlungen ausserhalb der USA.
- Der *USA Patriot Act* ist eine Reaktion auf die Terroranschläge vom 11. September 2001 und erweitert die Befugnisse von US-Sicherheitsbehörden zur Terrorismusbekämpfung.
- Der *USA Freedom Act* ersetzt teilweise abgelaufene Vorschriften des Patriot Act.
- Der *CLOUD Act* ermöglicht es US-Sicherheitsbehörden im Rahmen eines Strafverfahrens auf Daten zuzugreifen, die von US-Unternehmen oder deren Tochtergesellschaft kontrolliert werden, auch wenn diese extraterritorial (z.B. im EU-Raum) abgespeichert sind. Dies betrifft nicht nur beispielsweise die eigenen Daten eines Cloud-Unternehmens, sondern auch diejenigen des Cloud-Nutzers, wodurch auch Geschäftsgeheimnisse von europäischen Unternehmen betroffen sein können. Der CLOUD Act steht demnach in Konflikt zur DSGVO, welche solche Daten vor einem entsprechenden Zugriff schützt. Ein Datenverarbeiter steht so vor der Wahl, ob er gegen US-Recht oder gegen die DSGVO verstossen soll, wobei in beiden Fällen hohe Strafen drohen. Ein Rahmenabkommen zwischen der EU und den USA zur Auflösung dieses Konflikts ist in Arbeit, aber noch nicht abgeschlossen.

Durch die genannten Regelungen ergaben sich verschiedene Rechtsunsicherheiten und -streitigkeiten, beispielsweise:

- Bei der Einführung von Office 365 sorgten die Aussagen eines Microsoft-Mitarbeiters für Aufregung, gemäss derer Microsoft nicht in der Lage sei den Verbleib von Anwenderdaten in der EU zu gewährleisten.
- Microsoft sollte 2013 den E-Mail-Verkehrs eines mutmasslichen Drogenhändlers an Ermittlungsbehörden herausgeben. Betroffen waren dabei nicht nur die in den USA abgespeicherten E-Mails, sondern auch solche, die in Irland abgespeichert waren. Microsoft verweigerte letzteres, wurde aber in erster Instanz durch ein US-amerikanisches Gericht zur Herausgabe verurteilt. In zweiter Instanz bekam Microsoft doch Recht und musste die Daten vorerst nicht herausgeben. Als Reaktion auf dieses Urteil wurde jedoch bald der CLOUD Act verabschiedet und Microsoft musste die Daten schliesslich doch offenlegen.

Durch die Konfliktsituation zwischen US-Recht und DSGVO ergeben sich einige Rechtsunsicherheiten. So ist es nicht klar, inwiefern einem Verarbeiter ein Verstoss gegen die DSGVO zur Last gelegt werden kann, wenn dessen Daten von einem US-amerikanischen Cloud-Anbieter an US-Sicherheitsbehörden weitergeleitet werden. Hier kann für den Verarbeiter argumentiert werden, dass der Cloud-Anbieter als Auftragsverarbeiter fungiert und dem entsprechenden AV-Vertrag zuwider handelt.

Weitere Fragen ergeben sich bei Konstellationen, wo die US-Tochter ein europäischen Unternehmens zur Datenherausgabe verpflichtet wird. Hier können die USA via Tochtergesellschaft Druck auf das Mutterhaus ausüben, um eine Datenherausgabe zu erreichen, wobei die DSGVO verletzt wird.

Als Mitigationsmassnahmen empfehlen sich Datentrennungen nach Territorien oder der Einsatz von Verschlüsselungsverfahren bei übertragenen und ruhenden Daten.