



European Cloud Service
Data Protection Certification

AUDITOR-Zertifizierungsgegenstand

- Fassung 1.00 -

Stand 05.06.2024

Weitere AUDITOR-Dokumente:

- Zertifizierungsgegenstand Kurzfassung
- Kriterienkatalog
- Konformitätsbewertungsprogramm
- Modularitätskonzept
- Schutzklassenkonzept

Online verfügbar: www.auditor-cert.de

Empfohlene Zitation:

Roßnagel, A., Sunyaev, A., Lins, S., Maier-Reinhardt, N., Müller, J., & Teigeler, H. (2024). AUDITOR-Zertifizierungsgegenstand – Fassung 1.00. Online verfügbar: www.auditor-cert.de

Beitrag zum Forschungsprojekt „European Cloud Service Data Protection Certification (AUDITOR)“, das aufgrund eines Beschlusses des Deutschen Bundestages vom Bundesministerium für Wirtschaft und Klimaschutz gefördert wird (FKZ 01MT17003).

Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

Autoren

Alexander Roßnagel^a, Ali Sunyaev^b, Sebastian Lins^b, Natalie Maier-Reinhardt^a, Johannes Müller^a, Heiner Teigeler^b

^a Projektgruppe verfassungsverträglichen Technikgestaltung (provet) im Wissenschaftlichen Zentrum für Informationstechnik-Gestaltung (ITeG) der Universität Kassel

^b Forschungsgruppe Critical Information Infrastructures (cii) am Institut für Angewandte Informatik und Formale Beschreibungsverfahren (AIFB) des Karlsruher Instituts für Technologie

U N I K A S S E L
V E R S I T Ä T

provet }



Inhaltsverzeichnis

Abkürzungsverzeichnis.....	2
A. Konkretisierung des Zertifizierungsgegenstands für den AUDITOR-Kriterienkatalog aus juristischer Perspektive.....	3
1. Herleitung des Zertifizierungsgegenstands aus der Datenschutz-Grundverordnung	3
1.1. Juristische Literaturmeinungen zum Zertifizierungsgegenstand	4
1.2. Leitlinien des Ausschusses zum Zertifizierungsgegenstand	5
2. Gegenstand des AUDITOR-Zertifizierungsverfahrens	6
B. Konkretisierung von Verarbeitungsvorgängen von personenbezogenen Daten im Kontext von Cloud-Diensten.....	9
1. Definition Cloud Computing und Cloud-Dienste.....	9
2. Verarbeitung von personenbezogenen Daten in der Cloud	12
2.1. Definition personenbezogener Daten.....	12
2.2. Verarbeitungsvorgänge in Cloud-Diensten	12
2.3. Schematisches Verarbeitungsvorgangmodell	16
C. Zertifizierungsreichweite und Verantwortlichkeiten.....	26
1. Schichtenmodell zur Abgrenzung von Verantwortlichkeiten.....	26
1.1. Schichtenmodell.....	26
1.2. Beispiele	28
2. Verantwortungsverteilung zwischen Cloud-Anbieter und Cloud-Nutzer	30
3. Verantwortungsverteilung zwischen Cloud-Anbieter und Subauftragsverarbeiter.....	30
Literaturverzeichnis	32

Abkürzungsverzeichnis

Abs.	Absatz
Art.	Artikel
BDSG	Bundesdatenschutzgesetz neue Fassung (Geltung ab 25.5.18)
bspw.	beispielsweise
ders.	derselbe
DSGVO	EU-Datenschutz-Grundverordnung (Geltung ab 25.5.18)
engl.	englisch
et al.	et alii = und andere
f.	folgende
Hrsg.	Herausgeber
i.F.	im Folgenden
i.V.m.	in Verbindung mit
insb.	insbesondere
Lit.	litera = Buchstabe
Nr.	Nummer
Rn.	Randnummer
TOM	technische und organisatorische Maßnahmen
u.a.	unter anderem / und andere
UAbs.	Unterabsatz
z.B.	zum Beispiel

Hinweis zur geschlechtsneutralen Formulierung:

Alle personenbezogenen Bezeichnungen in diesem Dokument sind geschlechtsneutral zu verstehen. Zum Zweck der besseren Lesbarkeit wird daher auf die geschlechtsspezifische Schreibweise verzichtet, sodass die grammatikalisch maskuline Form kontextbezogen jeweils als Neutrum zu lesen ist (z.B. ist bei der Bezeichnung *Datenschutzbeauftragter* die Funktionsbezeichnung als Neutrum zu lesen und meint nicht einen ausschließlich maskulinen Personenbezug).

A. Konkretisierung des Zertifizierungsgegenstands für den AUDITOR-Kriterienkatalog aus juristischer Perspektive

Der Zertifizierungsgegenstand beschreibt das im Rahmen von AUDITOR zu überprüfende datenschutzkritische Untersuchungsobjekt auf Basis der Zertifizierungskriterien des AUDITOR-Kriterienkatalogs. Eine klare Bestimmung des Zertifizierungsgegenstands ist wichtig, da sich die spätere Aussage des Zertifikats auf diesen bezieht. Sowohl die Cloud-Anbieter als Antragsteller im Zertifizierungsverfahren als auch die Cloud-Nutzer als Kunden des zertifizierten Cloud-Dienstes müssen sich auf den Aussagegehalt verlassen können. Schließlich wollen die Cloud-Anbieter mit der Zertifizierung ihre Konformität mit der Datenschutz-Grundverordnung nachweisen und mit dieser am Markt werben, um gegenüber Mitbewerbern Wettbewerbsvorteile zu erzielen. Der Cloud-Nutzer möchte durch die Zertifizierung darauf vertrauen können, dass der verwendete Cloud-Dienst datenschutzkonform ist. Schließlich darf der Cloud-Nutzer als Verantwortlicher gemäß Art. 28 Abs. 1 DSGVO nur mit Auftragsverarbeitern zusammenarbeiten, die über „hinreichende Garantien“ verfügen, die bestätigen, dass geeignete technische und organisatorische Maßnahmen (TOM) so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der Datenschutz-Grundverordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

Das Dokument enthält in Abschnitt A eine Definition des Zertifizierungsgegenstands aus juristischer Perspektive gemäß der Datenschutz-Grundverordnung. In Abschnitt B erfolgt eine cloud-spezifische Konkretisierung des Zertifizierungsgegenstands aus technischer Sicht. Schließlich werden in Abschnitt C auch die Reichweite der Zertifizierung und die Verantwortlichkeiten diskutiert.

1. Herleitung des Zertifizierungsgegenstands aus der Datenschutz-Grundverordnung

Datenschutzrechtliche Zertifizierungsverfahren als solche werden bisher allein durch die Datenschutz-Grundverordnung geregelt. Lediglich den Regelungsauftrag an die Mitgliedstaaten in Art. 43 Abs. 1 Satz 2 DSGVO hat § 39 BDSG dadurch erfüllt, dass er die Akkreditierung von Zertifizierungsstellen der Deutschen Akkreditierungsstelle und die Erteilung der Befugnis, als Zertifizierungsstelle datenschutzspezifische Zertifikate zu erteilen der zuständigen Datenschutz-Aufsichtsstelle überträgt. Zwar kann der nationale Gesetzgeber auch ohne explizite Öffnungsklausel im Bereich der Zertifizierung tätig werden und eigene Regelungen vorsehen, soweit diese den Regelungen der Datenschutz-Grundverordnung nicht widersprechen.¹ Dies ist der Fall, solange der nationale Gesetzgeber unbestimmte Rechtsbegriffe lediglich präzisiert,² ausfüllungsbedürftige Vorgaben konkretisiert, Regelungslücken schließt oder unvollständige Regelungen ergänzt.³ Soweit die Datenschutz-Grundverordnung unvollständig, ergänzungs- oder konkretisierungsbedürftig ist, ist daher eine Ko-Regulierung durch den nationalen Gesetzgeber möglich und erforderlich, um die Rechtsanwendung praktikabel zu machen.⁴ Grundsätzlich ist es daher auch möglich, Verfahrensfragen zur Zertifizierung nach Art. 42 DSGVO ergänzend zur Datenschutz-Grundverordnung im nationalen Recht zu regeln. Solche ergänzenden Regelungen liegen bisher jedoch noch nicht vor.

Die Datenschutz-Grundverordnung sieht die bisher im deutschen Recht bekannte Zweiteilung zwischen Auditierung und Zertifizierung nicht mehr vor.⁵ Sie stellt weder auf die Zertifizierung von Produkten noch auf die Auditierung von Datenschutz-Managementsystemen ab.⁶ In Art. 42 Abs. 1 Satz 1 DSGVO ist nur die Rede von „datenschutzspezifischen Zertifizierungsverfahren“ mit dem Ziel der Überprüfung und Bestätigung von „Verarbeitungsvorgängen“. Prüfungsmaßstab ist damit nach dem Wortlaut der Norm die Einhaltung der Verordnungsvorgaben und somit eine „rechtliche Selbstverständlichkeit“,⁷ da die Normen der Datenschutz-Grundverordnung ohnehin verbindlich sind und Pflichtverletzungen durch Verantwortliche und Auftragsverarbeiter zum Teil mit sehr hohen Bußgeldern belegt werden. Ob Zertifizierungsverfahren auch Zertifizierungskriterien beinhalten können, die einen höheren Datenschutzstan-

¹ *Biervert*, in: Schwarze u.a. 2012, Art. 288 AEUV, Rn. 6; *Roßnagel*, in: ders. 2018, § 2 I, Rn. 17.

² *Brühmann*, EuZW 2009, 643; *Roßnagel*, in: ders. 2018, § 2 I, Rn. 17.

³ *Roßnagel*, in: ders. 2018, § 2 I, Rn. 17.

⁴ *Roßnagel*, in: ders. 2018, § 2 I, Rn. 29.

⁵ *Hofmann/Roßnagel*, in: Krcmar/Eckert/Roßnagel/Sunyaev/Wiesche 2018, 104; s. hierzu auch *Hornung/Hartl*, ZD 2014, 219 ff.; zum Datenschutzaudit *Roßnagel* 2000.

⁶ *Bile*, in: *Roßnagel* 2018 § 5 VII., Rn. 237.

⁷ *Roßnagel/Richter/Nebel*, ZD 2015, 459; *Bile*, in: *Roßnagel* 2018, § 5 VII, Rn. 238.

Standard fordern als dieser in der Datenschutz-Grundverordnung niedergelegt ist, wird unterschiedlich beurteilt. Zum Teil wird ein höherer Standard aufgrund des abschließenden Charakters der Verordnung für nicht möglich gehalten.⁸ Andere halten ein freiwilliges „Mehr“ an Datenschutz bei Zertifizierungsverfahren für durchaus möglich,⁹ sofern sich die zusätzlichen Anforderungen im Einklang mit den Zielen der Verordnung befinden.¹⁰ Diese Ansicht schien auch der Datenschutzausschuss (Ausschuss) zu vertreten. Im Anhang 2 der Leitlinien 1/2018 zur Zertifizierung und zur Identifizierung von Zertifizierungskriterien¹¹ wurde erläutert, dass Zertifizierungsmechanismen nicht irreführend sein dürfen. Irreführung wurde bspw. angenommen, wenn ein Zertifizierungsmechanismus den Namen „Privacy Gold Standard“ trägt, gleichzeitig jedoch Kriterien enthält, die nur die Mindestanforderungen der Datenschutz-Grundverordnung abbilden.¹² In der angenommenen Version 3.0 der Leitlinien 1/2018 zur Zertifizierung¹³ finden sich diese Ausführungen jedoch nicht mehr. Ob daraus geschlussfolgert werden muss, dass Kriterienkataloge für die Zertifizierung nur Kriterien enthalten dürfen, die nicht über die gesetzlichen Mindestanforderungen der Datenschutz-Grundverordnung hinausgehen, wird hier nicht weiter diskutiert, da dies für die Bestimmung des Zertifizierungsgegenstands im Rahmen der AUDITOR-Zertifizierung keine Rolle spielt.

Gemäß Art. 42 Abs. 1 DSGVO sollen die Mitgliedstaaten, die Aufsichtsbehörden, der Ausschuss und die Kommission insbesondere auf Unionsebene die Einführung von datenschutzspezifischen Zertifizierungsverfahren sowie von Datenschutzsiegeln und -prüfzeichen fördern, die dazu dienen, nachzuweisen, dass die Datenschutz-Grundverordnung bei *Verarbeitungsvorgängen* von Verantwortlichen oder Auftragsverarbeitern eingehalten wird.

Der Begriff des Verarbeitungsvorgangs wird in der Grundverordnung jedoch nicht legaldefiniert, wohl aber der Begriff der Verarbeitung. *Verarbeitung* ist nach Art. 4 Nr. 2 DSGVO 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, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung. Aus dem Wortlaut der Norm kann daher zumindest geschlossen werden, dass jeder Umgang mit personenbezogenen Daten während der Zertifizierung einer Prüfung unterzogen werden muss.

1.1. Juristische Literaturmeinungen zum Zertifizierungsgegenstand

Bevor die Leitlinien des Ausschusses zur Zertifizierung vorlagen, fanden sich in der juristischen Literatur unterschiedliche Ansichten zum Zertifizierungsgegenstand. Angelehnt an den Gesetzeswortlaut von Art. 42 Abs. 1 DSGVO wurde zum einen die Ansicht vertreten, dass einzelne oder mehrere Verarbeitungsvorgänge den Gegenstand einer Zertifizierung zu bilden haben, nicht jedoch die Organisation des Verantwortlichen oder Auftragsverarbeiters in ihrer Gesamtheit oder auch Teile der Organisation.¹⁴ Zum anderen wurde die Ansicht vertreten, dass Zertifizierungen nach Art. 42 Abs. 1 DSGVO als Verfahrensaudits anzusehen sind und somit verfahrens- und prozessbezogene Verarbeitungsvorgänge den Zertifizierungsgegenstand zu bilden haben.¹⁵

Andere Ansichten stützten sich auf Erwägungsgrund 100, der als Zertifizierungsgegenstand Produkte und Dienstleistungen nennt, und erklärten, dass auch die ganzheitliche Zertifizierung von Produkten oder Dienstleistungen möglich ist¹⁶ und sich die Zertifizierung nicht nur auf einzelne Verarbeitungsvorgänge im technischen Sinn beschränkt.¹⁷

⁸ *Hornung/Hartl*, ZD 2014, 224; *Schweinoch/Will*, in: Ehmann/Selmayr 2018, Vorb. Art. 40-43, Rn. 8.

⁹ *Hofmann/Roßnagel*, in: Krcmar/Eckert/Roßnagel/Sunyaev/Wiesche 2018, 106; *Bergt*, in: Kühling/Buchner 2018, Art. 42, Rn. 15; *Bile*, in: Roßnagel 2018, § 5 VII., Rn. 238.

¹⁰ *Bile*, in: Roßnagel 2018, § 5 VII., Rn. 238.

¹¹ *European Data Protection Board*, Annex 2 on the review and assessment of certification criteria pursuant to Article 42(5) to the Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679, version for public consultation (i.F. Annex 2).

¹² *European Data Protection Board*, Annex 2, 9.

¹³ *European Data Protection Board*, Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679, Version 3.0, June 2019.

¹⁴ *Schweinoch/Will*, in: Ehmann/Selmayr 2018, Vorb. Art. 40-43, Rn. 8; *Will*, in: Ehmann/Selmayr 2018, Art. 42, Rn. 15; *Eckhardt*, in: Wolff/Brink 2018, Art. 42, Rn. 35.

¹⁵ *Hornung*, in: Auernhammer 2018, Art. 42, Rn. 46.

¹⁶ *Bergt*, in: Kühling/Buchner 2018, Art. 42, Rn. 3; *Eckhardt*, in: Wolff/Brink 2018, Art. 42, Rn. 32.

¹⁷ *Bergt*, in: Kühling/Buchner 2018, Art. 42, Rn. 3; aA *von Braunmühl/Wittmann*, in: Plath 2018, Art. 42, Rn. 7.

Dieser Ansicht wurde entgegengehalten, dass Zertifizierungen in erster Linie dem Nachweis der Einhaltung der Datenschutz-Grundverordnung dienen und Anknüpfungspunkte für einen Rechtsverstoß daher lediglich Verarbeitungsvorgänge sein können und nicht ganze Produkte. Daher könnten nur Verarbeitungsvorgänge den Zertifizierungsgegenstand bilden und nicht Produkte als solche.¹⁸ Dieser Ansicht nach sollte es Verantwortlichen oder Auftragsverarbeiter jedoch möglich sein, sämtliche mit dem Produkt oder Dienst in Zusammenhang stehenden Verarbeitungsvorgänge zertifizieren zu lassen.¹⁹ Wichtig sollte nur sein, dass nicht ein Produkt oder eine Dienstleistung den Zertifizierungsgegenstand darstellt, sondern die Zertifizierung auf spezifische Verarbeitungsvorgänge beschränkt bleibt.²⁰ Dies sollte nicht ausschließen, dass der zu Zertifizierende lediglich datenschutzrechtlich kritische Teilprozesse zertifizieren lassen kann, um so Kosten durch eine Zertifizierung zweifelsfrei datenschutzrechtlich unkritischer Verarbeitungsvorgänge zu vermeiden.²¹ Diese Ansicht wurde von Teilen der Literatur dahingehend geteilt, dass der Verantwortliche oder der Auftragsverarbeiter selbst den Gegenstand und den Umfang der Zertifizierung bestimmen könnte.²²

Auch andere Stimmen gingen in diese Richtung und trafen die Aussage, dass Zertifizierungen eine „große Spannweite des inhaltlichen Geltungsumfangs von einzelnen Verarbeitungsvorgängen“ bis hin zu „(sinnvoll abgrenzbaren) Teilen von Verarbeitungsvorgängen“ beinhalten können. So soll bspw. das Bewerberdatenmanagement einer Personalabteilung zertifizierbar sein.²³ Auch in rechtlich-organisatorischer Hinsicht sollen die Anwendungsbereiche von Zertifizierungen nicht eingeschränkt sein, sodass hierfür weder Minimal- noch Maximalvorgaben gelten sollten.²⁴

1.2. Leitlinien des Ausschusses zum Zertifizierungsgegenstand

Seit Juni 2019 liegen die vom Ausschuss nach öffentlicher Konsultation angenommenen Leitlinien zur Zertifizierung in Version 3.0 vor,²⁵ die Aussagen zum Zertifizierungsgegenstand enthalten. Der Ausschuss bleibt in seinen Leitlinien technologieneutral und benennt als Zertifizierungsgegenstand Verarbeitungsvorgänge oder Bündel von Verarbeitungsvorgängen. Er zählt drei Komponenten auf, die für die Bestimmung des Zertifizierungsgegenstands entscheidend sind: 1. personenbezogene Daten, 2. technische Systeme (Infrastruktur, Hardware und Software, die genutzt werden, um personenbezogene Daten zu verarbeiten) und 3. Prozesse und Verfahren, die mit Verarbeitungsvorgängen in Verbindung stehen.²⁶ Der Ausschuss stellt klar, dass jede Komponente der betreffenden Verarbeitungsvorgänge den Zertifizierungskriterien unterworfen werden muss. Je nach konkretem Zertifizierungsgegenstand kann die Bedeutung der einzelnen Komponenten jedoch unterschiedlich groß sein. Bedeutsam kann die IT-Infrastruktur sein, die die Verarbeitungsvorgänge unterstützt, inklusive des Betriebssystems, virtueller Systeme, Datenbanken, Authentifizierungs- und Autorisierungssystemen, Routern und Firewalls, Speichersystemen, Kommunikationsinfrastrukturen oder Internet-Zugängen, zugehörigen technischen Maßnahmen und der Personen, die in die Verarbeitungsvorgänge involviert sind.²⁷ Klargestellt wird ebenfalls, dass Verarbeitungsvorgänge auch organisatorische Maßnahmen umfassen. Die organisatorischen Maßnahmen können wiederum von den Kategorien und der Menge der verarbeiteten personenbezogenen Daten und der eingesetzten technischen Infrastruktur abhängen. Weiterhin sind Gegenstand, Inhalt und Zwecke der Verarbeitung im Rahmen der organisatorischen Maßnahmen von Verarbeitungsvorgängen ebenso zu betrachten wie die Risiken der Verarbeitung für die Rechte und Freiheiten der betroffenen Personen.²⁸

Die Leitlinien des Ausschusses sind auch deshalb hilfreich für die Bestimmung des Zertifizierungsgegenstands, weil der Begriff des Verarbeitungsvorgangs in Kontext zu den Begriffen der für die Zertifizierung von Produkten und Diensten wichtigen Norm DIN EN ISO/IEC 17065 gesetzt wird. Klargestellt wird, dass Verarbeitungsvorgänge oder Bündel von Verarbeitungsvorgängen in der Terminologie der

¹⁸ von Braunmühl/Wittmann, in: Plath 2018, Art. 42, Rn. 7.

¹⁹ von Braunmühl/Wittmann, in: Plath 2018, Art. 42, Rn. 7.

²⁰ Laue/Nink/Kremer 2016, Rn. 29

²¹ von Braunmühl/Wittmann, in: Plath 2018, Art. 42, Rn. 7.

²² Eckhardt, in: Wolff/Brink 2018, Art. 42, Rn. 34.

²³ Schweinoch/Will, in: Ehmann/Selmayr 2018, Vorb. Art. 40-43, Rn. 9.

²⁴ Schweinoch/Will, in: Ehmann/Selmayr 2018, Vorb. Art. 40-43, Rn. 8.

²⁵ European Data Protection Board, Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679, Version 3.0, June 2019.

²⁶ European Data Protection Board, Guidelines 1/2018, V. 3.0, Rn. 52.

²⁷ European Data Protection Board, Guidelines 1/2018, V. 3.0, Rn. 53f.

²⁸ European Data Protection Board, Guidelines 1/2018, V. 3.0, Rn. 56f.

Verordnung in ein Produkt oder eine Dienstleistung in der Terminologie von DIN EN ISO/IEC 17065 münden und dann Gegenstand einer Zertifizierung sein können.²⁹

Weiterhin stellt der Ausschuss klar, dass jedes Zertifizierungsprogramm seinen Zertifizierungsgegenstand allgemein auf Verarbeitungsvorgänge oder bezogen auf eine spezifische Art oder einen spezifischen Bereich von Verarbeitungsvorgängen festlegen kann. Im Fall von AUDITOR sind es Datenverarbeitungsvorgänge im Kontext von Cloud Computing. In jedem Fall müssen die konkreten Verarbeitungsvorgänge, die den Zertifizierungsgegenstand bilden sollen, klar beschrieben werden. Dies schließt eine Benennung der Daten, Prozesse und technischen Infrastrukturen ein.³⁰ Auch Schnittstellen zu anderen Prozessen oder Diensten müssen bedacht und beschrieben werden. Selbst in dem Fall, in dem bspw. nur einzelne Verarbeitungsvorgänge eines Dienstes zertifiziert werden sollen, ein Dienst aber aus mehreren Verarbeitungsvorgängen besteht, können Verarbeitungsvorgänge nur dann aus dem Zertifizierungsgegenstand herausgenommen werden, wenn sie keine direkten Verbindungen zu den zu zertifizierenden Verarbeitungsvorgängen haben. Auch in diesem Fall sind jedoch die Verbindungen der jeweiligen Verarbeitungsvorgänge zu beschreiben, um sie klar zu unterscheiden und eventuelle Datenflüsse zwischen diesen zu identifizieren.³¹

2. Gegenstand des AUDITOR-Zertifizierungsverfahrens

Für das AUDITOR-Zertifizierungsverfahren ist festzuhalten, dass Datenverarbeitungsvorgänge im Kontext von Cloud Computing, die in Cloud-Diensten oder von (auch mehreren) Cloud-Diensten erbracht werden, den Zertifizierungsgegenstand bilden.

Dass die Zertifizierung nach der Datenschutz-Grundverordnung trotz Erwägungsgrund 100, der von „einschlägigen Produkten und Dienstleistungen“ als Zertifizierungsgegenstand spricht, keine reine Produkt- oder Dienstzertifizierung meint,³² wird durch die Zielrichtung der Zertifizierung deutlich. Schließlich soll die Zertifizierung Verantwortlichen und Auftragsverarbeitern den Nachweis verschiedener Prüf- und Dokumentationspflichten erleichtern: Sie ist beim Nachweis der Einhaltung des Datenschutzrechts nach Art. 24 Abs. 3 DSGVO „als Faktor“ zu berücksichtigen, ebenso für die Erfüllung der Vorgabe zu Privacy by Design und Privacy by Default gemäß Art. 25 Abs. 3 DSGVO. Sie soll beim Nachweis ausreichender technisch-organisatorischer Sicherheit bei Auftragsverarbeitern gemäß Art. 28 Abs. 5 DSGVO sowie bei der Sicherheit der Datenverarbeitung gemäß Art. 32 Abs. 3 DSGVO ebenfalls zu berücksichtigen sein. Zusätzlich sieht Art. 83 Abs. 2 lit. j DSGVO vor, dass die Aufsichtsbehörde bei der Verhängung von Geldbußen bestandene Zertifizierungsverfahren „gebührend“ zu berücksichtigen hat. Schließlich kann eine Zertifizierung als Nachweis für das Vorhandensein von geeigneten Garantien bei einer Datenübermittlung ins EU-Drittland gemäß Art. 46 Abs. 2 lit. f i.V.m. Art. 42 Abs. 1 DSGVO dienen.

Diese Normen machen deutlich, dass es bei der Zertifizierung nach der Datenschutz-Grundverordnung um eine Überprüfung der tatsächlichen Datenverarbeitung anhand der Verordnungsvorgaben gehen muss. Eine Produktzertifizierung scheidet daher aus, da sie nur einen Teil der technischen und organisatorischen Maßnahmen der Datenverarbeitung beim Verantwortlichen oder Auftragsverarbeiter bestätigen könnte.³³ Schließlich ist es von entscheidender Bedeutung, in welcher Weise Produkte und Dienste beim Verantwortlichen oder Auftragsverarbeiter eingesetzt und nicht wie sie vom Hersteller angeboten werden. Weiterhin würde die Datenschutz-Grundverordnung bei einer reinen Produktzertifizierung gerade die Hersteller und nicht eine Vielzahl von Anwendern adressieren müssen, was sie jedoch gerade nicht tut. Dies ist auch schlüssig, da es für Verantwortliche und Auftragsverarbeiter als Anwender eines IT-Produkts wenig Sinn machen würde, wenn sie vielfach das jeweilige Produkt zertifizieren lassen würden, ohne selbst über ausreichende Informationen hierzu zu verfügen.³⁴ Auch würde es wenig Sinn machen, wenn das gleiche Produkt auf Wunsch des jeweiligen Verantwortlichen oder Auftragsverarbeiters vielfach dasselbe Zertifizierungsverfahren durchlaufen würde.

Vielmehr soll durch die Zertifizierung die Konformität der Verarbeitungsvorgänge, die in Produkten oder Diensten oder mit Hilfe von (auch mehreren) Produkten und Diensten erbracht werden, mit den Vorgaben der Datenschutz-Grundverordnung festgestellt werden. Diese liegen in der Einflussosphäre von Ver-

²⁹ *European Data Protection Board, Guidelines 1/2018, V. 3.0, Rn. 54.*

³⁰ *European Data Protection Board, Guidelines 1/2018, V. 3.0, Rn. 58.*

³¹ *European Data Protection Board, Guidelines 1/2018, V. 3.0, Rn. 59.*

³² *Hofmann/Roßnagel, in: Krcmar/Eckert/Roßnagel/Sunyaev/Wiesche 2018, 106.*

³³ *So auch bereits Hammer/Schuler, DuD 2007, 79.*

³⁴ *Roßnagel 2000, 57f.; für die alte Rechtslage nach dem BDSG Roßnagel, in: Hempel/Krasmann/Bröcking 2011, 267.*

antwortlichen und Auftragsverarbeitern und werden von diesen maßgeblich bestimmt, sodass folgerichtig auch nur diese beiden in Art. 42 Abs. 1 DSGVO als Adressaten von Zertifizierungsverfahren genannt werden.

In seinen Leitlinien zur Zertifizierung stellt der Ausschuss klar, dass Verarbeitungsvorgänge sowohl technischer als auch nicht technischer Natur sein können. Erfasst sind daher technikbasierte und -gesteuerte, aber auch organisatorische Vorgänge und Maßnahmen, die personeller oder manueller Natur sein können. Organisatorische Maßnahmen beziehen sich auf die Umstände der Verarbeitung außerhalb und innerhalb von technischen Systemen³⁵ und sind weit zu verstehen. Umfasst sind sämtliche Arten von Maßnahmen, angefangen von solchen, die Gebäude, die Sicherheit von IT-Systemen und organisatorische Regelungen betreffen, bis hin zu Zugriffsrechten, Administration, Wartung, und den Maßnahmen zur Umsetzung der in Art. 25 DSGVO genannten Grundsätze des Privacy by Design und by Default.³⁶ Organisatorische Maßnahmen können auch mit technischen und automatisierten Maßnahmen zusammenwirken. Es ist festzuhalten, dass die Datenschutz-Grundverordnung bei Verarbeitungsvorgängen von einem „dualen“ Verständnis ausgeht: Ein Verarbeitungsvorgang besteht sowohl aus nicht-technischen und nicht-automatisierten und somit personellen, manuellen und organisatorischen Prozessen als auch aus technischen und automatisierten Verfahren.

Zudem machen die Leitlinien des Ausschusses deutlich, dass einzelne Verarbeitungsvorgänge innerhalb eines Dienstes für sich nur zertifiziert werden können, wenn sie keine direkte Verbindung zu anderen Verarbeitungsvorgängen des Dienstes haben. In jedem Fall müssen die konkreten zu zertifizierenden Verarbeitungsvorgänge klar und vollständig beschrieben werden, was auch beinhaltet, dass Schnittstellen darzustellen sind. Einzelzertifizierungen von Teilen von Datenverarbeitungsvorgängen in Produkten oder Diensten im Sinne eines „Rosinenpickens“ unkritischer Teile und ihre Zertifizierung sind daher nach der Datenschutz-Grundverordnung nicht möglich. Schließlich sieht die Zertifizierung nach Art. 42 und Art. 43 DSGVO eine *Vollbestätigung* vor. Dies erfordert, dass der Zertifizierungsgegenstand so zu bestimmen ist, dass er eine in sich geschlossene Verfahrensstruktur für die Verarbeitung personenbezogener Daten aufweist, innerhalb der die spezifischen Datenschutzrisiken des jeweiligen Datenverarbeitungsvorgangs vollständig erfasst werden können.

Die Zertifizierung nach der Datenschutz-Grundverordnung darf nicht derart missverstanden werden, dass der in Art. 42 Abs. 3 DSGVO normierte Grundsatz der Freiwilligkeit eine beliebige Bestimmung des Zertifizierungsgegenstands ermöglicht, da diese ausschließlich die Teilnahme am Zertifizierungsverfahren und die Auswahl des konkreten zu zertifizierenden Datenverarbeitungsvorgangs meint. Der Cloud-Anbieter kann daher nicht darüber bestimmen, was ein Datenverarbeitungsvorgang ist und durch die Überprüfung welcher Teile eine Bestätigung der Datenschutzkonformität festgestellt werden soll, da nur in sich geschlossene Datenverarbeitungsvorgänge Zertifizierungsgegenstände sein können. Für den Cloud-Anbieter empfiehlt sich daher zunächst eine vollständige Datenflussanalyse der Anwendung mit allen an der Verarbeitung personenbezogener Daten beteiligten Akteuren wie bspw. auch der weiteren Auftragsverarbeiter (Subauftragsverarbeiter) zu erstellen³⁷ und zu bestimmen, welche Datenverarbeitungsschritte dem erweiterten Verantwortungsbereich des zu zertifizierenden Cloud-Anbieters zuzuordnen sind. Hierbei ist auch eindeutig darzulegen, wie die Zugriffsmöglichkeiten der Cloud-Nutzer und des Cloud-Anbieters in den jeweiligen Datenverarbeitungsvorgängen ausgestaltet sind. Diese internen Datenverarbeitungsschritte und -schnittstellen sind vollständig zu erfassen.

In der Zertifizierungspraxis werden hierfür Zertifizierungsvereinbarungen mit der Zertifizierungsstelle geschlossen, in denen die dem Cloud-Dienst zugrundeliegenden Datenverarbeitungsvorgänge identifiziert und klar bestimmt werden. Bei der AUDITOR-Zertifizierung werden diese im Zertifizierungsverfahren anhand der Kriterien des AUDITOR-Kriterienkatalogs von der Zertifizierungsstelle geprüft. Die Verarbeitungsvorgänge, die den Zertifizierungsgegenstand bilden, müssen für die Prämierung mit einem AUDITOR-Zertifikat allen relevanten Anforderungen der Datenschutz-Grundverordnung entsprechen. Dies umfasst bspw. die Festlegung von Verarbeitungszwecken, die eindeutige Festlegung der Verantwortlichkeiten zwischen Cloud-Nutzer und Cloud-Anbieter, die Einhaltung aller Grundsätze des Art. 5 DSGVO, die Wahrung der Betroffenenrechte und die Erfüllung weiterer Garantien für die Datenübermittlung außerhalb der Europäischen Union und des Europäischen Wirtschaftsraums. Alle diese Anforderungen sind als Kriterien im AUDITOR-Kriterienkatalog niedergelegt. Im individuellen Zertifizierungsprozess können die Besonderheiten der jeweiligen Cloud-Service-Modelle berücksichtigt werden. Im

³⁵ *Hartung*, in: Kühling/Buchner 2018, Art. 24, Rn. 17; *Martini*, in: Paal/Pauly 2018, Art. 24, Rn. 22.

³⁶ *Hartung*, in: Kühling/Buchner 2018, Art. 24, Rn. 17.

³⁷ So auch *EuroPriSe* 2017, Abschnitt C „the data flow resulting from the use of the product or service is to be illustrated and the legal provisions applicable for the certification are to be determined.“

Ergebnis bedeutet dies, dass der Cloud-Anbieter zwar vorab die zu zertifizierenden Datenverarbeitungsvorgänge analysieren muss, bei der konkreten Antragstellung und Durchführung des individuellen Zertifizierungsverfahrens jedoch die Zertifizierungsstelle miteinbezogen wird und selbst prüft.

Regelmäßig werden Cloud-Dienste nicht in ihrer Gesamtheit höchstpersönlich vom Cloud-Anbieter erbracht, sondern es werden Subauftragsverarbeiter für die Leistungserbringung eingesetzt. Einzelne Abschnitte oder Teile eines Datenverarbeitungsvorgangs werden dann an Subauftragsverarbeiter delegiert und von diesen erbracht. Das Einverständnis des Cloud-Nutzers zum Einsatz von Subauftragsverarbeitern vorausgesetzt, können auf diese Weise mehrstufige Subauftragsverhältnisse entstehen, was bei Cloud Computing auch sehr üblich ist. Die Auslagerung der Datenverarbeitung an Subauftragsverarbeiter darf jedoch nicht dazu führen, dass die Vorgaben der Datenschutz-Grundverordnung in der Leistungskette missachtet werden. Vielmehr muss der Cloud-Anbieter als Hauptauftragsverarbeiter dafür Sorge tragen, dass auf allen Stufen die einschlägigen Vorschriften der Datenschutz-Grundverordnung von allen Subauftragsverarbeitern eingehalten werden. Schließlich bleibt der Cloud-Anbieter gegenüber dem Cloud-Nutzer für die Auftragsdurchführung durchgängig verantwortlich. Aus diesem Grund muss der Cloud-Anbieter Sorgfalt bei der Auswahl der Subauftragsverarbeiter walten lassen und darf nur mit solchen zusammenarbeiten, die gemäß Art. 28 Abs. 1 DSGVO ebenfalls „geeignete Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Personen gewährleistet“. Subauftragsverarbeiter können die geforderten geeigneten Garantien ihrerseits bspw. durch ein datenschutzspezifisches Zertifikat erbringen.

Zusammengefasst bedeutet dies:

Der AUDITOR-Zertifizierungsgegenstand

Zertifizierungsgegenstand des AUDITOR-Verfahrens sind Datenverarbeitungsvorgänge, die in Produkten oder Diensten oder mit Hilfe von (auch mehreren) Produkten und Diensten erbracht werden. Schwerpunktmäßig werden im AUDITOR-Verfahren die Datenverarbeitungsvorgänge betrachtet, die der Cloud-Anbieter als Auftragsverarbeiter im Rahmen der Auftragsverarbeitung gemäß Art. 28 DSGVO durchführt. Es werden aber auch Datenverarbeitungsvorgänge betrachtet, die der Cloud-Anbieter als Verantwortlicher vornimmt, um den Vertrag mit dem Cloud-Nutzer über die Bereitstellung des Cloud-Dienstes schließen und diesen durchführen zu können und damit er rechtliche Pflichten erfüllen kann.

Bei der Bestimmung des Zertifizierungsgegenstands sind drei Komponenten wichtig, die Cloud-Anbieter als Adressaten des AUDITOR-Zertifizierungsverfahrens beachten müssen: 1. personenbezogene Daten, 2. technische Systeme (Infrastruktur, Hardware und Software, die genutzt werden, um personenbezogene Daten zu verarbeiten) und 3. Prozesse und Verfahren, die mit Verarbeitungsvorgängen in Verbindung stehen. Somit besteht ein Datenverarbeitungsvorgang in der Regel sowohl aus technischen und automatisierten als auch aus nicht-technischen organisatorischen Komponenten, die zu Datenschutzkonzepten und -managementsystemen zusammengefasst sind. So umfasst der Zertifizierungsgegenstand beispielsweise Support- oder Wartungstätigkeiten, wenn personenbezogene Daten verarbeitet werden. Der gesamte Datenverarbeitungsvorgang muss den Anforderungen der Datenschutz-Grundverordnung entsprechen.

Datenverarbeitungsvorgänge müssen eine geschlossene Verfahrensstruktur für die Verarbeitung personenbezogener Daten aufweisen, innerhalb derer die spezifischen Datenschutzrisiken des jeweiligen Cloud-Dienstes vollständig erfasst werden können. Dies bedeutet, dass auch Schnittstellen des zu zertifizierenden Cloud-Dienstes zu anderen Diensten betrachtet werden müssen, um Datenflüsse zu identifizieren, aus denen datenschutzrechtliche Risiken erwachsen können. Setzen die zu zertifizierenden Datenverarbeitungsvorgänge eines Cloud-Dienstes auf nicht-anbietereigene Plattformen oder Infrastrukturen auf oder setzt der Auftragsverarbeiter sonstige Subauftragsverarbeiter ein, so kann sich das Zertifikat nur auf diejenigen Datenverarbeitungsvorgänge beziehen, die im Verantwortungsbereich des jeweiligen Auftragsverarbeiters stehen. Der Auftragsverarbeiter muss sich jedoch davon überzeugen, dass auch diese fremden von ihm genutzten Plattformen, Infrastrukturen und Subauftragsverarbeiter die für sie relevanten datenschutzrechtlichen Vorschriften einhalten und darf nur solche einsetzen, um seinen Dienst zu erbringen.

B. Konkretisierung von Verarbeitungsvorgängen von personenbezogenen Daten im Kontext von Cloud-Diensten

Zur Festlegung des Zertifizierungsgegenstands sollte eine vollständige Datenflussanalyse mit allen an der Verarbeitung personenbezogener Daten beteiligten Akteuren erstellt werden. Hierbei sollte insbesondere auch überprüft werden, ob im Hinblick auf die Verarbeitungsvorgänge des Zertifizierungsgegenstands eine Übermittlung personenbezogener Daten außerhalb der Europäischen Union bzw. des Europäischen Wirtschaftsraums oder an internationale Organisationen erfolgt. Zudem muss bestimmt werden, welche Datenverarbeitungsschritte dem erweiterten Verantwortungsbereich des Cloud-Anbieters zuzuordnen sind. Hierbei ist auch eindeutig darzulegen, wie die Zugriffsmöglichkeiten der Cloud-Nutzer und des Cloud-Anbieters in den jeweiligen Datenvorgängen ausgestaltet sind. Um eine Datenflussanalyse zu unterstützen, werden im zweiten Teil dieses Dokuments die Verarbeitungsvorgänge von personenbezogenen Daten im Kontext von Cloud-Diensten detailliert betrachtet.

1. Definition Cloud Computing und Cloud-Dienste

In der Fachliteratur existiert eine Vielzahl von Definitionen und Erklärungsansätzen von Cloud Computing.³⁸ Dabei hat sich die Definition des National Institute of Standards and Technology (NIST) in der Fachwelt als Grundlage etabliert. Nach dieser Definition bezeichnet Cloud Computing ein Modell, das einen flexiblen und bedarfsorientierten Zugriff auf einen gemeinsam genutzten Pool von konfigurierbaren IT-Ressourcen ermöglicht, die jederzeit und überall über das Internet oder ein Netzwerk abgerufen werden können.³⁹ Darunter fällt bspw. der Zugriff auf Netzwerke, Server, Speicher oder Anwendungen. Cloud-Dienste werden mit minimalem Managementaufwand und geringer Interaktion mit dem Cloud-Anbieter zur schnellen Nutzung bereitgestellt und können an den Bedarf der Cloud-Nutzer angepasst werden. Ferner zeichnet sich Cloud Computing durch fünf spezielle Charakteristiken aus.

Die für Cloud Computing kennzeichnenden Charakteristiken sind der bedarfsgerechte Zugriff, eine Netzwerkanbindung, die Möglichkeit zur Ressourcenbündelung, eine hohe Skalierbarkeit und eine verbrauchsabhängige Bezahlung:⁴⁰

- **Bedarfsgerechter Zugriff (On-Demand Self-Service).** Der bedarfsgerechte Zugriff ermöglicht es Cloud-Nutzern, selbstständig und nahezu unmittelbar Leistungsparameter der in Anspruch genommenen Cloud-Dienste anzupassen. Dies kann insbesondere automatisch und ohne menschliche Interaktion mit den jeweiligen Cloud-Anbietern durchgeführt werden. So ist es bspw. möglich, je nach aktuellem Bedarf, erhaltene Rechen-, Speicher- oder Bandbreitenkapazitäten zu erhöhen oder zu reduzieren.
- **Netzwerkanbindung (Broad Network Access).** Cloud-Dienste werden über ein Breitbandnetzwerk bereitgestellt, in der Regel über das Internet. Cloud-Dienste nutzen standardisierte Kommunikationsschnittstellen und können mit einer Vielzahl von Endgeräten benutzt werden, darunter bspw. Smartphones, Tablets oder Laptops.
- **Ressourcenbündelung (Resource Pooling).** Die vom Cloud-Anbieter bereitgestellten Ressourcen werden durch eine Multi-Mandanten-Architektur von mehreren Cloud-Nutzern gleichzeitig genutzt. Dabei werden die physischen und virtuellen Ressourcen je nach Bedarf dynamisch den verschiedenen Cloud-Nutzern zugeteilt. Cloud-Nutzer können hierbei nicht immer den exakten Standort feststellen, an dem sich die genutzten Ressourcen befinden. Jedoch ist eine grobe Eingrenzung hinsichtlich des Landes, der Region oder des Rechenzentrums in einigen Fällen möglich.
- **Skalierbarkeit (Rapid Elasticity).** Bereitgestellte Ressourcen können flexibel und schnell, in einigen Fällen vollautomatisch, erhöht oder freigegeben werden, um so die Ressourcen auf den aktuellen Bedarf abzustimmen. U.a. deshalb entsteht beim Cloud-Nutzer der Eindruck, dass Ressourcen nahezu unbegrenzt und zu jeder Zeit in jedem Ausmaß verfügbar sind.
- **Verbrauchsabhängige Bezahlung (Measured Service).** Um Cloud-Dienste messbar und transparent zu gestalten, kontrollieren und optimieren Cloud-Dienste den Ressourcenverbrauch anhand von serviceabhängigen Kennzahlen, bspw. dem Speicherplatz, der Rechenleistung

³⁸ Leimeister et al. 2010; Marston et al. 2011; Schneider und Sunyaev 2015.

³⁹ Mell und Grance 2011.

⁴⁰ Mell und Grance 2011; Sunyaev und Schneider 2013.

oder der Bandbreite. Dadurch ist eine bedarfsgerechte Abrechnung möglich. Zudem wird die Ressourcennutzung überwacht, kontrolliert, protokolliert und kommuniziert, sodass sowohl für den Cloud-Nutzer, als auch für den Cloud-Anbieter, Transparenz über die Nutzung entsteht.

Im Cloud Computing kann zwischen den drei grundlegenden Service-Modellen Software as a Service (SaaS), Platform as a Service (PaaS) sowie Infrastructure as a Service (IaaS) unterschieden werden:⁴¹

- **Software as a Service (SaaS).** Der Cloud-Nutzer kann mittels verschiedener Geräte entweder über ein Thin-Client-Interface, bspw. einen Web-Browser, oder über ein entsprechendes Anwendungsinterface auf angebotene Softwareanwendungen zugreifen. Der Cloud-Nutzer hat hierbei keine Kontrolle über die zugrundeliegende Cloud-Infrastruktur, sondern kann nur spezifische Anwendungseinstellungen vornehmen („Nutzerspezifika“).
- **Platform as a Service (PaaS).** Der Cloud-Nutzer kann selbstentwickelte oder erworbene Anwendungen auf der Cloud-Infrastruktur des Cloud-Anbieters installieren und betreiben. Hierzu werden Betriebssysteme, Datenbanken, Programmierumgebungen, Programmbibliotheken oder weitere vom Cloud-Anbieter unterstützte Dienste und Werkzeuge genutzt. Ähnlich wie bei dem Software as a Service Modell hat der Cloud-Nutzer keine Kontrolle über die zugrundeliegende Cloud-Infrastruktur. Auf der anderen Seite kann er eigene installierte oder ausgeführte Anwendungen verwalten und kann gegebenenfalls eine limitierte Anzahl von Einstellungen in der entsprechenden technischen Anwendungsumgebung durchführen.
- **Infrastructure as a Service (IaaS).** Der Cloud-Nutzer erhält Zugang zu Hardwareressourcen des Cloud-Anbieters, darunter fallen bspw. Rechenleistung, Speicherkapazitäten oder Netzwerke. Diese kann er zur Installation und zum Betrieb beliebiger Software verwenden, bspw. Betriebssystemen oder Anwendungen. Ihm obliegt die Kontrolle über Betriebssysteme, Datenbanken und installierte Anwendungen, gegebenenfalls auch über ausgewählte Netzwerkressourcen, bspw. über Firewalls, jedoch nicht über die zugrundeliegende Cloud-Infrastruktur.

Darüber hinaus findet sich in der Praxis und Literatur eine Vielzahl von weiteren Service-Modellen, bspw. Database as a Service oder Security as a Service. Diese werden oft auch als **Everything as a Service (XaaS)** zusammengefasst.⁴² Im Folgenden wird nur zwischen den drei Modellen SaaS, PaaS und IaaS unterschieden.

Ferner wird zwischen den vier grundlegenden Bereitstellungsmodellen (engl.: „Deployment Models“) Private-, Community-, Public- und Hybrid-Cloud unterschieden.⁴³ Auch werden die Bereitstellungsmodelle Virtual-Private-Cloud und Multi-Cloud oft in der Literatur und Praxis angeführt.⁴⁴

- **Private-Cloud.** Die Cloud-Infrastruktur wird nur durch eine einzelne Organisation und deren Mitglieder genutzt. Sie kann sowohl von der Organisation, Dritten oder einer Kombination dieser besessen, verwaltet und betrieben werden. Ferner muss sich die Cloud-Infrastruktur dafür nicht zwingend lokal bei der Organisation befinden. Somit dient die Private-Cloud im Allgemeinen unternehmensinternen Zwecken, und der Cloud-Nutzer hat die volle Kontrolle, wer, wie und wann der Dienst genutzt werden kann.
- **Public-Cloud.** Die Cloud-Infrastruktur kann durch die allgemeine Öffentlichkeit genutzt werden. Unternehmen, akademische oder staatliche Organisationen oder eine Kombination dieser besitzen, verwalten und betreiben die Cloud-Infrastruktur. Die Public-Cloud stellt eine Auswahl von Dienstleistungen (bspw. Geschäftsprozesse, Geschäftsabläufe, Anwendungen und Infrastrukturen) auf Basis einer verbrauchsabhängigen Bezahlung grundsätzlich für jedermann gleichzeitig (Multimandantenfähigkeit) über das Internet zur Verfügung. Eines der wesentlichen Unterscheidungsmerkmale einer Public-Cloud ist, dass der Cloud-Nutzer keinerlei Einfluss darauf nehmen kann (weder technisch noch vertraglich), welche weiteren Parteien den Cloud-Dienst des Cloud-Anbieters nutzen. Somit teilen sich die Cloud-Nutzer (unwissentlich oder im Ausmaß und Umfang unbekannt) die zugrundeliegende Infrastruktur, die jedoch von der Anwendungsschicht komplett abstrahiert wird. Eine Anpassung an spezifische Nutzeranforderungen ist oft nur sehr eingeschränkt möglich oder widerspricht den Skalierungs- und Effizienzinteressen des Cloud-Anbieters.

⁴¹ Mell und Grance 2011; Schneider und Sunyaev 2015.

⁴² Singh et al. 2016.

⁴³ Mell und Grance 2011; Schneider und Sunyaev 2015.

⁴⁴ Dillon et al. 2010; Amazon Web Services 2015.

- **Community-Cloud.** Die Cloud-Infrastruktur wird ausschließlich durch eine Gruppe von Organisationen genutzt, welche ähnliche Anforderungen an den Cloud-Dienst stellen. Eine oder mehrere Organisationen der Community, Dritte oder eine Kombination dieser Parteien besitzen, verwalten und betreiben die Cloud-Infrastruktur. Auch hierbei muss sich die Cloud-Infrastruktur dafür nicht zwingend lokal bei der Organisation oder den Organisationen befinden.
- **Hybrid-Cloud.** Die Cloud-Infrastruktur besteht aus einer Kombination von zwei oder mehreren der oben beschriebenen Modelle (insb. Public- und Private-Cloud). Die einzelnen Infrastrukturen bleiben als Einheit erhalten, werden jedoch durch standardisierte oder proprietäre Technologien verbunden. Dies ermöglicht die Übertragung von Daten und Anwendungen zwischen den angebotenen Infrastrukturen. Mit dieser Mischform von Diensten soll eine Lösung entstehen, die den konkreten Anforderungen des jeweiligen Unternehmens am besten gerecht wird.
- **Virtual-Private-Cloud.** Erstmals wurde der Begriff „Virtual-Private-Cloud“ von Amazon Web Services (AWS) eingeführt, als deren neues Produkt „Amazon VPC“ vorgestellt wurde.⁴⁵ Beim Virtual-Private-Cloud-Modell wird die Infrastruktur de facto für eine einzelne Organisation bereitgestellt, die mehrere Nutzer (zum Beispiel Geschäftsbereiche) umfassen kann.⁴⁶ Der Zugriff auf den Cloud-Dienst wird unter der Verwendung eines Virtual Private Networks (VPN) realisiert. Die Cloud-Infrastruktur ist im Eigentum eines Cloud-Anbieters. Sie wird durch den Cloud-Anbieter betrieben und verwaltet, wobei der Cloud-Nutzer die vollständige Kontrolle über die virtuelle Netzwerkumgebung behält.
- **Multi-Cloud.** Werden Cloud-Dienste verschiedener Cloud-Anbieter aggregiert und zusammengefasst, kann dies als Multi-Cloud verstanden werden.⁴⁷ Hierbei können sowohl Cloud-Anbieter ihre Cloud-Infrastrukturen und Dienste mit anderen Cloud-Anbietern freiwillig vernetzen, oder ein Cloud-Broker tritt auf dem Markt auf, der verschiedene Cloud-Dienste von (unterschiedlichen) Cloud-Anbietern aggregiert und einen separaten Zugriff zu ihnen ermöglicht. Abbildung 1 stellt beispielhafte Multi-Cloud-Szenarien dar. Die Unterscheidung zwischen einer Multi-Cloud und einer Hybrid-Cloud stellt sich als schwierig und uneinheitlich dar. Im Gegensatz zu einer Hybrid-Cloud, bei der üblicherweise die Cloud-Infrastrukturen verbunden sind und gemeinsam arbeiten (Orchestrierung), werden bei Multi-Clouds gezielt nur bestimmte Cloud-Komponenten eines Cloud-Dienstes von einem weiteren Cloud-Anbieter genutzt. So kann ein Cloud-Anbieter einer Multi-Cloud bspw. die Berechnungs- und Netzwerkoperationen in einer AWS-Cloud durchführen, während die Speicherung allein durch die Azure-Cloud durchgeführt wird.

⁴⁵ Amazon Web Services 2015.

⁴⁶ Dillon et al. 2010.

⁴⁷ Grozev und Buyya 2014.

Zertifizierungsgegenstand

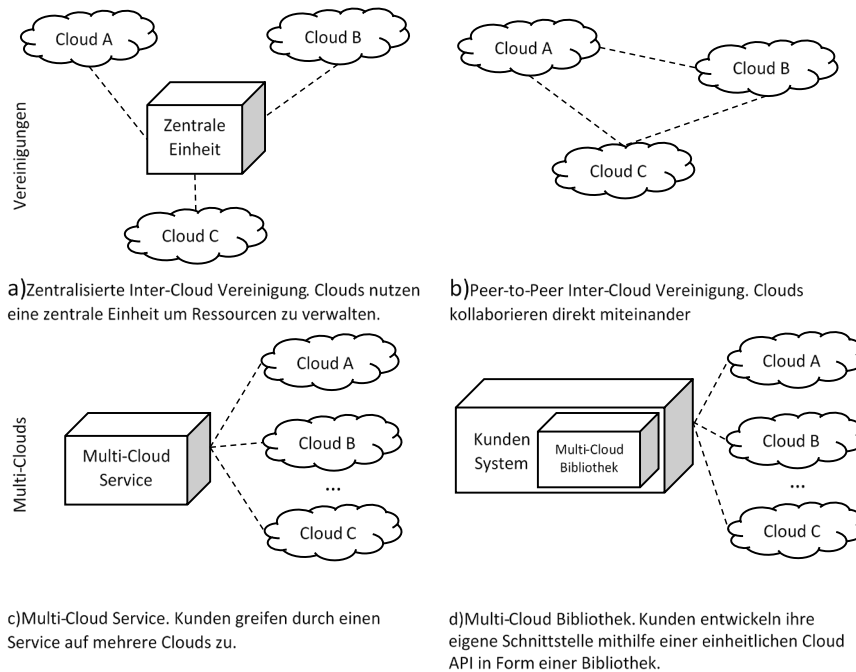


Abbildung 1. Beispielhafte Formen einer Multi-Cloud.⁴⁸

2. Verarbeitung von personenbezogenen Daten in der Cloud

2.1. Definition personenbezogener Daten

Gemäß Art. 4 Nr. 1 DSGVO sind „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche 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 identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

2.2. Verarbeitungsvorgänge in Cloud-Diensten

Wie dargestellt, bezeichnet Datenverarbeitung jeden Vorgang, der im Zusammenhang mit personenbezogenen Daten steht. Es ist individuell zu prüfen, welche Vorgänge dem Verantwortungsbereich des Cloud-Anbieters zuzuweisen sind. Insbesondere gilt zu beachten, dass Cloud-Anbieter durch den AUDITOR-Kriterienkatalog in zweierlei Hinsicht adressiert werden:

- (1) **Als Auftragsverarbeiter** von Datenverarbeitungsvorgängen. Die Cloud-Anbieter können sowohl B2B⁴⁹- als auch B2C⁵⁰-Anbieter sein. Wichtig ist nur, dass sie hinsichtlich der Daten, die

⁴⁸ Grozev und Buyya 2014.

⁴⁹ Business to Business (B2B) bedeutet, dass der Kunde entweder eine juristische oder eine natürliche Person ist, die personenbezogene Daten im Rahmen ihrer Geschäftstätigkeit verarbeitet. Ein „Unternehmen“ ist jede natürliche oder juristische Person, die bei Verträgen zu Zwecken handelt, die ihrer gewerblichen oder beruflichen Tätigkeit zugerechnet werden können.

⁵⁰ Business to Consumer (B2C) bedeutet, dass der Kunde eine natürliche und private Person ist und daher keine personenbezogenen Daten im Rahmen seiner Geschäftstätigkeit verarbeitet. Siehe auch „Cloud-Nutzer als Nutznießer“ (S. 8 im Kriterienkatalog) in Bezug auf den Cloud-Nutzer als natürliche Person, die unter die „Haushaltsausnahme“ fällt. Ein „Verbraucher“ ist jede natürliche Person, die bei Verträgen zu Zwecken handelt, die nicht ihrer gewerblichen oder beruflichen Tätigkeit zugerechnet werden können. Es ist jedoch zu beachten, dass ein Verbraucher nicht automatisch unter die sogenannte „Haushaltsausnahme“ gemäß Art. 2 Abs. 2 lit.c DSGVO fällt. Diese Ausnahme ist der Nichtanwendbarkeit in Bezug auf die Verarbeitung personenbezogener Daten durch eine natürliche Person im Rahmen einer rein persönlichen oder häuslichen Tätigkeit vorbehalten. Die Datenverarbeitung eines Verbrauchers kann also entweder unter diese Ausnahmeregelung fallen oder nicht, was zur Folge hat, dass seine Datenverarbeitung entweder privilegiert ist oder nicht. Im letzteren Fall ist der Verbraucher als für die Verarbeitung Verantwortlicher zu behandeln.

in der Cloud verarbeitet werden („**Inhalts- oder Anwendungsdaten**“⁵¹), als Auftragsverarbeiter und nicht als Verantwortliche tätig sind und die Datenschutzkonformität ihrer Datenverarbeitungsvorgänge durch ein Zertifikat bestätigen lassen möchten. Gerade im B2B-Bereich werden die Inhalts- und Anwendungsdaten häufig personenbezogene Daten von Kunden, Mitarbeitern oder anderen betroffenen Personen sein, mit denen der Cloud-Nutzer in Vertragsbeziehungen steht. Jedoch können Inhalts- und Anwendungsdaten auch personenbezogene Daten des Cloud-Nutzers sein.

- (2) **Als Verantwortlicher** von Datenverarbeitungsvorgängen. Der Cloud-Anbieter wird auch als Verantwortlicher von Datenverarbeitungsvorgängen adressiert, die erforderlich sind, um den Vertrag mit dem Cloud-Nutzer über die Bereitstellung des Cloud-Dienstes schließen und diesen durchführen zu können. Wird der Cloud-Dienst im B2C-Bereich angeboten, stellt der Cloud-Nutzer häufig auch die betroffene Person dar, deren Daten erforderlich sind, um den Cloud-Dienst bereitzustellen, sodass der Cloud-Anbieter seine datenschutzrechtlichen Pflichten (z.B. Informationspflichten) gegenüber dem Cloud-Nutzer erfüllen muss.

Im B2B-Bereich ist zu beachten, dass Daten juristischer Personen wie z.B. Namen oder Adressen gemäß EG 14 vom Anwendungsbereich der Datenschutz-Grundverordnung ausgenommen sind. Dies gilt jedoch nicht, wenn die Daten der juristischen Person eine enge personelle oder wirtschaftliche Verbindung zu einer natürlichen Person aufweisen wie dies z.B. bei einer Ein-Mann-GmbH der Fall ist. Dann liegen ebenfalls personenbezogene Daten vor und die Datenschutz-Grundverordnung ist anwendbar.

Schließt der Cloud-Nutzer einen Vertrag mit dem Cloud-Anbieter über die Bereitstellung und Nutzung des Cloud-Dienstes ab, wird der Cloud-Anbieter vor allem durch handels- und steuerrechtliche Aufzeichnungs- und Aufbewahrungspflichten zur Verarbeitung personenbezogener Daten verpflichtet, sodass die Datenverarbeitung zur Erfüllung rechtlicher Pflichten ebenfalls in den Anwendungsbereich der AUDITOR-Zertifizierung fällt.

Obwohl der Cloud-Anbieter grundsätzlich frei darin ist, den Zweck einer Verarbeitung und die hierfür passende Rechtsgrundlage aus Art. 6 Abs. 1 UAbs. 1 lit. a bis f DSGVO zu wählen und Art. 5 Abs. 1 lit. b i.V.m. Art. 6 Abs. 4 DSGVO auch keine strikte Zweckbindung, sondern nur eine Zweckvereinbarkeit kennt, werden im Rahmen der AUDITOR-Zertifizierung nur Datenverarbeitungen des Cloud-Anbieters in seiner Rolle als Verantwortlicher betrachtet, die in einem inneren Zusammenhang zum Vertrag zwischen dem Cloud-Anbieter und dem Cloud-Nutzer über die Bereitstellung und Nutzung des Cloud-Dienstes und die Durchführung der Auftragsverarbeitung stehen. Im Rahmen der AUDITOR-Zertifizierung werden daher nur Datenverarbeitungsvorgänge betrachtet, die der Cloud-Anbieter durchführt, um den Cloud-Dienst gegenüber dem Cloud-Nutzer zu erbringen, um diesem die Nutzung zu ermöglichen und um den Dienst abzurechnen.

Um den Vertrag mit dem Cloud-Nutzer über die Nutzung des Cloud-Dienstes abzuschließen und durchzuführen, entscheidet der Cloud-Anbieter, welche personenbezogenen Daten er erhebt und verarbeitet. In der Regel werden hier Daten wie Namen, Adressen, Zahlungsdaten wie beispielsweise Bankverbindungen, Rufnummern, Benutzernamen und Passwörter fürs Einloggen in den Cloud-Dienst verarbeitet. Diese können unter dem Begriff „**Bestandsdaten**“ zusammengefasst werden. Gerade im B2B-Bereich können neben den Daten des Cloud-Nutzers auch Daten anderer betroffener Personen wie beispielsweise von Mitarbeitern des Cloud-Nutzers erforderlich sein, um den Vertrag über die Nutzung des Cloud-Dienstes mit dem Cloud-Nutzer schließen und durchführen zu können. So werden z.B. Namen und Kontaktdaten von Mitarbeitern des Cloud-Nutzers verarbeitet, die dem Cloud-Anbieter als Ansprechpartner dienen sollen. Da der Cloud-Anbieter den Vertrag über die Cloud-Nutzung nicht mit dem Mitarbeiter schließt, kann Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO nicht die Verarbeitung der Mitarbeiterdaten legitimieren. Stattdessen kann sich der Cloud-Anbieter auf Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO und seine berechtigten Interessen an der Datenverarbeitung stützen, solange wie die Daten zur Begründung und Erfüllung des Vertrags mit dem Cloud-Nutzer erforderlich sind.

Um dem Cloud-Nutzer die Inanspruchnahme des Cloud-Dienstes zu ermöglichen und diese abzurechnen, muss der Cloud-Anbieter weitere personenbezogene Daten wie beispielsweise

⁵¹ Inhaltsdaten tragen die Informationen über eine betroffene Person in sich, wohingegen Anwendungsdaten Informationen über eine betroffene Person sind, die aus der Verwendung einer Softwareanwendung abgeleitet werden, z. B. wären Inhaltsdaten in einem Dokument die Bedeutung in Worten, während Anwendungsdaten aus dem Softwareprogramm stammen würden, das verwendet wird, um den Inhalt des Dokuments zu lesen.

Ein- und Auslogdaten zu Nutzerkonten, IP-Adressen, die genutzten Dienstmodule und den Umfang der Nutzung verarbeiten. Diese Daten können unter dem Begriff „**Nutzungsdaten**“⁵² zusammengefasst werden. Auch die Verarbeitung von Telemetrie- und Diagnosedaten fällt unter diesen Begriff, sofern die Daten für die Durchführung des Vertrags mit dem Cloud-Nutzer erforderlich sind.

Da die Datenschutz-Grundverordnung die Unterscheidung in Bestands- und Nutzungsdaten nicht kennt, werden diese Daten im Rahmen dieses Kriterienkatalogs als **personenbezogene Daten** bezeichnet, die ihm Rahmen der Durchführung des Auftrags über die Erbringung des Cloud-Dienstes anfallen.

Datenverarbeitungsvorgänge, die der Cloud-Anbieter **als für die Verarbeitung Verantwortlicher** vornimmt, um den Vertrag mit dem Cloud-Nutzer über die Bereitstellung des Cloud-Dienstes schließen und diesen durchführen zu können, sind z.B.:

- um den Vertrag schließen zu können: solche Daten, die der Anbieter entweder benötigt, um eine technische Schnittstelle bereitzustellen oder um zu entscheiden, ob seine derzeitigen Schnittstellen zur technischen Basis des Cloud-Nutzers für die Nutzung des Dienstes passen. Zu den Daten, die verarbeitet werden können, gehören beispielsweise technische Daten für die Erbringung des Dienstes, wie der verwendete Browser und Gerätetyp, die Version des Betriebssystems, eindeutige Gerätekennungen und Informationen über das Mobilfunknetzwerk. Dazu zählen etwa der Name, eine Telefonnummer, eine Adresse, eine E-Mail-Adresse, um ein Angebot übersenden zu können.
- solche zur Durchführung: Daten, die sich aus der Verarbeitung der in der rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung vereinbarten Daten ergeben, um den Dienst im Hinblick auf das konzeptionelle Ziel des Dienstes zu erhalten, sowie Nutzungsdaten⁵³, um entsprechend die Dienstnutzung abrechnen zu können. Zu den Daten, die verarbeitet werden können, gehören beispielsweise Zahlungsinformationen (z. B. Bankverbindung), Benutzernamen und Passwörter für die Anmeldung beim Cloud-Dienst oder nutzerspezifische Qualitätsindikatoren (z. B. für die Überwachung oder die Erbringung von Dienstleistungen). Dazu zählen etwa der Name, eine Telefonnummer, eine Adresse, eine E-Mail-Adresse, um eine Rechnung übersenden zu können.
- solche zur Erfüllung rechtlicher Verpflichtungen: Daten, die erforderlich sind, um Anomalien in Bezug auf kritische Infrastrukturen zu erkennen (z. B. An- und Abmeldedaten für Benutzerkonten und IP-Adressen, Standortdaten, etc.)

Im Gegensatz dazu stellen die folgenden Beispiele keine Datenverarbeitungsvorgänge dar, die von einem Cloud-Anbieter als für die Verarbeitung Verantwortlichem durchgeführt werden, um einen Vertrag mit einem Cloud-Nutzer zu schließen oder zu erfüllen:

- Datenverarbeitungsvorgänge für Marktforschung und -analyse (z. B. Erhebung und Analyse von Daten, um Erkenntnisse über Markttrends, Kundenpräferenzen und -verhalten zu gewinnen),
- Datenverarbeitungsvorgänge für Marketingzwecke (z. B. Erhebung und Verarbeitung von Daten zur Information über verwandte Produkte),
- Datenverarbeitungsvorgänge zur (betrieblichen) Geschäftsoptimierung, die nicht mit dem Cloud-Dienst zusammenhängen (z. B. Nutzung von Daten zur Optimierung interner Prozesse und Verfahren, um Kosten zu sparen).

Sobald der Cloud-Anbieter sich entschließt die Zertifizierung zu erlangen, wird er mit der Zertifizierungsstelle ausführliche Gespräche führen, um den Umfang der Zertifizierung und die konkreten Datenverarbeitungsvorgänge, die zertifiziert werden sollen, festzulegen. Das AUDITOR-Konformitätsbewertungs-

⁵² "Nutzungsdaten" sind zusätzliche personenbezogene Daten wie z.B. Login-/Logout-Daten für Nutzerkonten, IP-Adressen, die genutzten Servicemodule und der Umfang der Nutzung, die sich aus der Nutzung des Dienstes ergeben.

⁵³ "Nutzungsdaten" sind zusätzliche personenbezogene Daten wie z.B. Login-/Logout-Daten für Nutzerkonten, IP-Adressen, die genutzten Servicemodule und der Umfang der Nutzung, die sich aus der Nutzung des Dienstes ergeben.

programm spezifiziert diese Prozesse und die Zertifizierungsstellen sind verpflichtet, die entsprechenden Prozesse zu befolgen und anzuwenden.⁵⁴ Beispiele für Datenverarbeitungsvorgänge, die **nicht** unter der AUDITOR-Zertifizierung zertifiziert werden können sind: a) Datenverarbeitungsvorgänge, die ausschließlich für die Verarbeitung als Verantwortlicher durchgeführt werden, um den Vertrag mit dem Cloud-Nutzer über die Erbringung des Cloud-Dienstes abzuschließen und zu erfüllen, OHNE dass die Datenverarbeitungsvorgänge in seiner Rolle als Auftragsverarbeiter zertifiziert werden; b) Datenverarbeitungsvorgänge, die der Durchführung rechtswidriger Tätigkeiten dienen; oder c) wenn die den Cloud-Anbieter betreffenden Rechtsvorschriften ihn daran hindern würden, die Grundsätze der DSGVO einzuhalten.

⁵⁴ Unter anderem muss eine Zertifizierungsstelle die Durchführung einer bestimmten Zertifizierung ablehnen, wenn ihr (a) die Kompetenz oder Fähigkeit zur erforderlichen Durchführung der Zertifizierungsaktivitäten fehlt, (b) wenn ihr die Ressourcen fehlen, um alle Auswahl- und Ermittlungstätigkeiten durchzuführen, oder c) wenn ihre Unparteilichkeit gefährdet ist. Eine Zertifizierungsstelle kann ferner den Antrag eines Cloud-Anbieters auf Zertifizierung ablehnen, wenn der Cloud-Anbieter in illegale Aktivitäten verwickelt ist, der Cloud-Anbieter wiederholt gegen die AUDITOR-Zertifizierungskriterien verstoßen hat oder es Beweise für ähnliche Probleme in Bezug auf den Cloud-Anbieter gibt. Die Zertifizierungsstelle ist aufgefordert, Auswahlverfahren durchzuführen, die frei von Willkür bei der Bewertung sind, und ihre Entscheidungen transparent zu dokumentieren.

2.3. Schematisches Verarbeitungsvorgangsmodell

Das nachfolgende Modell stellt ein Referenzmodell für Vorgänge mit (personenbezogenen) Daten im Kontext von Cloud-Diensten dar. Abbildung 2 stellt das Modell graphisch dar und Tabelle 1 fasst die einzelnen Vorgänge des Modells zusammen. Das Modell soll Cloud-Anbieter und Zertifizierungsstellen bei der Datenflussanalyse unterstützen, um einen Datenverarbeitungsvorgang als Zertifizierungsgegenstand zu identifizieren, klassifizieren und alle relevanten Vorgänge einer Vorgangsreihe zu definieren. Eine allgemeine Zuordnung von Verantwortlichkeiten in dem folgenden Referenzenmodell ist nicht möglich, da diese Zuordnung stark abhängig von dem individuellen Service-Modell und der jeweiligen Ausgestaltung der Vereinbarung zur Auftragsverarbeitung mit dem Cloud-Nutzer ist.

Bei der Interpretation des Verarbeitungsvorgangsmodells sind folgende Annahmen zu berücksichtigen:

1. Nicht jeder Vorgang muss in einem zu zertifizierenden Datenverarbeitungsvorgang enthalten sein.
2. Die Verantwortlichkeiten pro Vorgang müssen einzeln festgelegt werden, da ein Cloud-Anbieter einzelne oder eine Auswahl von Vorgängen an Subauftragsverarbeiter auslagern kann oder Vorgänge in die Verantwortlichkeit des Cloud-Nutzers fallen können.
3. Modularisierungskonzepte sind in diesem Modell nicht berücksichtigt.
4. Das Modell erhebt keinen Anspruch auf Vollständigkeit.
5. Das Modell gibt keinerlei Auskunft über die Konformität zur DSGVO. Diese bestimmt sich nach den Kriterien des AUDITOR-Kriterienkatalogs.

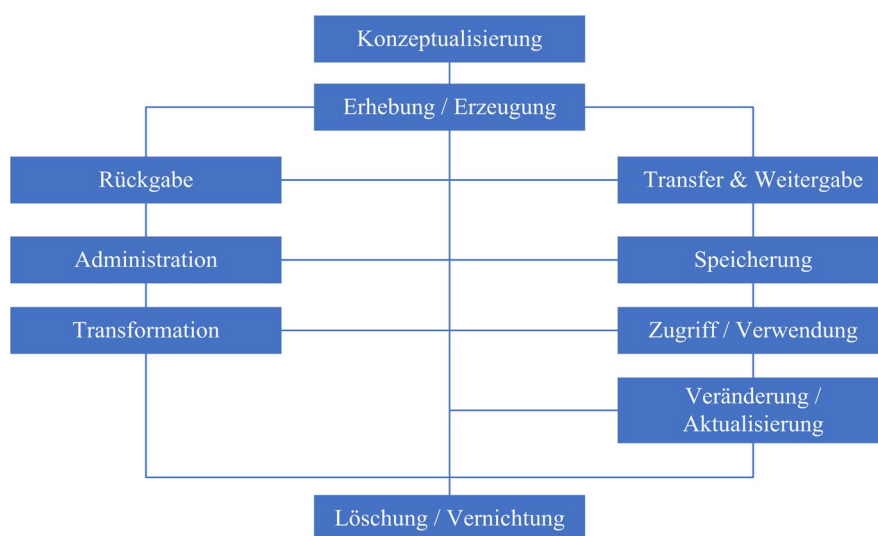


Abbildung 2. Verarbeitungsvorgangsmodell von (personenbezogenen) Daten im Kontext von Cloud-Diensten zur Unterstützung von Datenflussanalysen.

Vorgang in der Datenverarbeitung	Beschreibung
Konzeptualisierung	Definition und Beschreibung von zu erhebenden und verarbeitenden personenbezogenen Daten.
Erhebung / Erzeugung	Vorgänge zur Erhebung oder Erzeugung von relevanten Daten.
Transfer & Weitergabe	Vorgänge, die dazu führen, dass die Daten ihren Speicher oder Verarbeitungsort erreichen, oder an Dritte weitergegeben werden.
Speicherung	Vorgänge zur sicheren Speicherung der Daten.
Zugriff / Verwendung	Lesender Zugriff auf Daten zur weiteren Verwendung und Verarbeitung.
Veränderung / Aktualisierung	Schreibender Zugriff auf Daten, um die gespeicherten Werte zu verändern.

Transformation	Zweckgerichtete Veränderung der Daten, insbesondere zu ihrem Schutz.
Administration	Manuelle und automatische Vorgänge zur Verwaltung von Daten.
Rückgabe	(Vollständige) Rückgabe der Daten an den Cloud-Nutzer.
Löschung / Vernichtung	Löschung der Daten und ggf. Vernichtung der Speichermedien.

Tabelle 1. Mögliche Vorgänge eines Datenverarbeitungsvorgangs in der Cloud.

2.3.1 Konzeptualisierung

Vor der eigentlichen Datenerhebung und -verarbeitung durch einen Cloud-Dienst sollte ein Cloud-Anbieter prüfen, welche personenbezogenen Daten erhoben oder erzeugt werden müssen.⁵⁵ Während ein Cloud-Anbieter keine oder nur eine sehr begrenzte Kontrolle darüber hat, welche personenbezogenen Daten in der Cloud tatsächlich verarbeitet werden (bspw. Anwendungsdaten eines Nutzers), entscheidet er über die Daten, die zum Betrieb des Dienstes notwendig sind (bspw. Identifizierungs- und Abrechnungsdaten eines Nutzers).

Diese für den Betrieb des Cloud-Dienstes zu verarbeitenden personenbezogenen Daten sollten hinreichend definiert und beschrieben werden.⁵⁶ Dazu zählt bspw. die Bestimmung der Verarbeitungszwecke für die Daten.⁵⁷ Eine hinreichende Datenkonzeptualisierung unterstützt bspw. eine anschließende Festlegung von Sicherheitsmaßnahmen zum Schutz dieser Daten⁵⁸ und die Zuweisung von Rollen und Verantwortlichkeiten beim Datenmanagement.⁵⁹ Zudem können auch Anforderungen an die Daten, bspw. in Hinblick auf Qualitätsanforderungen oder notwendige Meta-Daten spezifiziert werden.⁶⁰ Ein Cloud-Anbieter sollte den Konzeptualisierungsvorgang unabhängig vom Service-Modell durchführen, da bei jedem Service-Modell prinzipiell personenbezogene Daten erhoben und verarbeitet werden können.

2.3.2 Erhebung / Erzeugung

Einen initialen und zentralen Vorgang stellt die Erhebung und Erzeugung von personenbezogenen Daten dar.⁶¹ Es können grundsätzlich vielfältige Daten erhoben oder erzeugt. Im Folgenden sind einige Beispiele aufgezeigt.

Beispiele für Inhalts- oder Anwendungsdaten:

- allgemeine Personendaten (Name, Geburtsdatum und Alter, Geburtsort, Anschrift, E-Mail-Adresse, Telefonnummer usw.);
- Kennnummern (Sozialversicherungsnummer, Steueridentifikationsnummer, Versichertennummer, Personalausweisnummer, Matrikelnummer usw.);
- Bankdaten (Kontonummern, Kreditinformationen, Kontostände usw.);
- Gesundheitsdaten;
- Online-Daten (IP-Adresse, Standortdaten usw.);
- physische Merkmale (Geschlecht, Haut-, Haar- und Augenfarbe, Statur, Kleidergröße usw.);
- Besitzmerkmale (Fahrzeug- und Immobilieneigentum, Grundbucheintragungen, Kfz-Kennzeichen, Zulassungsdaten usw.);
- Nutzerdaten (Bestellungen, Adressdaten, Kontodaten usw.);
- Bewertungen (Schul-, Prüfungs- und Arbeitszeugnisse usw.).

Beispiele für Bestandsdaten:

- Namen;
- Adressen;
- Zahlungsdaten wie Bankverbindungen;
- Rufnummern;

⁵⁵ Higgins 2008.

⁵⁶ Villazón-Terrazas et al. 2011; Möller 2013.

⁵⁷ van Veenstra und van den Broek 2015.

⁵⁸ van Veenstra und van den Broek 2015.

⁵⁹ Higgins 2012.

⁶⁰ Ofner et al. 2013; van Veenstra und van den Broek 2015.

⁶¹ Higgins 2008.

Zertifizierungsgegenstand

- Benutzernamen und Passwörter⁶² fürs Einloggen in den Cloud-Dienst;
- kundenindividuelle Qualitätskennzahlen, wodurch Monitoring- oder Service-Bereitstellung ermöglicht werden.

Beispiele für Nutzungsdaten:

- Angaben über Beginn und Ende sowie den Umfang der jeweiligen Nutzung;
- Angaben über die vom Nutzer in Anspruch genommenen Telemedien;
- Ein- und Auslogdaten zu Benutzerkonten und IP-Adressen;⁶³
- Identifizierungs- und Authentifizierungsdaten für die Identifizierung des Nutzers und den Zugriff auf den Cloud-Dienst wie Benutzernamen, IDs und E-Mail-Adressen. Bei einer Mehrfaktor-Authentifizierung können bspw. Mobil-Nummern, Fingerabdrücke, die menschliche Stimme oder Chipkarten erforderlich werden;
- technische Daten für die Dienstbereitstellung wie bspw. der verwendete Browser- und Gerätetyp, die Version des Betriebssystems, eindeutige Gerätekennungen, Informationen über das Mobilfunknetz, einschließlich der Telefonnummer;
- Meta-Daten aus dem Betrieb des Cloud-Dienstes wie bspw. Log Files, die Datenmigrationsvorgänge protokollieren oder Datenstandorte speichern. Der Personenbezug der Daten kann direkt gegeben sein oder durch gezielte Kombination verschiedener Meta-Daten entstehen;
- Standortdaten, wenn sie für die Inanspruchnahme des Dienstes erforderlich sind. Zur Standortbestimmung werden verschiedene Technologien genutzt, wie bspw. IP-Adressen, GPS und andere Sensoren, Informationen über nahe gelegene Geräte, WLAN-Zugangspunkte oder Mobilfunkmasten.

2.3.3 Transfer

Werden Daten erhoben und anschließend an die Cloud-Infrastruktur oder an das Rechenzentrum übertragen, sollten geeignete Schutzmaßnahmen getroffen werden.⁶⁴ Der Datentransfer umfasst alle Vorgänge, die dazu führen, dass die Daten ihren Speicher oder Verarbeitungsort erreichen.⁶⁵ Im Kontext von Cloud-Diensten werden zur Übertragung der Daten das Internet und Wide Area Network Technologien verwendet. Das bedeutet, dass bekannte Attacken, wie z.B. IP Spoofing, Paket Sniffer und Malware, im Kontext von Cloud-Diensten von Relevanz sind.⁶⁶

Insbesondere beim SaaS-Dienstmodell muss ein Cloud-Anbieter festlegen, welche Richtlinien und Maßnahmen zum Schutz der Daten bei der Übertragung durchgeführt werden. Ein PaaS- und IaaS-Anbieter muss sicherstellen, dass angebotene und offene Datenschnittstellen (bspw. zu angebotenen Datenbanken oder Virtuellen Maschinen) ausreichend gesichert werden. Zudem müssen Full-Stack- und IaaS-Anbieter die Übertragung innerhalb der Cloud-Infrastruktur oder zwischen verteilten Infrastrukturen überwachen und sichern. Werden Daten an Zwischenstellen oder Dritte weitergeleitet, müssen alle Cloud-Anbieter einen sicheren und datenschutzkonformen Datentransfer gewährleisten. Die Durchführung eines Datentransfers muss nicht in der Verantwortlichkeit eines Cloud-Anbieters liegen. Sie ist abhängig vom jeweiligen Service-Modell sowie der Gestaltung des Cloud-Dienstes und der individuellen Auftragsverarbeitungsvereinbarung mit dem Cloud-Nutzer.

SaaS	PaaS	IaaS
Sichere Erhebung und anschließende Übertragung an die Cloud-Infrastruktur, bspw. durch Verschlüsselung der Kommunikation.	Sicherung der Schnittstellen zum Datenempfang oder zur Anwendungsintegration.	Sicherung der Schnittstellen zum Datenempfang. Sichere Datenübertragung innerhalb und außerhalb der Cloud-Infrastruktur, bspw. zu einem externen Rechenzentrum zur redundanten Speicherung.

Tabelle 2. Datentransfer nach Dienst-Modell.

Wesentliche Datentransfervorgänge bei Cloud-Diensten sind:

- **Datentransfer an die Cloud-Infrastruktur über das Internet.** Wird ein Cloud-Dienst im Internet angeboten, so erfolgt die Übertragung von erhobenen Daten meist über das öffentliche Netz. Die

⁶² Dix, in: Roßnagel, Recht der Telemedien, 2013, § 14, Rn. 2; Boos/Kroschwald/Wicker, ZD 2013, 206.

⁶³ Boos/Kroschwald/Wicker, ZD 2013, 207.

⁶⁴ Higgins 2008.

⁶⁵ Bernard 2007

⁶⁶ Fernandes et al. 2014.

Daten müssen daher verschlüsselt übertragen werden, um mögliche Attacken vermeiden zu können.

- **Datentransfer an die Cloud-Infrastruktur über unternehmensinterne Netze.** Werden Daten über unternehmensinterne Netze wie WAN, LAN, VPN oder ähnlichen Technologien übertragen, muss auch hier die Sicherheit bei der Übertragung gewährleistet sein.
- **Datentransfer innerhalb der physischen Cloud-Infrastruktur.** Werden Daten vom Festplattenspeicher in den Arbeitsspeicher geladen, zwischen Servern ausgetauscht, Daten dupliziert oder ähnliche Operationen durchgeführt, muss sichergestellt werden, dass die Übertragung innerhalb einer (multimandantenfähigen) Cloud-Infrastruktur sicher durchgeführt wird.⁶⁷
- **Datentransfer innerhalb einer logisch getrennten Cloud-Infrastruktur.** Aufgrund der Multimandantenfähigkeit von Cloud-Diensten kann es von Nöten sein, dass Daten zwischen zwei logisch getrennten Netzen übertragen werden.⁶⁸ Sichere Mandantentrennungskonzepte sind daher erforderlich.
- **Datentransfer zwischen Cloud-Infrastrukturen.** Besitzt ein Cloud-Anbieter verteilte Cloud-Infrastrukturen oder Rechenzentren und tauscht Daten zwischen diesen aus (bspw. aufgrund eines Load-Balancings oder einer redundanten Speicherung), so muss die Übertragung sicher durchgeführt werden.
- **Datentransfer zwischen „Cloud-Federations“.** Werden Cloud-Infrastrukturen unterschiedlicher Cloud-Anbieter zusammengeschlossen, was als „Cloud-Federation“ bezeichnet wird, so findet ein definierter Datenaustausch zwischen den jeweiligen Cloud-Infrastrukturen statt und muss entsprechend gesichert werden.⁶⁹
- **Datentransfer an Zwischenstellen.** Es ist möglich, dass Daten an Zwischenstellen wie bspw. Content-Delivery-Networks (CDN) übertragen werden. So bietet u.a. Amazon mit „CloudFront“ ein CDN an, um Inhalte und Anwendungen schneller und effizienter bereitstellen zu können. Bei der Nutzung von Zwischenstellen ist auf einen sicheren Datentransfer zu achten.

Zur Dienstbringung kann es auch notwendig sein, personenbezogene Daten an Dritte weiterzugeben. Hierbei können verschiedene Szenarien denkbar sein, wie bspw. die Weitergabe an Subauftragsverarbeiter, die zur Dienstbringung unabdinglich sind, die Weitergabe von Daten als Beweismittel an Ermittlungsbehörden oder an weitere Dritte. Der Cloud-Anbieter sollte geeignete TOM implementieren, die sicherstellen, dass durch Voreinstellung und somit ohne aktive Nutzerzustimmung grundsätzlich keine personenbezogenen Daten weitergegeben werden. Insbesondere bei der Strafverfolgung können Cloud-Anbieter dazu verpflichtet werden, bspw. eine forensische Datenanalyse mit der Weitergabe der Nutzerdaten zu unterstützen.⁷⁰ Die Durchführung einer Datenweitergabe muss nicht in der Verantwortlichkeit eines Cloud-Anbieters liegen. Sie ist abhängig vom jeweiligen Service-Modell sowie der Gestaltung des Cloud-Dienstes und der individuellen Auftragsverarbeitungsvereinbarung mit dem Cloud-Nutzer.

Wesentliche Datenweitergabevorgänge bei Cloud-Diensten sind:

- **Weitergabe an Subauftragsverarbeiter zur Dienstbringung.** Sind Subauftragsverarbeiter in die Dienstbringung involviert, so können personenbezogene Daten an diese weitergegeben werden, um den Verarbeitungsvorgang durchführen zu können.
- **Weitergabe an autorisierte Nutzer.** Nach Zustimmung des Cloud-Nutzers können erhobene Daten an autorisierte Nutzer des Cloud-Dienstes weitergegeben werden, bspw. das Teilen von Dokumenten mit anderen Nutzern.
- **Weitergabe an Dritte.** Nach Zustimmung der betroffenen Person können Daten auch an Dritte, bspw. zu Werbezwecken weitergegeben werden.
- **Weitergabe an (Ermittlungs-)Behörden.** Unter Umständen können Daten auf richterliche Anweisung an Strafverfolgungsbehörden oder andere Behörden weitergegeben werden.

⁶⁷ Jäger et al. 2016.

⁶⁸ Jäger et al. 2016.

⁶⁹ Massonet et al. 2011.

⁷⁰ Fernandes et al. 2014.

2.3.4 Speicherung

Wurden die Daten übertragen, kann eine Vielzahl von Vorgängen angestoßen werden, welche im Folgenden weiter betrachtet werden.

Vorbereitung der Datenspeicherung

Zur Vorbereitung der Datenspeicherung können verschiedene Vorgänge durchgeführt werden. So sollte gemäß dem Grundsatz der Datensparsamkeit nach der Erhebung oder Erzeugung von Daten geprüft werden, ob die personenbezogenen Daten (langfristig) gespeichert werden müssen.⁷¹ Eine Auswahl von Daten für die Speicherung reduziert das Speichervolumen und entsprechende Kosten, und kann ggf. mögliche Risiken bei der Speicherung sensibler Daten reduzieren. Eine Festlegung von flüchtigen (bspw. DRAM) und nicht-flüchtigen Speichern (bspw. HDD) zur Datenspeicherung könnte getroffen werden.

Darüber hinaus können Meta-Daten (bspw. Datenformat, Datenspeicherort oder Restriktionen und Anforderungen an die Daten) definiert und hinterlegt werden.⁷² Auch eine Indexierung der Daten wäre denkbar, um die Daten zukünftig besser auffinden und verwenden zu können.⁷³ Zudem können Maßnahmen durchgeführt werden, welche sicherstellen, dass gespeicherte Daten ein hohes Maß an Authentizität, Verlässlichkeit, Nutzbarkeit, Langlebigkeit, Richtigkeit und Integrität aufweisen.⁷⁴

Die Durchführung von Datenvorbereitungsvorgängen muss nicht in der Verantwortlichkeit eines Cloud-Anbieters liegen. Sie ist abhängig vom jeweiligen Service-Modell sowie der Gestaltung des Cloud-Dienstes und der individuellen Auftragsverarbeitungsvereinbarung mit dem Cloud-Nutzer.

Wesentliche Datenvorbereitungsvorgänge bei Cloud-Diensten sind:

- **Filterung / Selektion.** Der Cloud-Dienst analysiert zu speichernde Daten und trifft eine Auswahl von tatsächlich gespeicherten Daten basierend auf definierten Kriterien, um den Anforderungen des AUDITOR-Kriterienkatalogs gerecht zu werden, oder gemäß der Weisung des Cloud-Nutzers. Verworfenen Daten werden in flüchtigen Datenspeichern zwischengespeichert oder sicher gelöscht.
- **Generierung von Meta-Daten zur Speicherung.** Der Cloud-Dienst generiert (automatisch) Meta-Daten, die bei der Speicherung notwendig sind, bspw. Festlegung des Standorts der Speicherung, Größe der Daten, Zugriffsrechte oder Backup-Intervalle.

Durchführung der Datenspeicherung

Die personenbezogenen Daten werden auf ein geeignetes Speichermedium gemäß der Sicherheitsanforderungen persistiert.⁷⁵ Je nach Architektur des Cloud-Dienstes können unterschiedliche Datenbanken und Speichertechnologien eingesetzt werden. Zudem werden verschiedene Vorgänge durchgeführt, die bei der Speicherung unterstützen, darunter bspw. die Datenpartitionierung. Die Durchführung einer Datenspeicherung muss nicht in der Verantwortlichkeit eines Cloud-Anbieters liegen. Sie ist abhängig vom jeweiligen Service-Modell sowie der Gestaltung des Cloud-Dienstes und der individuellen Auftragsverarbeitungsvereinbarung mit dem Cloud-Nutzer.

Wesentliche Datenspeicherungsvorgänge bei Cloud-Diensten sind:

- **Datenindexierung.** Den Daten wird zum schnelleren Wiederauffinden ein Index gemäß definierter Indexstrukturen zugewiesen.
- **Datenspeicherung auf relationalen Datenbanken.** Die Daten werden in relationalen Datenbanken (bspw. MySQL, PostgreSQL, SQL Server Oracle) dauerhaft gespeichert.
- **Datenspeicherung auf NoSQL-Datenbanken.** Um eine erhöhte Flexibilität und Skalierbarkeit zu erreichen, können Daten in NoSQL-Datenbanken (bspw. Apache Cassandra, CouchDB, MongoDB) persistiert werden.
- **Logische Zuordnung von Daten.** Zur Sicherstellung einer Mandantentrennung können logische Speicherbereiche definiert werden.⁷⁶

⁷¹ Higgins 2012.

⁷² Higgins 2008; Burton und Treloar 2009; Curtin 2010.

⁷³ Burton und Treloar 2009)

⁷⁴ Higgins 2008, 2012.

⁷⁵ Higgins 2008.

⁷⁶ Jäger et al. 2016.

- **Datenpartitionierung.** Der Cloud-Dienst teilt die zu speichernden Datenpakete auf, um sie effizienter verwalten zu können.⁷⁷
- **Datenreplizierung.** Datenreplizierung beschreibt die Kopie von Daten, um einen parallelen Zugriff auf diese zu ermöglichen.⁷⁸ Hierbei muss ein Managementsystem durch Synchronisationsvorgänge sicherstellen, dass Änderungen an den Daten auf allen Kopien durchgeführt werden.

Datensicherung (Backup)

Um die Verfügbarkeit von gespeicherten Daten sicherzustellen, sollte von erhobenen Daten eine Kopie (engl. Backup) erstellt werden. Backups dienen zur Wiederherstellung von Dateien, falls diese u.a. manipuliert oder zerstört wurden. Eine redundante Datenspeicherung ist zudem auch insbesondere im Sinne von Disaster-Recovery-Maßnahmen von Cloud-Diensten relevant.⁷⁹ Die Durchführung einer Datensicherung muss nicht in der Verantwortlichkeit eines Cloud-Anbieters liegen. Sie ist abhängig vom jeweiligen Service-Modell sowie der Gestaltung des Cloud-Dienstes und der individuellen Auftragsverarbeitungsvereinbarung mit dem Cloud-Nutzer.

Wesentliche Datensicherungsvorgänge bei Cloud-Diensten sind:

- **Erstellung von Backups.** Daten werden redundant gespeichert, um ihre Verfügbarkeit und Ausfallsicherheit zu erhöhen. Bei Cloud-Diensten werden Backups meist auf unterschiedlichen Speicherorten hinterlegt.
- **Erstellung von Snapshots.** Ein Snapshot umfasst eine abgespeicherte Momentaufnahme bspw. eines Systems oder einer Datenbank. Sie unterstützen oder ermöglichen eine Datenwiederherstellung. Beim Herstellen von Snapshots in virtuellen Maschinen können allerdings unter Umständen Daten, die in lokalen Datenbanken oder Monitoringsystemen persistiert wurden, versehentlich gelöscht werden.⁸⁰
- **Datenwiederherstellung.** Fehlerhafte, manipulierte oder gelöschte Daten werden durch die Verwendung von Backups oder replizierten Daten wiederhergestellt und stehen dem Nutzer im Anschluss wieder zur Verfügung.

Datenarchivierung

Ferner können Daten archiviert werden. Datenarchive bewahren langfristig ältere Datenoriginalen auf, die für den täglichen Betrieb nicht mehr relevant sind, jedoch gelegentlich benötigt werden. Datenarchive sind meist indiziert und mit einer Suchfunktion versehen, um Daten ganz oder teilweise wieder abrufen zu können. Die Durchführung einer Datenarchivierung muss nicht in der Verantwortlichkeit eines Cloud-Anbieters liegen. Sie ist abhängig vom jeweiligen Service-Modell sowie der Gestaltung des Cloud-Dienstes und der individuellen Auftragsverarbeitungsvereinbarung mit dem Cloud-Nutzer.

Wesentliche Datenarchivierungsvorgänge bei Cloud-Diensten sind:

- **Prüfung auf Archivierbarkeit.** Prozess, bei dem die Daten fortlaufend hinsichtlich der definierten Archivierungskriterien überprüft werden, die eine Archivierung veranlassen. So können Daten, die über einen längeren Zeitraum ungenutzt bleiben, archiviert werden.
- **Daten aus der Datenbank ins Archiv schreiben.** Ist die Prüfung auf Archivierbarkeit erfolgreich, werden Daten in das Archiv verschoben und der bisherige Speicherplatz wird freigegeben.
- **Zugriff auf Daten im Archiv.** Der Zugriff auf Archivdaten kann notwendig werden.
- **Daten aus dem Archiv löschen.** Eine Archivierung über mehrere Jahre führt zu einer immensen Datenmenge, die durch Löschvorgänge gemäß definierter Aufbewahrungsfristen unter Kontrolle gebracht werden sollte.

Migration von gespeicherten Daten

Der Begriff der Datenmigration ist vielschichtig. Zum einen umfasst die Datenmigration die Umstellung der Datenformate, die sich bspw. aufgrund der Änderung zugrundeliegender Technologien, Software oder Hardware ergeben.⁸¹ Zum anderen beschreibt die Datenmigration den Vorgang, den Speicherort von Daten zu verändern.⁸² Insbesondere im Cloud Computing-Umfeld ist der Speicher- und Verarbeitungsort von (personenbezogenen) Daten flexibel und kann meist ohne großen Aufwand verändert werden, bspw. aus Gründen des Lastenausgleichs, der Verfügbarkeit von (redundanten) Datenzentren oder

⁷⁷ Zhao et al. 2014.

⁷⁸ Sun et al. 2012.

⁷⁹ Ofner et al. 2013.

⁸⁰ Pearce et al. 2013.

⁸¹ Higgins 2008.

⁸² Michener und Jones 2012; Alatorre et al. 2014.

flexiblen Speicherkosten.⁸³ Aus diesem Grund müssen geeignete Regelwerke für die Migration von (personenbezogenen) Daten innerhalb der Cloud-Infrastruktur festgelegt werden. Die Durchführung einer Datenmigration muss nicht in der Verantwortlichkeit eines Cloud-Anbieters liegen, abhängig vom jeweiligen Service-Modell sowie der Gestaltung des Cloud-Dienstes und der individuellen Auftragsverarbeitungsvereinbarung mit dem Cloud-Nutzer.

Wesentliche Datenmigrationsvorgänge bei Cloud-Diensten sind:

- **Veränderung des Datenspeicherungsorts.** Im Rahmen eines Load-Balancings, eines Ausfalls oder aus anderen Gründen kann ein Cloud-Dienst den Speicherort von Daten verändern und die Daten somit in ein anderes Rechenzentrum migrieren.
- **Veränderung des Datenformats.** Bei Änderung zugrundeliegender Technologien, Software, Hardware oder Datenmodellen kann es dazu kommen, dass Datenformate angepasst werden müssen. Bei der Veränderung von Datenformaten können auch personenbezogene Daten verarbeitet werden. Bspw. kann es notwendig sein, dass personenbezogene Daten in einem JSON-Format umgewandelt und in einem XML-Format gespeichert werden.

2.3.5 Zugriff und Verwendung

Ein weiterer zentraler Vorgang ist der lesende Zugriff auf die Daten. Hierbei kann bspw. der Zugriff durch einen Cloud-Dienst-Nutzer auf seine eigenen Daten vom Zugriff durch den Cloud-Anbieter zur weiteren Verarbeitung der Daten unterschieden werden. Um den Zugriff auf personenbezogene Daten sicherzustellen, sind entsprechende Identity- und Access-Managementsysteme und -Regelwerke erforderlich.⁸⁴ Das Management des Datenzugriffs muss nicht in der Verantwortlichkeit eines Cloud-Anbieters liegen. Es ist abhängig vom jeweiligen Service-Modell sowie der Gestaltung des Cloud-Dienstes und der individuellen Auftragsverarbeitungsvereinbarung mit dem Cloud-Nutzer.

Wesentliche Datenzugriffsvorgänge bei Cloud-Diensten sind:

- **Zugriffsprüfung.** Bevor ein Zugriff auf Daten gewährt werden kann, müssen etwaige Identifizierungs-, Autorisierungs- und Authentifizierungsvorgänge durchlaufen werden. Im Rahmen dieser Prüfung werden eingegebene personenbezogene Daten mit den im System hinterlegten abgeglichen.
- **Auffindung der Daten.** Zur Auffindung der angefragten Daten können Suchvorgänge durchgeführt werden, die ggf. auf eine Vielzahl von personenbezogenen Daten zugreifen, bevor das angefragte Datum gefunden wurde.
- **Lesender Zugriff durch den Cloud-Nutzer.** Der Cloud-Nutzer oder eine durch ihn befugte Person initiiert den Zugriff auf seine Daten, die im Anschluss durch den Cloud-Dienst angezeigt oder bereitgestellt werden (bspw. über eine Schnittstelle).
- **(Automatischer) lesender Zugriff durch den Cloud-Dienst zur Durchführung des Verarbeitungsvorgangs.** Ein Cloud-Dienst kann im Rahmen des primären Verarbeitungsvorgangs auf die Daten zugreifen, um diese bspw. auszulesen und im Anschluss zur Verarbeitung zu verwenden.
- **(Automatischer,) lesender Zugriff durch den Cloud-Dienst zur Durchführung weiterer Vorgänge.** Ein Cloud-Dienst kann zudem auf personenbezogene Daten zugreifen, um sekundäre oder unterstützende Vorgänge durchzuführen. Dazu gehören u.a. Monitoring- oder interne Auditierungsvorgänge.
- **(Manueller) Zugriff durch Mitarbeiter des Cloud-Anbieters.** Mitarbeiter des Cloud-Anbieters können bspw. im Rahmen von Support-Aktivitäten einen lesenden Zugriff auf personenbezogene Daten haben.
- **Lesender Zugriff durch Dritte.** Nach Zustimmung des Cloud-Nutzers können Daten auch von Dritten abgerufen und verwendet werden, bspw. durch definierte Schnittstellen in einer Anwendung.

2.3.6 Veränderung im Rahmen der Verarbeitung

Neben dem bloß lesenden Zugriff auf die personenbezogenen Daten können diese bspw. aufgrund von Nutzeraktionen oder Verarbeitungsergebnissen verändert oder aktualisiert werden. Es handelt sich hierbei somit nicht um einen lesenden, sondern einen schreibenden Vorgang, der die bestehenden Daten aktiv verändert.⁸⁵ Das Management von Datenveränderungen muss nicht in der Verantwortlichkeit eines

⁸³ Alatorre et al. 2014.

⁸⁴ Higgins 2008.

⁸⁵ Möller 2013; Higgins 2008.

Cloud-Anbieters liegen. Es ist abhängig vom jeweiligen Service-Modell sowie der Gestaltung des Cloud-Dienstes und der individuellen Auftragsverarbeitungsvereinbarung mit dem Cloud-Nutzer.

Wesentliche Datenveränderungen bei Cloud-Diensten sind:

- **Veränderungen durch den Cloud-Nutzer.** Der Cloud-Nutzer oder eine durch ihn autorisierte Person verändert oder aktualisiert personenbezogenen Daten, bspw. im Rahmen einer Adressänderung.
- **(Automatische) Veränderungen durch den Cloud-Dienst.** In der Cloud gespeicherte Daten können im Rahmen von Verarbeitungsprozessen durch den Cloud-Dienst geändert werden, bspw. die Veränderung der Standortdaten eines Benutzers.
- **(Manuelle) Veränderungen durch Mitarbeiter des Cloud-Anbieters.** Mitarbeiter des Cloud-Anbieters können theoretisch eine Veränderung an den Daten durchführen, bspw. im Rahmen von Support-Aktivitäten.
- **Veränderungen durch Dritte.** Dritte können die Daten verarbeiten, sofern eine Rechtsgrundlage hierfür vorliegt, z.B. Einwilligung der betroffenen Person.

2.3.7 Transformation

Neben der Veränderung von personenbezogenen Daten im Rahmen der eigentlichen Verarbeitung können diese auch zweckgerichtet durch Sekundär- oder Unterstützungsprozesse transformiert werden. Dazu zählen bspw. Transformationsvorgänge wie Filterung, Harmonisierung, Synthese, Aggregation und Anreicherung. Eine wichtige Rolle nehmen aber vor allem Transformationen zum Schutz der Daten ein. Darunter zählen insbesondere Verschlüsselungs-, Pseudonymisierungs- und Anonymisierungsvorgänge. Die Durchführung von Datentransformationen muss nicht in der Verantwortlichkeit eines Cloud-Anbieters liegen, abhängig vom jeweiligen Service-Modell sowie der Gestaltung des Cloud-Dienstes und der individuellen Auftragsverarbeitungsvereinbarung mit dem Cloud-Nutzer.

Wesentliche Datentransformationen bei Cloud-Diensten sind:

- **Datenbereinigung.** Eine Datenbereinigung kann durchgeführt werden, um bspw. Datenfehler in Datenbanken zu korrigieren oder zu entfernen. Die Fehler können bspw. aus falschen, veralteten oder inkonsistenten Daten resultieren.
- **Datensortierung.** Daten können in eine Reihenfolge gemäß definierter Kriterien gebracht werden.
- **Datenmapping.** Abbildung und Transformation von Daten zwischen unterschiedlichen Datenmodellen.
- **Datenkonvertierung.** Eine Datenkonvertierung beschreibt die Veränderung des Datenformats und umfasst bspw. das Ändern des gewählten Zeichenformats von UTF-8 auf UTF-16.
- **Aggregation.** Die Aggregation beschreibt die Zusammenfassung von Daten, bspw. die Summenbildung.
- **Integration.** Daten werden aus unterschiedlichen Quellen zu einem Datensatz zusammengeführt.
- **Verknüpfung.** Die logische Verknüpfung von Daten stellt eine Beziehung zwischen Daten aus unterschiedlichen Quellen her.
- **Verschlüsselung.** Ein Klartext wird mittels eines Schlüssels und einem Verschlüsselungsalgorithmus in einen verschlüsselten Text („Geheimtext“) umgewandelt.
- **Anonymisierung.** Die Anonymisierung ist das Verändern personenbezogener Daten derart, dass diese nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitseinsatz einer bestimmten oder bestimmbarer natürlichen Person zugeordnet werden können.
- **Pseudonymisierung.** Gemäß Art. 4 Nr. 5 DSGVO bezeichnet die Pseudonymisierung die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.

2.3.8 Administration

Ferner können Vorgänge zur Verwaltung der Daten etabliert werden. Hierzu zählen bspw. qualitätssichernde Maßnahmen, die (manuell) durchgeführt werden und eine hohe Datenqualität sicherstellen,⁸⁶ oder administrative Tätigkeiten aufgrund von Weisungen des Cloud-Nutzers. Es müssen Richtlinien geschaffen werden, welche die Administration von Daten festlegen.⁸⁷ Besonders im Kontext von Cloud-Diensten sind administrative Vorgänge von hoher Relevanz, da bspw. ein Administrator durch einen Fehler bei der Migration von Daten oder bei dem Erstellen von Backups einen Datenverlust verursachen kann.⁸⁸ Die Administration von Daten muss nicht in der Verantwortlichkeit eines Cloud-Anbieters liegen, abhängig vom jeweiligen Service-Modell sowie der Gestaltung des Cloud-Dienstes und der individuellen Auftragsverarbeitungsvereinbarung mit dem Cloud-Nutzer.

- **Administration von Anwendungs-, Nutzungs-, oder Bestandsdaten.** Aufgrund von Support-Anfragen von Cloud-Nutzern können Administratoren des Cloud-Anbieters Daten administrieren, bspw. das Wiederherstellen von Daten oder Starten von virtuellen Maschinen.
- **Administration von Meta-Daten.** Im Rahmen des Monitorings werden Meta-Daten des Cloud-Dienstes und Nutzungsdaten von Administratoren ausgewertet, um den laufenden Betrieb zu optimieren.
- **Überprüfung / Verfolgung von Datenbewegungen.** Zur Sicherstellung der Datenlokalitätsanforderungen können automatisierte oder manuelle Prozesse zur Durchsicht und Analyse von Data Traces durchgeführt werden.
- **Datenvvalidierung.** Es können automatisierte oder manuelle Vorgänge zur Überprüfung der Richtigkeit von personenbezogenen Daten durchgeführt werden, bspw. die Überprüfung, ob die eingetragene Postleitzahl mit dem Ort übereinstimmt.
- **Identifikation von Datenanomalien.** Zur Sicherung der Datenqualität können automatisierte oder manuelle Administrationsvorgänge durchgeführt werden, die bspw. Schreib-Lese-Konflikte, Dateninkonsistenzen, Insertion-, Update- und Delete-Anomalien identifizieren und auflösen.
- **Korrektur von Daten.** Eine administrative Korrektur von Daten kann durchgeführt werden, um bspw. Datenfehler in Datenbanken zu korrigieren oder zu entfernen. Die Fehler können bspw. aus falschen, veralteten oder inkonsistenten Daten resultieren.

2.3.9 Rückgabe der Daten

Zum Ende der Vertragslaufzeit der Auftragsverarbeitung oder bei Aufforderung des Cloud-Nutzers können Vorgänge initiiert werden, die eine (vollständige) Rückgabe der Daten durchführen. Dies wird auch als Backsourcing verstanden. Insbesondere im Cloud Computing-Umfeld ist daher bei Rückgabevorgängen die Portabilität der Daten entscheidend. So ist gefordert, dass die Übermittlung von personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format möglich sein sollte. Das Management zur Rückgabe von Daten muss nicht in der Verantwortlichkeit eines Cloud-Anbieters liegen. Es ist abhängig vom jeweiligen Service-Modell sowie der Gestaltung des Cloud-Dienstes und der individuellen Auftragsverarbeitungsvereinbarung mit dem Cloud-Nutzer.

- **Automatisierter Datenexport.** Der Cloud-Dienst ermittelt automatisch alle relevanten Datensätze und transformiert diese in ein definiertes Format (bspw. XML, CSV oder JSON), sodass die Datensätze über eine Export-Schnittstelle (bspw. API oder Dateidownload) exportiert werden können.
- **Manueller Datenexport.** Ein Administrator extrahiert alle Daten und überträgt oder übergibt sie an den Cloud-Nutzer.

2.3.10 Löschung / Vernichtung

Der letzte Schritt der Datenverarbeitung stellt die endgültige Löschung von personenbezogenen Daten dar.⁸⁹ Diese kann insbesondere dann durchgeführt werden, wenn der Cloud-Nutzer dies verlangt. In Bezug auf Cloud-Dienste ist insbesondere anzumerken, dass eine dauerhafte und vollständige Löschung u.a. aufgrund der Multi-Mandanten-Architektur, Ressourcenbündelung, Datenredundanzen und der verteilten Systeme besonderer Aufmerksamkeit bedarf.⁹⁰ Eine abschließende, physische Vernichtung von Speichermedien kann unter Umständen erforderlich sein. Die Durchführung einer Datenlö-

⁸⁶ van Veenstra und van den Broek 2015; Michener und Jones 2012.

⁸⁷ Ofner et al. 2013.

⁸⁸ Fernandes et al. 2014.

⁸⁹ Higgins 2008; Bernard 2007.

⁹⁰ Pearson und Benameur 2010.

schung muss nicht in der Verantwortlichkeit eines Cloud-Anbieters liegen. Sie ist abhängig vom jeweiligen Service-Modell sowie der Gestaltung des Cloud-Dienstes und der individuellen Auftragsverarbeitungsvereinbarung mit dem Cloud-Nutzer.

- **Datenlöschung (engl. clear).** Die Datenlöschung umfasst alle logischen Techniken zur Löschung von allen Speichermedien mit personenbezogenen Daten. Hierbei werden meist simple Techniken angewendet, wie das iterative Beschreiben des Mediums mit einer Reihenfolge von 0 und 1. Die Datenlöschung ist nur gegen simple und nicht-invasive Datenwiederherstellungsmethoden effektiv.
- **Datensäuberung (engl. purge, erasure).** Die Datensäuberung umfasst physische oder logische State-of-the-Art Techniken, die eine Datenwiederherstellung unmöglich machen. Nur diese Form entspricht der von Art. 17 DSGVO geforderten Löschung.⁹¹
- **Datenvernichtung (engl. destroy).** Die Datenvernichtung umfasst die physische Zerstörung des Speichermediums, sodass dieses nicht weiterverwendet werden kann. Hierzu zählt bspw. die Einschmelzung des Speichermediums.

Zu unterscheiden ist außerdem:

- **Löschung von Primärdaten.** Es sollten alle primären Daten des Cloud-Nutzers gelöscht werden, hierzu zählen u.a. Anwendungsdaten, welche zur Datenverarbeitung benötigt werden.
- **Löschung von Sekundärdaten.** Es sollten zudem alle weiteren Daten des Cloud-Nutzers gelöscht werden, hierzu zählen insbesondere Backups, Replikationen oder Meta-Daten.

⁹¹ Roßnagel 2019, Art. 4 Nr. 2 DSGVO, Rn. 30.

C. Zertifizierungsreichweite und Verantwortlichkeiten

Bei der Zertifizierung nach AUDITOR müssen die Zertifizierungsreichweite und der Anwendungsbereich klar abgegrenzt werden. Wichtig sind hierbei die Identifikation und Abgrenzung von Verantwortlichkeiten des Cloud-Anbieters von Cloud-Nutzern und Subauftragsverarbeitern.

1. Schichtenmodell zur Abgrenzung von Verantwortlichkeiten

1.1. Schichtenmodell

Im Cloud Computing wird vor allem von einem verschachtelten Wertschöpfungsnetzwerk ausgegangen, das als Schichtenarchitektur verstanden wird („Cloud-Stack“). Diese Schichtenarchitektur spiegelt auch die verschiedenen Service-Modelle des Cloud Computing wider. Basierend auf dem Cloud-Stack können die Einflussmöglichkeiten für den Cloud-Anbieter und -Nutzer sowie für mögliche Subauftragsverarbeiter festgelegt werden. Tabelle 3 stellt die Einflussmöglichkeiten schematisch dar. Hierbei kann es in der Praxis zu Abweichungen je nach Architektur des Cloud-Dienstes kommen. Ein Cloud-Service ist zudem nicht singulär auf eine definierte Betriebsumgebung oder Schicht einzuschränken. Die Schichten können sich auf allen Ebenen beliebig aufspreizen und im Sinne der vernetzten Dienststruktur parallel durch rechtlich eigenständige Subauftragsverarbeiter betrieben werden. So können gleichzeitig verschiedene Akteure und eine Kombination von Akteuren (bspw. Cloud-Anbieter und Subauftragsverarbeiter) verantwortlich für die Plattformensicherheit sein.

Akteur	IaaS	PaaS	SaaS	Beschreibung der Schicht
Cloud-Nutzer	Sichere Anwendungsnutzung	Sichere Anwendungsnutzung	Sichere Anwendungsnutzung	Der Cloud-Nutzer ist für eine sichere Nutzung der Anwendung verantwortlich.
	Nutzerspezifika	Nutzerspezifika	Nutzerspezifika	Nutzerindividuelle Einstellungen oder Konfigurationen von genutzten Anwendungen.
	Anwendung	Anwendung	Anwendung	Angebotene Softwarelösungen.
	Softwaresicherheit	Softwaresicherheit	Softwaresicherheit	Mechanismen zur Erhöhung der Sicherheit von angebotenen Anwendungen.
	Administration und Support der Software	Administration und Support der Software	Administration und Support der Software	Administration der angebotenen Software sowie Entgegennahme und Behandlung von Support-Anfragen durch den Cloud-Nutzer.
	Betriebssystem	Betriebssystem	Betriebssystem	Grundlegende Software zum Betrieb von Anwendungen.
	Laufzeitumgebung	Laufzeitumgebung	Laufzeitumgebung	Die Laufzeitumgebung führt Applikationen aus, für welche die Laufzeitumgebung geeignet ist.
	Datenbank	Datenbank	Datenbank	Software zur Verwaltung und Strukturierung von Daten.
	Plattformsicherheit	Plattformsicherheit	Plattformsicherheit	Mechanismen zur Erhöhung der Sicherheit von angebotenen Plattformen.
	Administration und Support der Plattform	Administration und Support der Plattform	Administration und Support der Plattform	Administration der angebotenen Plattform sowie Entgegennahme und Behandlung von Support-Anfragen durch den Cloud-Nutzer.
Cloud-Anbieter	Virtuelle Maschinen	Virtuelle Maschinen	Virtuelle Maschinen	Virtuelle Repräsentation von Rechnerressourcen wie bspw. Server oder CPUs.
	Virtualisierungsschicht	Virtualisierungsschicht	Virtualisierungsschicht	Mechanismen zur Erstellung und Verwaltung von Virtuellen Maschinen.
	Berechnungskomponenten	Berechnungskomponenten	Berechnungskomponenten	Komponenten zur Durchführung von Berechnungen oder Verarbeitung von Daten im Cloud-Dienst.
	Speicher	Speicher	Speicher	Mechanismen zur Speicherung von Daten.
	Netzwerk	Netzwerk	Netzwerk	Mechanismen zum Transport von Daten.
	Infrastruktursicherheit	Infrastruktursicherheit	Infrastruktursicherheit	Mechanismen zur Erhöhung der Sicherheit von angebotenen Ressourcen.
	Administration und Support für die Infrastruktur	Administration und Support für die Infrastruktur	Administration und Support für die Infrastruktur	Administration der angebotenen Infrastruktur sowie Entgegennahme und Behandlung von Support-Anfragen durch den Cloud-Nutzer.
	Hardware			Die physische Hardware zur Erbringung des Cloud-Dienstes.
	Gebäude, Einrichtung und Equipment			Die physische Einrichtung des Cloud-Dienstes.
	Konnektivität- und Netzanbindung			Die physische Konnektivität des Rechenzentrums.
Rechenzentrumsicherheit			Mechanismen zur Erhöhung der Sicherheit des Rechenzentrums, darunter Gebäudeverantwortliche mit Wachpersonal und physische Sicherungssysteme.	

Tabelle 3. Einflussmöglichkeiten nach dem Schichtenmodell.⁹²

Bei der Nutzung eines SaaS-Dienstes hat der Cloud-Nutzer im Allgemeinen keine technischen Änderungsmöglichkeiten beim Cloud-Dienst. Es ist lediglich möglich, dass ein Cloud-Nutzer gewisse Konfigurationen oder Einstellungen bei bezogenen Cloud-Anwendungen durchführen kann, bspw. wie das Ein- und Ausschalten gewisser Funktionalitäten oder das Anpassen von grafischen Benutzeroberflä-

⁹² Adaptiert von Singh et al. 2016; European Network and Security Agency 2012.

chen. Zudem sei anzumerken, dass der Cloud-Nutzer dafür Sorge zu tragen hat, dass die Cloud-Anwendung sicher und konform genutzt wird. Zum Kerngeschäft des SaaS-Anbieters gehören die Entwicklung, der Betrieb und die Administration der Softwareanwendung sowie die Sicherstellung der Softwaresicherheit. Die verbleibenden Cloud-Schichten obliegen der Verantwortung des SaaS-Cloud-Anbieters (Full-Stack-Anbieter) oder werden an einen Subauftragsverarbeiter ausgelagert.

Im Falle eines PaaS-Dienstes betreibt ein Cloud-Nutzer eigene Anwendungen auf einer angebotenen Cloud-Plattform. Somit ist der Cloud-Nutzer für die Erstellung und den Betrieb der Anwendungen verantwortlich. Zudem muss der Cloud-Nutzer die Sicherheit der Anwendung verantworten, um bspw. Cross-Site-Scripting oder Softwareschwachstellen zu verhindern. Zum Kerngeschäft des PaaS-Anbieters gehören die Entwicklung, der Betrieb und die Administration der Plattform (bspw. der angebotenen Betriebssysteme oder Datenbanken) sowie die Sicherstellung der Plattformsicherheit. Die verbleibenden Cloud-Schichten obliegen der Verantwortung des PaaS-Cloud-Anbieters (Full-Stack-Anbieter) oder werden an einen Subauftragsverarbeiter ausgelagert.

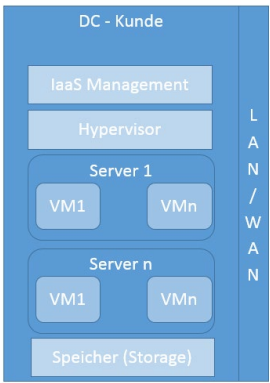
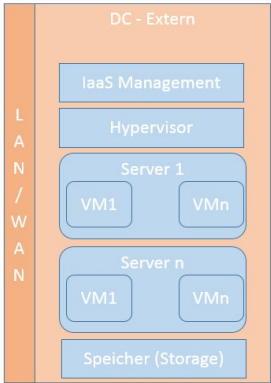
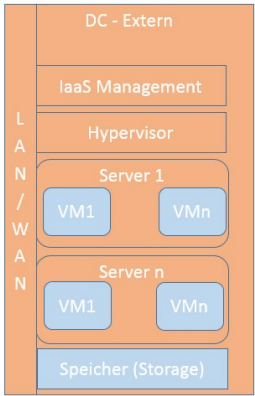
Beim Angebot eines IaaS-Dienstes ist der Cloud-Anbieter für die korrekte und sichere Virtualisierung und die Bereitstellung der notwendigen physischen Ressourcen zuständig. Ein Cloud-Nutzer trägt die Verantwortung für angemietete virtuelle Maschinen oder Container und darauf ausgeführte Anwendungen, Datenbanken, Betriebssysteme und Laufzeitumgebungen. Zudem übernimmt der Cloud-Nutzer die Verantwortung für die Software- und Plattformsicherheit. Die notwendige physische Hardware, Einrichtungen und Equipment können durch einen IaaS-Anbieter bereitgestellt werden (Full-Stack-Anbieter) oder bei einem Rechenzentrum eines Subauftragsverarbeiters bezogen werden. Abhängig von der Ausgestaltung des Cloud-Services sowie den Auftragsverarbeitungsvereinbarungen mit Cloud-Nutzern kann es zu abweichenden Verantwortlichkeiten kommen.

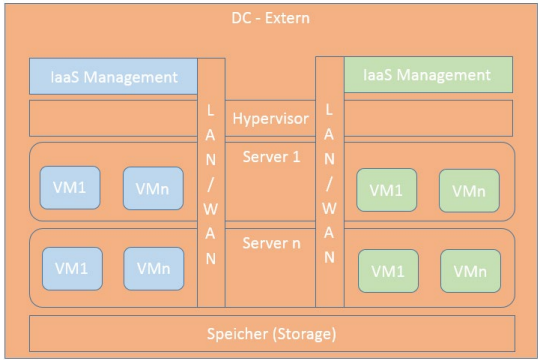
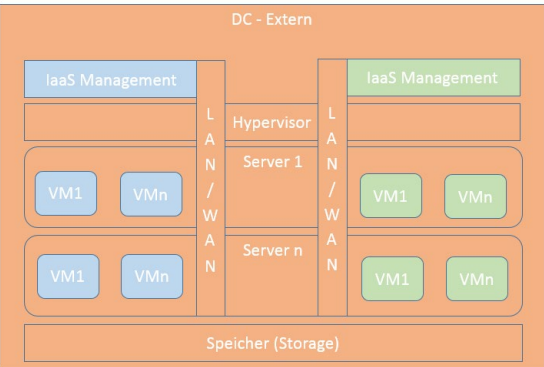
Als weiterführende Literatur sei auf die NIST „*Cloud Security Reference Architecture*“ verwiesen, die im Anhang D eine detaillierte Betrachtung der Einflussmöglichkeiten für die verschiedenen Service-Modelle auflistet.⁹³

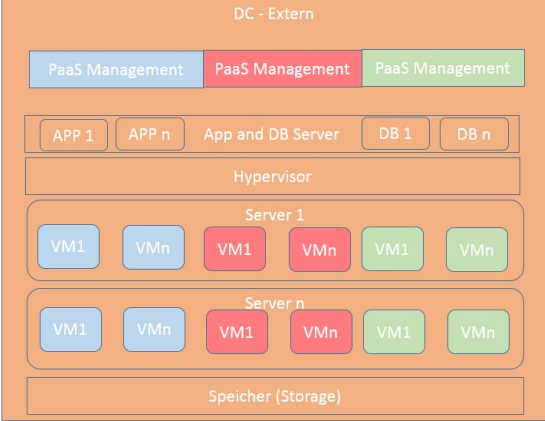
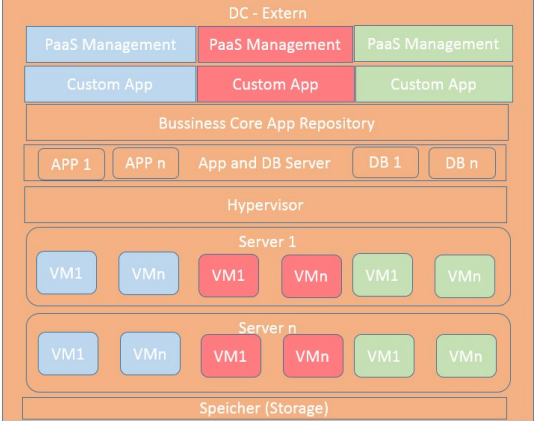
⁹³ NIST Cloud Computing Security Working Group 2013.

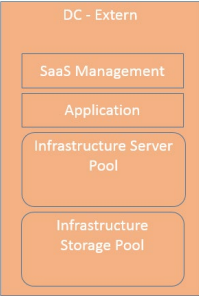
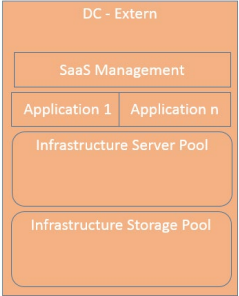
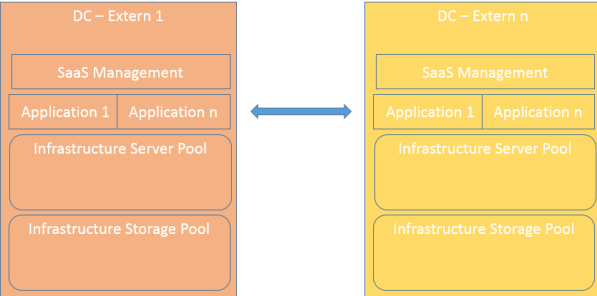
1.2. Beispiele

Die folgende Betrachtung beschreibt verschiedene Service-Modelle in Kombination mit Bereitstellungsmodellen. Hierbei ist besonders die Konstellation mit einem bis mehreren externen Cloud-Anbietern im Rahmen der Dienstbringung zu berücksichtigen. Durch farbliche Markierung werden die jeweiligen Verantwortlichkeitsbereiche des Cloud-Nutzers und -Anbieters illustriert.

Private Cloud – On Premise	Private Cloud – External Hosted	Private Cloud – External Managed
<p>Bei der Private Cloud On Premise wird angenommen, dass die gesamte technische Infrastruktur der uneingeschränkten und unmittelbaren Verfügung des Cloud-Nutzers unterliegt.</p> 	<p>Bei der Private Cloud External Hosted erfolgt die Bereitstellung der technischen Umgebungsstruktur durch einen Cloud-Anbieter (DC CoLocation, WAN, IX), die IT Systeme (Server, Storage, Local Switch, LAN) gehören dagegen dem Cloud-Nutzer. Üblicherweise werden mit dem Cloud-Anbieter zusätzliche Dienstleistungen (Hands On Services, Zutrittskontrollsysteme, Systemüberwachung) vereinbart.</p> 	<p>Ergänzend zur Private Cloud External Hosted wird die technische Betreuung der Systeme mit direktem System- und Datenzugriff durch den Cloud-Anbieter übernommen.</p> 
<p><i>* Blau: Im primären Verantwortungsbereich des Cloud-Nutzers</i> <i>Orange: Im primären Verantwortungsbereich des Cloud-Anbieters</i></p>		

Virtual Private Cloud IaaS	Public Cloud IaaS
<p>Bei der Virtual Private Cloud handelt es sich um eine Sonderform der Public Cloud. Durch eine logische Separierung auf Infrastrukturebene (LAN, SAN, dedizierte Virtual Hosts) erfolgt eine spezifische Mandantenzuordnung für die dedizierte Nutzung eines Cloud-Nutzers.</p> 	<p>Bei der Public Cloud IaaS werden alle Infrastrukturreourcen mittels dedizierter gebuchter virtueller Server aus einem Gesamtpool technischer Server bereitgestellt. Speicherkapazitäten werden dynamisch aus verfügbaren Speicher-pools (SAN) zugeordnet und für die Buchungsdauer fix allokiert.</p> 
<p><i>* Blau: Im primären Verantwortungsbereich des Cloud-Nutzers</i> <i>Orange: Im primären Verantwortungsbereich des Cloud-Anbieters</i> <i>Grün: Verantwortlichkeitsbereich anderer Cloud-Nutzer</i></p>	

Public Cloud PaaS – Core Packaged	Public Cloud PaaS – Core Business App
<p>Bei der Public Cloud PaaS – Core handelt es sich um eine Erweiterung einer Public Cloud IaaS um standardisierte Betriebssystem- und Anwendungsdienste (Datenbanken, App- und Web Server, IDM), die ein aufeinander abgestimmtes Management ermöglichen.</p> 	<p>Bei der Public Cloud PaaS – Core Business App handelt es sich um eine SaaS Basisvorstufe für Applikationsdienste, die durch direkte Programmierung auf spezielle Bedürfnisse angepasst werden können. Diese Zusatzmodule werden als isolierte Anwendungen im Public SaaS Modell bereitgestellt.</p> 
<p>* Blau: Im primären Verantwortungsbereich des Cloud-Nutzers Orange: Im primären Verantwortungsbereich des Cloud-Anbieters Grün, Rot: Verantwortlichkeitsbereich anderer Cloud-Nutzer</p>	

Public Cloud SaaS – Single	Public Cloud SaaS – Suite	Public Cloud Multi SaaS – Suite
<p>Bei der Public Cloud SaaS – Single wird eine dedizierte mandantenfähige Anwendung für die öffentliche Nutzung bereitgestellt.</p> 	<p>Bei der Public Cloud SaaS – Suite wird eine logische Gruppe mandantenfähiger Anwendungen für die öffentliche Nutzung bereitgestellt.</p> 	<p>Bei der Public Cloud Multi SaaS – Suite wird eine logische Gruppe mandantenfähiger Anwendungen über mehrere SaaS Betreiber hinweg für die öffentliche Nutzung bereitgestellt.</p> 
<p>* Orange: Im primären Verantwortungsbereich des Cloud-Anbieters Gelb: Im primären Verantwortungsbereich eines weiteren Cloud-Anbieters</p>		

2. Verantwortungsverteilung zwischen Cloud-Anbieter und Cloud-Nutzer

Da sich der Anwendungsbereich der Datenschutz-Zertifizierung nach AUDITOR auf die Verarbeitung personenbezogener Daten im Auftrag gemäß Art. 28 DSGVO erstreckt, adressiert der AUDITOR-Kriterienkatalog schwerpunktmäßig die datenschutzrechtlichen Anforderungen an den Cloud-Anbieter in seiner Funktion als Auftragsverarbeiter. Datenverarbeitungsvorgänge, bei denen der Cloud-Anbieter nicht lediglich weisungsgebunden agiert, sondern als Verantwortlicher über Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet, werden im Rahmen der AUDITOR-Zertifizierung nur betrachtet, soweit es um die Verarbeitung personenbezogener Daten des Cloud-Nutzers oder anderer betroffener Personen wie beispielsweise der Mitarbeiter des Cloud-Nutzers geht, die erforderlich ist, um den Cloud-Dienst zu erbringen und um dessen Nutzung und Abrechnung zu ermöglichen und soweit die Datenverarbeitung zur Erfüllung rechtlicher Pflichten dient, denen der Cloud-Anbieter unterliegt.

Dass es beim Cloud Computing regelmäßig zu einem Nebeneinander der Verantwortlichkeiten zwischen dem Cloud-Anbieter und dem Cloud-Nutzer kommt, ist nicht ungewöhnlich. Allgemeine Leitlinien zur Verantwortungsabgrenzung sind nur schwer zu bilden, da die Verantwortungsverteilung maßgeblich von den Dienst-Modellen und den konkreten Ausgestaltungen sowie den individuellen Auftragsverarbeitungsvereinbarungen mit den jeweiligen Cloud-Nutzern abhängt. Daher liegt es an dem Cloud-Nutzer und dem Cloud-Anbieter Regelungen zur Verantwortungsverteilung zu treffen.

Die Regelungen müssen die tatsächlichen Einflussmöglichkeiten zwischen den Parteien abbilden. Je größer die Einflussmöglichkeiten des Cloud-Anbieters auf die Datenverarbeitung sind, desto eher muss er als Verantwortlicher angesehen werden. Als Verantwortlicher ist gemäß Art. 4 Nr. 7 DSGVO stets derjenige anzusehen, der über die Zwecke und Mittel der Datenverarbeitung entscheidet. Der Cloud-Anbieter ist Auftragsverarbeiter, wenn er die Auftragsverarbeitung weisungsgemäß durchführt und mit den zu verarbeitenden Daten keine eigenen Zwecke verfolgt. Häufig verfügt der Cloud-Anbieter jedoch über gewisse Entscheidungsbefugnisse hinsichtlich der Wahl der technischen und organisatorischen Mittel. Solange diese Mittel angemessen sind, um den Verarbeitungszweck zu erreichen und er den Cloud-Nutzer über diese informiert und dieser damit einverstanden ist, bleibt der Cloud-Anbieter jedoch Auftragsverarbeiter.

Als Faustformel kann festgehalten werden, dass der Cloud-Nutzer regelmäßig für diejenigen personenbezogenen Daten als Verantwortlicher anzusehen ist, die er oder ihm zurechenbare Personen in die Cloud übertragen. Dies betrifft die Inhalts- und Anwendungsdaten des Cloud-Nutzers. Der Cloud-Anbieter wird für diejenigen Datenverarbeitungsvorgänge verantwortlich sein, die er vornimmt, um den Cloud-Dienst zu erbringen und um dessen Nutzung und Abrechnung zu ermöglichen. In der Regel betrifft dies Bestands- und Nutzungsdaten.

3. Verantwortungsverteilung zwischen Cloud-Anbieter und Subauftragsverarbeiter

Der Cloud-Anbieter hat die Möglichkeit, den Cloud-Dienst nicht vollständig selbst zu erbringen, sondern sich für die Leistungserbringung weiterer Subauftragsverarbeiter zu bedienen, soweit der Cloud-Nutzer damit einverstanden ist. In diesem Fall können einzelne Abschnitte oder Teile des Datenverarbeitungsvorgangs an weitere Auftragsverarbeiter delegiert oder ausgelagert werden, sodass eine Leistungskette entsteht.

Die Auslagerung der Datenverarbeitung an weitere Subauftragsverarbeiter darf jedoch nicht dazu führen, dass die Vorgaben der Datenschutz-Grundverordnung in der Leistungskette missachtet werden. Vielmehr muss der Cloud-Anbieter als Hauptauftragsverarbeiter dafür Sorge tragen, dass auf allen Stufen die einschlägigen Vorschriften der Datenschutz-Grundverordnung von allen Subauftragsverarbeitern eingehalten werden. Für die Auftragsdurchführung gegenüber dem Cloud-Nutzer bleibt der Cloud-Anbieter durchgängig verantwortlich.

Setzen die zu zertifizierenden Verarbeitungsvorgänge eines Cloud-Dienstes auf nicht-anbiereigene Plattformen oder Infrastrukturen auf oder setzt der Auftragsverarbeiter sonstige Subauftragsverarbeiter ein, so kann sich das Zertifikat nur auf diejenigen Datenverarbeitungsvorgänge beziehen, die im Verantwortungsbereich des jeweiligen Auftragsverarbeiters liegen. Der Auftragsverarbeiter muss sich jedoch als Hauptauftragsverarbeiter davon überzeugen, dass auch diese fremden, von ihm genutzten

Zertifizierungsgegenstand

Plattformen, Infrastrukturen und sonstigen Subauftragsverarbeiter die für sie relevanten datenschutzrechtlichen Vorschriften einhalten und darf nur solche für die Erbringung seines Cloud-Dienstes einsetzen.

Ein Cloud-Anbieter darf daher nur solche Subauftragsverarbeiter auswählen, die gemäß Art. 28 Abs. 1 DSGVO ebenfalls *„geeignete Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Personen gewährleistet“*. Subauftragsverarbeiter können die geforderten geeigneten Garantien ihrerseits beispielsweise durch den Nachweis durchlaufener Zertifizierungsverfahren oder durch die Befolgung von anerkannten Verhaltensregeln („Code of Conduct“) gemäß Art. 40 DSGVO erbringen. Kapitel V des Kriterienkatalogs regelt insbesondere die Subauftragsverarbeitung.

Literaturverzeichnis

- Alatorre, Gabriel; Ayala, Richard; Chavda, Kavita; Gopisetty, Sandeep; Singh, Aameek*, Data lifecycle management within a cloud computing environment. Angemeldet durch International Business Machines Corporation. Veröffentlichungsnr: US8918439 B2, 2014.
- Amazon Web Services, AWS | Amazon Virtual Private Cloud (VPC) – Sichere private Cloud (VPN)*, 2015.
- Bernard, Ray*, Information Lifecycle Security Risk Assessment. A tool for closing security gaps. In: *Computers & Security* 26 (1), 2017, 26–30. DOI: 10.1016/j.cose.2006.12.005.
- Bile, Tamer*, § 5 VII. Zertifizierung, in: Roßnagel, Alexander (Hrsg.), *Das neue Datenschutzrecht, Europäische Datenschutz-Grundverordnung und deutsche Datenschutzgesetze*, Baden-Baden 2018, 211-220.
- Brink, Stefan, Wolff, Amadeus* (Hrsg.), *BeckOK Datenschutzrecht*, 24. Edition, München 2018.
- Brühmann, Ulf*, Mindeststandards oder Vollharmonisierung des Datenschutzes in der EG, Zugleich ein Beitrag zur Systematik von Richtlinien zur Rechtsangleichung im Binnenmarkt in der Rechtsprechung des Europäischen Gerichtshofs, *Europäische Zeitschrift für Wirtschaftsrecht (EuZW)* 2009, 639-644.
- Burton, Adrian; Treloar, Andrew*, Designing for Discovery and Re-Use. The 'ANDS Data Shar-ing Verbs' Approach to Service Decomposition. In: *IJDC* 4 (3), 2009, 44–56. DOI: 10.2218/ijdc.v4i3.124.
- Curtin, Gregory G.*, Free the Data!: E-Governance for Megaregions. In: *Public Works Management & Policy* 14 (3), 2010, 307-326. DOI: 10.1177/1087724X09359352.
- Dillon, Tharam; Wu, Chen; Chang, Elizabeth* (Hrsg.), *Cloud Computing: Issues and Challenges*. Proceedings of the 24th IEEE International Conference on Advanced Information Networking and Applications (AINA 2010). Perth, Australia.
- Ehmann, Eugen, Selmayr, Martin* (Hrsg.), *DS-GVO, Datenschutz-Grundverordnung Kommentar*, 2. Auflage, München 2018.
- European Data Protection Board, Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679, Version 3.0, June 2019, abrufbar unter: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying-certification_en, zuletzt abgerufen am: 20.11.19.
- European Data Protection Board*, Annex 2 on the review and assessment of certification criteria pursuant to Article 42(5) to the Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 32 of the Regulation 2016/679, Version for public consultation, 23.1.2019 abrufbar unter: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying-0_en, zuletzt abgerufen am: 1.3.2019.
- European Network and Security Agency*, *Cloud Computing - Benefits, Risks and Recommendations for Information Security*, 2012.
- EuroPriSe*, Criteria for the certification of IT products and IT-based services (v201701), 2017, abrufbar unter: <https://www.european-privacy-seal.eu/EPS-en/Criteria>, zuletzt abgerufen am 12.9.2018.
- Fernandes, Diogo A. B.; Soares, Liliana F. B.; Gomes, João V.; Freire, Mário M.; Inácio, Pedro R. M.*, Security issues in cloud environments. A survey. In: *Int. J. Inf. Secur.* 13 (2), 2014, 113–170. DOI: 10.1007/s10207-013-0208-7.
- Grozev, Nikolay; Buyya, Rajkumar*, Inter-Cloud architectures and application brokering. Taxonomy and survey. In: *Softw. Pract. Exper.* 44 (3), 2014, 369–390. DOI: 10.1002/spe.2168.
- Hammer, Volker/Schuler, Karin*, Cui bono? – Ziele und Inhalte eines Datenschutz-Zertifikats, *Datenschutz und Datensicherheit (DuD)* 2007, 77-83.
- Higgins, Sarah*, The DCC Curation Lifecycle Model. In: *IJDC* 3 (1), 2008, 134–140. DOI: 10.2218/ijdc.v3i1.48.
- Higgins, Sarah*, The lifecycle of data management. In: *Graham Pryor* (Hg.): *Managing Re-search Data*. London: Facet Publishing 2012.
- Hofmann, Johanna/Roßnagel, Alexander*, Rechtliche Anforderungen an Zertifizierungen nach der DSGVO, in: *Krcmar, Helmut/Eckert, Claudia/Roßnagel, Alexander/Sunyaev, Ali/Wiesche, Manuel* (Hrsg.), *Management sicherer Cloud-Services, Entwicklung und Evaluation dynamischer Zertifikate*, Wiesbaden 2018, 101-112.
- Homung, Gerrit/Hartl, Korbinian*, Datenschutz durch Marktanziehe – auch in Europa? Stand der Diskussion zu Datenschutzzertifizierungen und Datenschutzaudit, *Zeitschrift für Datenschutz (ZD)* 2014, 219-225.
- Jäger, Bernd; Kraft, Reiner; Selzer, Annika; Waldmann, Ulrich*, Die teilautomatisierte Verifizierung der getrennten Verarbeitung in der Cloud, *Datenschutz und Datensicherheit (DuD)* 40 (5), 2016, 305–309. DOI: 10.1007/s11623-016-0601-2.
- Kühling, Jürgen, Buchner, Benedikt* (Hrsg.), *Datenschutz-Grundverordnung/BDSG Kommentar*, 2. Auflage, München 2018.
- Laue, Philipp/Nink, Judith/Kremer, Sascha*, Das neue Datenschutzrecht in der betrieblichen Praxis, Baden-Baden 2016.
- Leimeister, Stefanie; Böhm, Markus; Riedl, Christoph; Krcmar, Helmut* (Hrsg.), *The Business Perspective of Cloud Computing: Actors, Roles and Value Networks*. Proceedings of the 18th European Conference on Information Systems (ECIS 2010). Pretoria, South Africa.
- Marston, Sean; Li, Zhi; Bandyopadhyay, Subhajyoti; Zhang, Juheng; Ghalsasi, Anand*, Cloud Computing — The Business Perspective. In: *Decision Support Systems* 51 (1), 2011, 176–189.
- Massonet, Philippe; Naqvi, Syed; Ponsard, Christophe; Latanicki, Joseph; Rochwerger, Benny; Villari, Massimo*, A Monitoring and Audit Logging Architecture for Data Location Compliance in Federated Cloud Infrastructures. In: *Distributed Processing, Workshops and Phd Forum (IPDPSW)* 2011. Anchorage, AK, USA, 1510–1517.
- Mell, Peter; Grance, Timothy*, The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology. National Institute of Standards and Technology. Gaithersburg, Montgomery, USA 2011.
- Michener, William K.; Jones, Matthew B.*, Ecoinformatics: supporting ecology as a data-intensive science. In: *Ecological and evolutionary informatics* 27 (2), 2012, 85–93. DOI: 10.1016/j.tree.2011.11.016.
- Möller, Knud*, Lifecycle Models of Data-centric Systems and Domains: The Abstract Data Lifecycle Model. In: *Semant. web* 4 (1), 2013, 67–88. Online verfügbar unter <http://dl.acm.org/citation.cfm?id=2595053.2595060>.
- NIST Cloud Computing Security Working Group*, *NIST Cloud Computing Security Reference Architecture*. NIST. 2013. Online verfügbar unter <https://csrc.nist.gov/publications/detail/sp/500-299/draft>.
- Ofner, Martin Hubert; Straub, Kevin; Otto, Boris; Oesterle, Hubert*, Management of the master data lifecycle. A framework for analysis. In: *Journal of Ent Info Management* 26 (4), 2013, 472–491. DOI: 10.1108/JEIM-05-2013-0026.
- Paal, Boris, Pauly, Daniel A.* (Hrsg.), *Datenschutz-Grundverordnung Bundesdatenschutzgesetz Kommentar*, 2. Auflage, München 2018.
- Pearce, Michael; Zeadally, Sherali; Hunt, Ray*, *Virtualization*, in: *ACM Comput. Surv.* 45 (2), 2013, 1–39. DOI: 10.1145/2431211.2431216.
- Pearson, Siani; Benameur, Azzedine*, Privacy, Security and Trust Issues Arising from Cloud Computing. In: 2010 IEEE 2nd International Conference on Cloud Computing Technology and Science (CloudCom). Indianapolis, IN, USA, 2010, 693–702.
- Plath, Kai-Uwe* (Hrsg.), *DSGVO/BDSG, Kommentar zu DSGVO, BDSG und den Datenschutzbestimmungen von TMG und TKG*, 3. Auflage, Köln 2018.

Zertifizierungsgegenstand

- Roßnagel, Alexander*, Kommentierung der DSGVO, in: Simitis, Spiros/Hornung, Gerrit/Spiecker, Indra (Hrsg.), *Datenschutzrecht – DSGVO mit BDSG*, Baden-Baden 2019.
- Roßnagel, Alexander*, § 2 I. Anwendungsvorrang des Unionsrechts, in: ders. (Hrsg.), *Das neue Datenschutzrecht, Europäische Datenschutz-Grundverordnung und deutsche Datenschutzgesetze*, Baden-Baden 2018, 41-54.
- Roßnagel, Alexander*, Datenschutzaudit - ein modernes Steuerungsinstrument, in: Hempel, Leon/Krasmann, Susanne/Bröcking, Ulrich (Hrsg.), *Sichtbarkeitsregime, Überwachung, Sicherheit und Privatheit im 21. Jahrhundert*, Wiesbaden 2011, 263-280.
- Roßnagel, Alexander*, Datenschutzaudit, Konzeption, Durchführung, gesetzliche Regelung, Braunschweig/Wiesbaden 2000.
- Roßnagel, Alexander/Richter, Philipp/Nebel, Maxi*, Was bleibt vom Europäischen Datenschutzrecht? Überlegungen zum Ratsentwurf der DS-GVO, *Zeitschrift für Datenschutz (ZD)* 2015, 455-460.
- Schneider, Stephan; Sunyaev, Ali*, *Cloud-Service-Zertifizierung. Ein Rahmenwerk und Kriterienkatalog zur Zertifizierung von Cloud-Services*, Berlin Heidelberg 2015.
- Schwarze, Jürgen/Becker, Ulrich/Hatje, Armin/Schoo, Johann (Hrsg.), *EU-Kommentar*, 3. Auflage, Baden-Baden 2012 (zitiert: Autor, in: Schwarze u.a. 2012).
- Singh, Saurabh; Jeong, Young-Sik; Park, Jong Hyuk*, A survey on cloud computing security: Issues, threats, and solutions. In: *Journal of Network and Computer Applications* 75, 2016, 200–222. DOI: 10.1016/j.jnca.2016.09.002.
- Sun, Da-Wei; Chang, Gui-Ran; Gao, Shang; Jin, Li-Zhong; Wang, Xing-Wei*, Modeling a Dynamic Data Replication Strategy to Increase System Availability in Cloud Computing Environments. In: *J. Comput. Sci. Technol.* 27 (2), 2012, 256–272. DOI: 10.1007/s11390-012-1221-4.
- van Veenstra, Anne Fleur; van den Broek, Tijs*, A Community-driven Open Data Lifecycle Model Based on Literature and Practice. In: Imed Boughzala, Marijn Janssen und Saïd Assar (Hg.): *Case Studies in e-Government 2.0*. Cham: Springer International Publishing, 2015, 183–198.
- Villazón-Terrazas, Boris; Vilches-Blázquez, Luis. M.; Corcho, Oscar; Gómez-Pérez, Asunción*, Methodological Guidelines for Publishing Government Linked Data. In: David Wood (Hrsg.): *Linking Government Data*. New York, NY: Springer New York, 2011, 27–49. Online abrufbar unter https://doi.org/10.1007/978-1-4614-1767-5_2.
- Zhao, Liang; Sakr, Sherif; Liu, Anna; Bouguettaya, Athman*, *Cloud Data Management*. Cham: Springer International Publishing, 2014.