Formularhandbuch Datenschutzrecht

von
Dr. Ansgar Koreng, Matthias Lachenmann, Matthias Bergt, Nikolaus Bertermann, Jörg Jaenichen, Dr. Olaf Koglin, Sascha Kremer, Dr. Joachim Müller, Dr. Carlo Piltz, Stefan Sander, Steffen Weiß

1. Auflage

Verlag C.H. Beck München 2015

Verlag C.H. Beck im Internet:
www.beck.de
ISBN 978 3 406 66502 8

Zu Inhalts- und Sachverzeichnis

Eigenschaft	*Inhalt*
Rapid elasticity (schnell und flexibel)	Die Kapazitäten können flexibel zugewiesen werden, um sofort an den jeweiligen Bedarf angepasst zu werden. Für den Kunden scheinen sie daher unbegrenzt zu sein. Sie können ihm jederzeit in jeder Größe zugewiesen werden.
Measured service (Messung der Leistungen)	Cloud-Lösungen messen die Verwendung ihrer Resourcen, um deren Einsatz automatisch zu optimieren. Die Daten werden auch dem Kunden zur Verfügung gestellt und typischerweise auch für Abrechnungszwecke verwendet.

§ 2 Einordnung verschiedener Cloud-Angebote[1]

Kategorisierung	*Inhalt*
Betriebsart (public vs. private Cloud)	Hinsichtlich des Nutzerspektrums wird zwischen der (üblichen) Public Cloud, bei der die Leistungen einer Vielzahl von Kunden angeboten wird, und der Private Cloud unterschieden. Bei letzterer wird die Cloud nur von einem Kunden genutzt, so dass das Merkmal des „resource pooling" entfällt.[2] Die Public Cloud kann extern oder vom Nutzer selbst betrieben werden.
Art der Services	Die zweite Differenzierung erfolgt über die Art des angebotenen Services. Basierend darauf, dass der Nutzer eine Leistung, die aus hochkomplexen Hardware-, Netzwerk- und Softwarekomponenten besteht, ganz unkompliziert „as a service" erhält, wird zwischen Software as a Service (SaaS), Platform as a Service (PaaS) und Infrastructure as a Service (IaaS) unterschieden.[3]
SaaS	Bei SaaS wird ein Programm, das früher als eigene Software verkauft bzw. lizenziert worden wäre, nun als Rundum-Dienstleistung einschließlich der Rechenleistung, laufender Aktualisierung und weiteren Services angeboten. Beispiele sind die Vertriebsplattform Salesforce, Googles E-Mail-Produkt Gmail oder das Microsoft-Angebot Office 365, das das Office-Paket aus der Cloud heraus anbietet.
PaaS, IaaS	Im Rahmen von PaaS wird Kunden eine bereits mit dem Internet vernetzte Plattform zur Verfügung gestellt, auf der sie zum Beispiel Web-Anwendungen oder Apps testen und bereitstellen können. Bekannte Anbieter sind Amazon Web Services (AWS) oder

Kategorisierung	*Inhalt*
	Google App Engine. Bei IaaS ist die bereitgestellte Leistung, nämlich (virtuelle) IT-Infrastruktur, noch breiter verwendbar. Der Microsoft-Dienst Azure wird teils als PaaS und teils als IaaS eingestuft. Reine IaaS-Lösungen sind u. a. die „virtuellen Maschinen" von Google Compute Engine oder VMware.

§ 3 Unterschiede zu normaler Auftragsdatenverarbeitung

Aspekt	*Problematik*	*Lösung*
Anwendbarkeit des BDSG/Vorliegen personenbezogener Daten auch bei Verschlüsselung	In praktisch jeder Cloud werden Daten gespeichert und verarbeitet, die als personenbezogene Daten i. S. d. § 3 Abs. 1 BDSG zu qualifizieren sind. Sofern jedoch die Daten dergestalt verschlüsselt werden, dass der Cloud-Anbieter und dessen Mitarbeiter und Subunternehmer sie mit realistischem Aufwand nicht entschlüsseln können, sprechen unter Berücksichtigung der verschiedenen Rechtsauffassungen zur Definition der personenbezogenen Daten gute Gründe dafür, diesen Daten in Bezug auf den Cloud-Anbieter den Personenbezug abzusprechen.[5] Mit dieser Argumentation erübrigen sich weitere Ausführungen zum oder Einschränkungen durch das Datenschutzrecht. Ein großer Teil der Literatur sowie die Aufsichtsbehörden gehen – teils ohne weitere Erörterung dieser sich aufdrängenden Fragestellung – indes davon aus, dass die in der Cloud gespeicherten Daten auch für den Anbieter der Cloud personenbezogene Daten darstellen.[6]	Die Verschlüsselung ist bereits aus Gründen der Datensicherheit durchzuführen und wird von praktisch jedem Cloud-Dienstleister eingesetzt. Sie bringt jedoch hinsichtlich des Umgehens des Anwendungsbereiches des BDSG keine Rechtssicherheit. Zudem müssen die Daten nach heutigem Stand in den meisten Cloud-Rechnern wieder entschlüsselt werden, um dort verarbeitet werden zu können.[7]
Vorliegen einer Auftragsdatenverarbeitung	Die Leistungen des Cloud-Anbieters werden allgemein als Auftragsdatenverarbeitung i. S. d. § 11 BDSG und nicht als sog. Funktionsübertragung angesehen.[8] Denn der	Die Vereinbarung einer ordnungsgemäßen Vereinbarung über die Auftragsdatenver-

Aspekt	*Problematik*	*Lösung*
	Cloud-Anbieter trifft keine eigenen Entscheidungen über die inhaltliche Verarbeitung der Daten. Vielmehr legt der Cloud-Kunde durch seine Voreinstellungen und Nutzung in aller Regel selbst fest, welche Daten in welcher Form zu welchem Zweck verarbeitet werden soll. Eine Funktionsübertragung oder eine gänzlich eigene Funktion kommen daher nicht in Betracht.	arbeitung gehört bei Cloud-Verträgen zum Standard. Die Frage ist nicht das Ob, sondern das Wie; siehe hierzu die nachfolgenden Punkte.
Angaben über den Auftrag, betroffene Personen, Arten der Daten etc.[9]	Angesichts der Qualifikation als Auftragsdatenverarbeitung sind die Angaben nach § 11 Abs. 2 S. 1 BDSG zu machen, insbesondere zu – Nr. 1 (Gegenstand und Dauer des Auftrags) sowie – Nr. 2 (Umfang, Art und Zweck der Erhebung, Verarbeitung bzw. Nutzung von Daten, Art der Daten und Kreis der Betroffenen). Bei Cloud-Angeboten können diese Angaben in der geforderten konkreten Art und Weise regelmäßig nur sehr schwer gemacht werden. Während bei SaaS-Diensten durch die Vorgaben der virtuellen Software zumindest eine vorgegebene Nutzungsform existiert (wie etwa bei den Cloud-basierten Lösungen für E-Mails), sind PaaS und IaaS jeweils eine Stufe abstrakter. Wenn diese für immer wieder neue Lösungen eingesetzt werden sollen, ist eine entsprechende Dokumentation nur mit einer starken Bürokratie möglich.	Den formalen Anforderungen des § 11 Abs. 2 BDSG kann bei PaaS und IaaS nur schwer entsprochen werden. Sofern der Cloud-Vertrag nicht regelmäßig angepasst werden soll, werden in Rahmenverträgen oft breite, aber mit konkreten Beispielen veranschaulichte Szenarien vereinbart.
Technische und organisatorische Maßnahmen	Die Definition der technischen und organisatorischen Maßnahmen ist bei Cloud-Angeboten dadurch gekennzeichnet, dass die Anbieter regelmäßig über ein Bündel von vergleichsweise anspruchsvollen und sehr anerkannten Zertifizierungen verfügt, wie etwa ISO 27001 oder SAS 70.	Auch zu den vom Auftragnehmer (Kunde) gemanagten Punkten sollten zumindest allgemeine Festlegungen getroffen werden, um den Anforderungen

Aspekt	*Problematik*	*Lösung*
	In aller Regel gibt es im Cloud-Massengeschäft Vertragsklauseln, nach denen der Anbieter einzelne technische Spezifikationen auch ohne Einverständnis des Kunden ändern kann, sofern das vereinbarte Sicherheitsniveau hierdurch nicht verschlechtert wird. Deutlich knapper als in klassischen ADV-Verträgen sind die Festlegungen zu den technischen und organisatorischen Maßnahmen meist bei Themen, die vorrangig vom Kunden festgelegt werden, wie – Berechtigungsmanagement und Zugriffskontrolle (Anlage zu § 9 BDSG, S. 2 Nr. 3), – Weitergabekontrolle (Nr. 4), – Auftragskontrolle (Nr. 6) sowie – Datentrennung (Nr. 8).	der Anlage zu § 9 S. 2 BDSG zumindest in formaler Hinsicht zu genügen.
Vor-Ort-Prüfung	Der Kunde (Auftraggeber) hat gem. § 11 Abs. 2 S. 4 BDSG vor Beginn der Auftragsdatenverarbeitung und sodann regelmäßig die Einhaltung der technischen und organisatorischen Maßnahmen zu überprüfen. Eine Vor-Ort-Prüfung sieht das Gesetz nicht zwingend vor.[10] Zwar kann sie bei größeren Outsourcing-Projekten durchaus angemessen und sinnvoll sein. Wenn bei einer Cloud-Lösung aber zahlreiche, über die Welt verteilte Rechenzentren in Frage kommen und der Auftraggeber nicht einmal weiß, in welchem die Daten gespeichert werden, erscheint ein Vor-Ort-Audit nicht immer sinnvoll. Hinzu kommt, dass die großen Cloud-Rechenzentrum meist über exzellente Zertifizierungen verfügen und Verstöße oder rechtlich bedenkliche Vorgehensweisen – wie die Offenlegung von Daten an Sicherheitsbehörden in einem Umfang, der den Vorgaben des BDSG vielleicht nicht	Da eine Vor-Ort-Prüfung nicht zwingend vorgesehen ist, kann der Auftraggeber sich auch auf andere Weise von der Einhaltung der Vorgaben überzeugen. Hierzu kommen insbesondere Zertifizierungen in Betracht.

Aspekt	*Problematik*	*Lösung*
	Stand halten würde – bei einem Ortstermin nicht zu Tage treten würden.	
Subunternehmer/ Übermittlung in Länder außerhalb EU/EWR	Durch die Privilegierung des § 3 Abs. 8 S. 3 BDSG, wonach ein Auftragsdatenverarbeiter in der EU oder dem Europäischen Wirtschaftsraum nicht als Dritter im Sinne des Gesetzes gilt, wäre eine Cloud-Lösung mit Datenspeicherung alleine in der EU oder dem europäischen Wirtschaftsraum relativ unproblematisch möglich. Die meisten Cloud-Lösungen bieten j edoch keine solche verbindliche Lokalisation an oder beinhalten zumindest, dass von einer nicht-europäischen Gesellschaft zu Wartungszwecken auf die Cloud und die in ihr gespeicherten Daten zugegriffen werden darf, was wiederum in der Terminologie des Gesetzes eine Übermittlung der Daten darstellt (§ 3 Abs. 4 Nr. 3 lit b BDSG). Bei Anbietern aus Drittländern muss ein angemessenes Datenschutzniveau bestehen. Dies kann in der Praxis durch drei Varianten gewährleistet werden:[11] – Die Angemessenheit des Schutzniveaus eines anderen Staates kann formal festgestellt werde. – Speziell mit den USA existiert das Safe Harbour-Abkommen. US-Unternehmen können sich auf einer Website des Handelsministeriums registrieren lassen und müssen dabei zusichern, bestimmte Standards einzuhalten. Zudem ist dann ein „normaler“ Vertrag über die Auftragsdatenverarbeitung erforderlich. – Schließlich existieren Muster für internationale Verträge zur Auftragsdatenverarbeitung, die sog.	Ein Teil der Lösung besteht in dem von der Artikel-29-Datenschutzgruppe bei Microsoft Office 365 akzeptierten Weg, parallel zum ADV-Vertrag mit der europäischen Gesellschaft auch die EU Model Clauses mit der US-Gesellschaft abzuschließen, wenn diese Zugriff auf die in der EU gespeicherten Daten hat.

Aspekt	*Problematik*	*Lösung*
	EU Model Clauses oder Standardvertragsklauseln. Sie können mit jedem Unternehmen abgeschlossen werden. Problematisch ist, dass in Cloud-Lösungen auf Anbieterseite meist eine Vielzahl von Rechenzentren, Subunternehmern, Maintenance-Dienstleistern und Konzerngesellschaften involviert sind. Doch hier geben sich die Artikel-29-Datenschutzgruppe und die deutschen Aufsichtsbehörden z. T. pragmatisch. Sie goutieren, wenn innerhalb des Konzerns des Autragnehmers (des Cloudanbieters) mit einer europäischen Gesellschaft der Hauptvertrag geschlossen wird und parallel mit der US-Gesellschaft Model Clauses vereinbart werden.[12]	
Verarbeitung besonderer Arten personenbezogener Daten außerhalb EU/EWR	Ein besonderes Problem ergibt sich bei der Verarbeitung besonderer Arten von personenbezogenen Daten i. S. d. § 3 Abs. 9 BDSG. Die darunter fallenden Informationen über Gesundheit und Religionszugehörigkeit sind in gewissem Umfang in E-Mails von Unternehmen enthalten (z. B. Krankmeldung vorab per E-Mail; Angaben zu Lohnsteuerklasse und Kirchenzugehörigkeit). Nach dem Wortlaut des BDSG dürfen diese besonders sensiblen personenbezogenen Daten nur übermittelt werden, wenn eine Einwilligung oder andere, ganz enge Tatbestandsmerkmale wie etwa eine lebensgefährliche Notsituation vorliegen. Diese Voraussetzungen können beim Cloud-Einsatz realistischer Weise nicht vorliegen. Damit wäre eine Cloud mit Administrationszugriff von außerhalb des EWR für die meisten Anwendungsgebiete nicht zulässig, wohingegen	Mit der hier dargestellten neueren Rechtsauffassung und den damit verbundenen Rechtsrisiken ist die im BDSG vorgenommene Beschränkung nicht wirksam, da sie europäischem Datenschutzrecht widerspricht.

Aspekt	*Problematik*	*Lösung*
	solche Zugriffe innerhalb des EWR im Rahmen der Auftragsdatenverarbeitung dergestalt privilegiert sind, dass der Datenverarbeitende nicht als „Dritter" gilt (§ 3 Abs. 8 S. 3 BDSG) gilt und somit der Datenzugriff keine „Übermittlung" an einen Dritten darstellt (§ 3 Abs. 4 Nr. 3 lit. b) BDSG). **Dieser einfachgesetzlichen Definition und der damit verbundenen Folge wird auf Basis des EU-Rechts widersprochen, da die entsprechende Richtlinie nicht nur Mindeststandards setze, sondern im Rahmen einer Vollharmonisierung auch keine strengeren Regelungen zulasse.[13]** **Die in den allgemeinen Daten enthaltenen besonderen Arten personenbezogener Daten stellen somit auf Grundlage dieser neueren Rechtsauffassung kein Hindernis dar, um globale Cloud-Lösungen zu nutzen. Freilich sind die allgemeinen Anforderungen an die Auftragsdatenverarbeitung nebst entsprechender Dokumentation einzuhalten.**	

Anmerkungen

1. Differenzierung und Einteilung von Cloud-Dienstleistungen. Ausführlich dazu Bräutigam/*Bräutigam/Thalhöfer,* IT-Outsourcing und Cloud Computing, S. 1200 ff.

2. Resource Pooling und weitere Merkmale. Vgl. BSI, Eckpunktepapier „Sicherheitsempfehlungen für Cloud-Anbieter", S. 17; Bräutigam/*Bräutigam/Thalhöfer,* IT-Outsourcing und Cloud Computing, S. 1201.

3. Arten der zu erbringenden Cloud-Dienstleistungen. Siehe hierzu ausführlich BSI, Eckpunktepapier „Sicherheitsempfehlungen für Cloud-Anbieter", S. 17 ff.; Bräutigam/*Bräutigam/Thalhöfer,* IT-Outsourcing und Cloud Computing, S. 1200 f. *Heidrich/Wegener* in: Forgó/Helfrich/Schneider (Hrsg.), Betrieblicher Datenschutz, S. 475 ff.

4. Resource Pooling und weitere Merkmale. Vgl. BSI, Eckpunktepapier „Sicherheitsempfehlungen für Cloud-Anbieter", S. 17; Bräutigam/*Bräutigam/Thalhöfer,* IT-Outsourcing und Cloud Computing, S. 1201.

5. Entfallen des Personenbezugs durch Verschlüsselung. Vgl. mit ausführlicher Begründung *Kroschwald* in: Taeger (Hrsg.), Law as a Service, S. 289 (299 m. w. N.).

6. Bestehen des Personenbezugs. Vgl. Konferenz der Datenschutzbeauftragten des Bundes und der Länder, „Orientierungshilfe ‚Cloud Computing' ", S. 8.

7. Verschlüsselungstechniken und Datenverarbeitung. Bei einer solchen Argumentation ist jedoch zu beachten, dass nach § 3 Abs. 4 Nr. 3 lit. b) BDSG eine Übermittlung schon dann vorliegt, wenn ein Dritter zum Abruf bereit gehaltene Daten einsehen oder abrufen kann. Daher trägt diese Argumentation nur, wenn ein entsprechender Zugriff entweder technisch vollkommen ausgeschlossen ist oder wenn durch entsprechende Verschlüsselungsverfahren zwar technisch auf die gespeicherten Daten zugegriffen werden kann, diese jedoch dergestalt verschlüsselt sind, dass sie für den Cloud-Anbieter keinen Personenbezug haben. Letzteres scheitert aber bislang daran, dass die meisten Cloud-Lösungen nicht nur verschlüsselt eingereichte Daten speichern sollen, sondern bei allen Cloud-Formen (SaaS, PaaS und IaaS) die Daten in den Cloud-Rechenzentren verarbeitet werden müssen. Dies ist nur möglich, wenn die Daten unverschlüsselt zur Verarbeitung vorliegen. Um dieses Dilemma zu lösen, wird intensiv an sog. homomorphen Verschlüsselungstechniken geforscht, die aber bislang dem Markt nicht zur Verfügung stehen (vgl. hierzu *Kroschwald* in: Taeger (Hrsg.), Law as a Service, S. 289 (299); *Kast* in: Conrad/Grützmacher (Hrsg.), Recht der Daten und Datenbanken im Unternehmen, S. 1079; BMWi-Forschungsprojekt „Sealed Cloud"). Bei einer reinen „Miete" von Rechnerkapazität, also insbesondere bei IaaS, ist jedoch zu erörtern, ob der Anbieter Zugriff und die Möglichkeit der der Kenntnisnahme der personenbezogenen Daten hat (dazu B. V. § 3.). Ist dies nicht der Fall, liegt – bezogen auf den IaaS-Dienstleister – mangels Verarbeitung personenbezogener Daten die Annahme eines datenschutzrechtlich irrelevanten Sachverhaltes nahe. In der Praxis gibt es aber, zumindest für seltene technische Eingriffe, auf Seiten des Anbieters Administrator-Rechte mit der Möglichkeit des Zugriffs auf den gespeicherten Content.

8. Cloud Computing als Auftragsdatenverarbeitung. Dazu B. V. 2. Anm. 17.

9. Konkrete Angaben im ADV-Vertrag. Somit kann den Gefahren entgegengewirkt werden, entweder die Angaben zu eng gemacht zu haben oder aber später mit dem großen Aufwand einer späteren Vertragsänderung nachdokumentieren zu müssen. Risikoseitig ist festzuhalten, dass eine zu enge Definition ein eindeutiger und nach § 43 Abs. 1 Nr. 2b BDSG bußgeldbewährter Verstoß gegen das BDSG darstellt. Hingegen hat das eventuell überflüssige Nennen (noch) nicht durchgeführter Datenverarbeitungsschritte, zu weit gefasster Gruppen von Betroffenen oder zusätzlicher Zwecke wohl noch nie zu rechtlichen Konsequenzen geführt.

10. Vor-Ort-Audit. Dass eine Vor-Ort-Prüfung nicht zwingend notwendig ist, ist allg. Ansicht, vgl. nur BT-Drs. 16/13657, S. 18, *Gola/Schomerus*, BDSG, § 11 Rn. 21; Plath/*Plath*, BDSG, § 11 Rn. 113.

11. Datenübermittlung in Drittländer. Dies kann in der Unternehmenspraxis durch eine Konzernrichtlinie zur Auftragsdatenverarbeitung näher dargestellt werden. Dazu B. V. 3. § 5.

12. ADV-Vertrag plus EU Model Clause. Hierbei werden mit den europäischen Gesellschaften normale Verträge über die Auftragsdatenverarbeitung geschlossen. Parallel wird mit der (Mutter-)Gesellschaft in den USA ein Vertrag nach den EU Model Clauses abgeschlossen. Dies erscheint dogmatisch nicht konsequent, da unklar ist, welche Gesellschaft des Dienstleisters anzuweisen ist. Siehe zu der