D5.1

Datenschutzrechtliches Gutachten zur SPLITCloud-Pilotanwendung

(Umfasst die Inhalte der kontinuierlichen rechtlichen Beratung des Projekt-Konsortiums, D3.5)

Autoren:

Bud P. Bruegger (ULD)

Harald Zwingelberg (ULD)

Felix Bieker (ULD)

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

VDI|VDE|IT

Inhaltsverzeichnis

1. Einleitung

Das vorliegende Dokuments stellt die abschließende datenschutzrechtliche Bewertung des im Projekt SPLITCloud entwickelten Lösung für eine technisch realisierte und gesicherte Funktionstrennung im Bereich des Cloud-Computing sowie des zum Projektende im März 2017 vorgestellten Demonstrators dar.

Diese Beurteilung wurde unter Zugrundelegung der vom Unabhängigen Landezentrum für Datenschutz propagierten Vorgehensweise für eine Datenschutzfolgenabschätzung und unter Einbeziehung der von der Konferenz der unabhängigen Datenschutzbeauftragten des Bundes und der Länder empfohlenen Methodik des Standard-Datenschutzmodells erstellt. Die vorgestellte Lösung ist im Ergebnis eine geeignete Maßnahme, um im Vergleich zu konventionellen Cloud-Computing die datenschutzrechtlichen Gewährleistungsziele der Vertraulichkeit, Intervenierbarkeit und Transparenz erheblich zu stärken. Bei geeigneter Implementierung der SPLITCloud-Lösung kann die Kontrolle über wesentliche Teile der Datenverarbeitung an den Auftraggeber überwiesen werden, wobei insbesondere Zugriffe und Einflüsse der Mitarbeiter des Cloud-Infrastrukturanbieters ausgeschlossen werden können.

1.1 Zum Dokument

Das vorliegende Dokument stellt die abschließende Bewertung der in SPLITCloud entwickelten Lösung zur besseren Gewährleistung der Vertraulichkeit und der Kontrollierbarkeit des Cloud-Betreibers dar. Dieses Gutachten erfasst dabei an geeigneter Stelle auch die Inhalte der dauernden rechtlichen Begleitung der Projektpartner im Rahmen der Projektdurchführung, soweit für dies für die die abschließende Bewertung von Bedeutung ist. Daneben nimmt das Dokument die aus der laufenden rechtlichen Beratung erlangten Erkenntnisse an den geeigneten Orten in der Darstellung auf.

Im Rahmen des Arbeitspakets 1 oblag es dem Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein bereits, datenschutzrechtliche Anforderungen an eine Cloud-Computing-Architektur zu formulieren. Dabei wurden mit Stand vom Juli 2015 nationale datenschutz- und telemedienrechtliche Anforderungen ebenso betrachtet wie die rechtlichen Rahmenbedingungen für den grenzüberschreitenden Datenaustausch. Für diese allgemeinen Erwägungen zu rechtlichen Anforderungen an eine Cloud-Architektur wird insoweit auf das Dokument „D1.1 Datenschutzrechtliche Anforderungen

an das SPLITCloud-Framework“[1] verwiesen. Die Datenschutzgrundverordnung war nicht im finalen Text bekannt, so dass dieses Dokument dazu dient, ein Update zu den entsprechenden Normen zu liefern. Das Vorliegende Dokument nimmt dabei auch die im Rahmen des Projekts mit den Partnern in Begleitung der Entwicklung des Demonstrators erörterten Aspekte des rechtlichen und technischen Datenschutzes auf.

Im Projekt wurde die SPLITCloud-Lösung nebst eines entsprechenden Demonstrators vorgestellt. Diese Darstellung bezieht sich regelmäßig auf einen konkretisierender Muster-Use-Case unter Betrachtung der Anforderungen an Software-as-a-Service-Plattformen, die eine Einspeisung, Aufbereitung und Einsicht in Messwerte aus intelligenten digitalen Energieverbrauchszählern (Smart Meter) ermöglichen soll.

Die Gliederung dieses Dokuments orientiert sich an den Anforderungen einer Datenschutz-Folgenabschätzung. Datenschutz-Folgenabschätzungen dienen dazu ein personenbezogenes Verfahren zu beschreiben, Risiken für die Grundrechte der Betroffenen zu bewerten und Maßnahmen zur Minimierung dieser Risiken zu beschreiben und umzusetzen, Sie ist daher ein hilfreiches Instrument, um die in diesem Dokument angestrebte Evaluation in Hinblick auf Datenschutz, Datensicherheit und Risikominimierung nachvollziehbar und plausibel darzustellen. Der Prozess folgt einem Modell[2], dass sich als Methodologie des Standard-Datenschutzmodells der deutschen Datenschutz-Aufsichtsbehörden bedient, dass sich in der Praxis bereits bewährt hat. Zudem ist für Verarbeitungsverfahren, die ein hohes Risiko für die Rechte der Betroffenen darstellen, wie etwa die in SPLITCloud vorgesehen Speicherung personenbezogener Daten in der Cloud, in der ab dem 25. Mai 2018 anwendbaren europäischen Datenschutz-Grundverordnung (DSGVO) gemäß Artikel 35 verbindlich die Durchführung einer solchen Datenschutz-Folgenabschätzung vorgeschrieben.[3]

---

[1] http://www.splitcloud.de/?page_id=10.

[2] Basierend auf Michael Friedewald, Hannah Obersteller, Maxi Nebel, Felix Bieker, Martin Rost, in; Peter Zoche, Regina Ammicht Quinn, Michael Friedewald, Marit Hansen, Jessica Heesen, Thomas Hess, Jörn Lamla, Christian Matt, Alexander Roßnagel, Sabine Trepte, Michael Waidner (Hrsg.) White Paper Datenschutz-Folgenabschätzung, 2016, abrufbar unter: https://www.forum-privatheit.de/forum-privatheit-de/texte/veroeffentlichungen-des-forums/themenpapiere-white-paper/Forum_Privatheit_White_Paper_Datenschutz-Folgenabschaetzung_2016.pdf.

[3] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl.EU L 119 vom 4.5.2016, 1-88, abrufbar unter: http://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX%3A32016R0679.

1.2 Rahmen und Ziel des SPLITCloud-Projekts

Das Projekt SPLITCloud dient der Entwicklung einer Cloud-Architektur in der Software-as-a-Service (SaaS) als Cloud-Dienst mit datenschutzfördernden Gestaltungen angeboten werden soll, insbesondere indem die Rollen der Entitäten mit Verfügungsrechten an Daten und Systemen auf mehrere Personen verteilt werden und nach Möglichkeit die Kontrolle zum Cloud-Kunden hin „verschoben“ werden können soll. Für den Begriff Cloud fehlt es dabei an einem allgemeinverbindlichen Verständnis. Nach der verbreiteten Definition des US-amerikanischen National Institute of Standards and Technology (NIST)[4] ist Cloud Computing ein Modell, „das es erlaubt bei Bedarf, jederzeit und überall bequem über ein Netz auf einen geteilten Pool von konfigurierbaren Rechnerressourcen (z.B. Netze, Server, Speichersysteme, Anwendungen und Dienste) zuzugreifen, die schnell und mit minimalem Managementaufwand oder geringer Service-Provider-Interaktion zur Verfügung gestellt werden können.“[5] Der Cloud-Anwender ist dabei, wer zu beruflichen oder sonstigen Zwecken einen Cloud-Dienst in Anspruch nimmt. Cloud-Diensteanbieter ist, wer eigene oder fremde Cloud-Dienste zur Nutzung bereithält oder die angebotenen Dienste wirksam kontrolliert. Bei Cloud-Diensten wird hauptsächlich zwischen vier Bereitstellungsmodellen unterschieden:[6]

1. Private Cloud mit Cloud-Infrastruktur für nur eine Institution mit verschiedenen Möglichkeiten, welche Abteilung intern die Infrastruktur betreibt;
2. Public Cloud mit Services eines Cloud-Diensteanbieters für die Allgemeinheit oder große Gruppen;
3. Community Cloud mit von mehreren Institutionen geteilter Cloud-Infrastruktur, verbreitet u.a. bei Zusammenschlüssen öffentlicher Einrichtungen zur gemeinsamen Organisation der Datenverarbeitung;
4. Hybrid Cloud bei der gemeinsamen Nutzung von mehreren eigenständigen Cloud-Infrastrukturen über Schnittstellen.

Davon unabhängig wird zwischen drei Service-Modellen unterschieden:[7]

---

[4] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.
[5] Mell/Grance, NIST SP - 800-145, S. 2; verwendete Übersetzung nach https://www.bsi.bund.de/DE/Themen/CloudComputing/Grundlagen/Grundlagen_node.html.
[6] Manche Modelle wie beispielsweise Virtual Private Cloud – also eine durch logische Unterteilung einer Public Cloud geschaffene Private Cloud – sind von dieser Einteilung nicht umfasst, https://www.bsi.bund.de/DE/Themen/CloudComputing/Grundlagen/Grundlagen_node.html.
[7] BSI, Einführung Cloud Mangement,

1. Infrastructure-as-a-Service (IaaS) besteht aus hardwaregebundenen IT-Ressourcen – also Rechenleistung, Datenspeicher oder Netzen. Der Cloud-Anwender baut auf diesem Dienst seine Betriebssysteme und Anwendungen auf.
2. Platform-as-a-Service (PaaS) beinhaltet über IaaS hinaus eine komplette Infrastruktur bestehend aus Hardware und Betriebssystem. Auf dieser kann der Cloud-Anwender mittels standardisierter Schnittstellen eigene Anwendungen laufen lassen.
3. Software-as-a-Service (SaaS) oder auch Application Service Providing (ASP) stellt dem Cloud-Anwender über Computernetzwerke Anwendungen und Programmfunktionalitäten des Cloud-Diensteanbieters bereit.

Beim Cloud-Computing sind Hardware Ressourcen nicht mehr statisch bestimmten Diensten oder Prozessen zugewiesen,[8] sondern können dynamisch verwaltet und genutzt werden, womit eine effizientere Auslastung und hohe Skalierbarkeit im Bedarfsfall ermöglicht wird.

Ein zentrales Risiko des Cloud-Computing besteht im Kontrollverlust für den Cloud-Anwender über Hardware, Software und Daten. Damit geht das Bedürfnis einher, über zentrale Aspekte der Verarbeitung die Kontrolle zurückzuerlangen. Mit Blick auf die umfassenden Zugriffs- und Manipulationsmöglichkeiten, die mit der Gelegenheit zum physikalischen Zugriff auf die Geräte einhergehen, trifft dies auch zu, wenn lediglich Bereitstellung und Pflege der Hardware und bestimmter Systemkomponenten ausgelagert werden sollen. Die SPLITCloud-Architektur adressiert diesen Bedarf. Dieser besteht nicht nur im Hinblick auf den Schutz von Daten in Form von Geheimnissen als „Unternehmens-Assets“ sondern bei der Verarbeitung personenbezogener Daten in Cloud-Umgebungen auch als Voraussetzung für eine angemessen organisierte und durchgeführte Auftragsdatenverarbeitung. Zugleich dient die Überweisung möglichst umfangreicher Teile der Kontrolle an den Kunden auch den Cloud-Anbietern, die so von Ihren Kunden weniger Vertrauensvorschuss bedürfen und bei der Vertragsdurchführung die Weisungskonformität ihrer Diensterbringung darlegen können. Damit ergeben sich bei einer korrekten Durchführung entsprechender Maßnahmen nicht nur Vorteile im Rahmen einer Auswahl als Auftragsverarbeiter sondern ggf. auch eine Minderung des Haftungsrisikos.

Unter diesen allgemeinen Rahmenbedingungen und Zielen entwickelte das Projekt SPLITCloud Maßnahmen, die eine Rückverlagerung wesentlicher Systementscheidungen ermöglicht und zur Kontrolle zentraler Vorgänge für den

[8] Grünwald/Döpkens, MMR 2011, 287.

Verantwortlichen beiträgt. In diesem Dokument wird erörtert, in welchen Fällen aus Sicht des Datenschutzes ein Einsatz Mehrwerte erzeugt.

1.3 Begriffsbestimmungen

In diesem Dokument verwenden wir, soweit nicht anders angegeben und definiert, die etablierten Begrifflichkeiten aus dem Bereich des Cloud-Computing. Rechtliche Begriffe werden, soweit nicht anders bezeichnet, in der vom Gesetzgeber ausgeprägten Bedeutung verwendet, im Bereich des Datenschutzrechts kommt dabei die Terminologie der DSGVO zur Anwendung, soweit sich der Kontext nicht explizit auf andere Rechtsbereiche bezieht.

2. Ermittlung der Anforderungen

Dieses Kapitel stellt konkretisierend die Anforderungen an einen Einsatz der SPLITCloud-Architektur dar. Der hier verfolgten Art der Darstellung an Hand der Vorgehensweise für eine Datenschutzfolgenabschätzung (DSFA) wird der Prüfmaßstab daher an den Gewährleistungszielen des Standard-Datenschutzmodells entwickelt (2.2). Vorangestellt wird eine Beschreibung des Prüfgegenstandes und eine Übersicht der einschlägigen Rechtsgrundlagen, wobei für den Betrieb des Cloud-Dienstes ein besonderes Augenmerk auf der Auftragsdatenverarbeitung liegt (2.1.4).

Im Laufe der Entwicklung des SPLITCloud-Dokuments D1.1 war die Datenschutz-grundverordnung (DSGVO) noch nicht in einer finalen Fassung bekannt. Vielmehr befand sich die politische Diskussion um den Verordnungs-Entwurf selbst bei Redaktionsschluss zu D1.1 in einer sehr bewegten Phase. Konsequenterweise wurde das Gutachten zu den Anforderungen daher nicht an dem DSGVO-Entwurf sondern am Maßstab der geltende Gesetzte (BDSG, LDSG und den bereichsspezifischen Normen) verfasst. Nunmehr ist die DSGVO in ihrer finalen Fassung in Kraft getreten und ist ab Mai 2018 unmittelbar anwendbares Datenschutzrecht. Die in D1.1 entwickelten Anforderungen werden daher nachfolgend noch einmal aufgenommen und dem neuen Prüfungsmaßstab angepasst.

2.1 Beschreibung des Prüfgegenstands

Nachfolgend wird der Prüfgegenstand, die SPLITCloud-Lösung zur Gewinnung einer verbesserten Kontrolle in Cloud-Umgebungen, näher beschrieben (2.1.1), ein mögliches Einsatzszenario als Musteranwendungsfall für diese Lösung skizziert, wobei SPLITCloud bei einem Dienstleister für lokale Energie- und Wasserversorger zum Einsatz kommen könnte (2.1.2). Einer Beschreibung und Definition der die betroffenen Personen und die relevanten Akteure beschrieben (2.1.3) folgen schließlich Ausführungen zu den maßgeblichen Rechtsgrundlagen (2.1.4) und eine Zusammenfassung (2.1.5).

2.1.1 Abstrakter Prüfgegenstand: SPLITCloud-Architektur

In dieser Sektion wird der Prüfgegenstand, d.h. eine generische Drei-Schichten-Architektur für eine Datenbank-Anwendung näher beschrieben, wie sie im nachfolgend skizzierten exemplarischen Anwendungsfall einer Dienstleistung für lokale Energie und Wasserversorger Einsatz finden kann. Dies dient als Grundlage für die Betrachtung der Gewährleistungsziele und der daraus abgeleiteten Maßnahmen.

Abbildung 1 zeigt die generische 3-schichtige-Anwendung. In der Praxis wird aktuell davon ausgegangen, dass in der Regel Virtualisierungstechnologien verwendet werden so dass Hardware dynamisch von mehreren Anwendungen genutzt werden kann. Nach einem weit verbreiteten Ansatz wird die Applikation in drei Schichten unterteilt. Jede Schicht ist dabei ein eigenständiger Prozess.

Die Schichten kommunizieren über einen Socket, der lokal auf demselben Host verortet sein kann, oder eine Netzwerkverbindung zwischen verschiedenen Hosts darstellen kann. Der Anwender der Applikation verwendet einen Web Browser und verbindet sich mit der Darstellungsschicht (Presentation Logic), die ein Web Interface zur Applikation darstellt. Die Presentation Logic ist für die Interaktion mit dem Anwender verantwortlich, nimmt Eingaben entgegen und stellt die Resultate von Abfragen dar. Sie delegiert jegliche Verarbeitung an die Komponente der Business Logic. Auf dieser Ebene finden sich die eigentlichen Spezialanwendungen – in dem hier gewählten Beispiel also die Softwarelösungen für Betriebs- und Abrechnungsbelange lokaler Energielieferanten. Die Daten selbst sind dann noch einmal separat in einer Datenbank, der dritten Schicht, abgelegt. Dies wird typisch durch ein Database Management System (DBMS) implementiert.

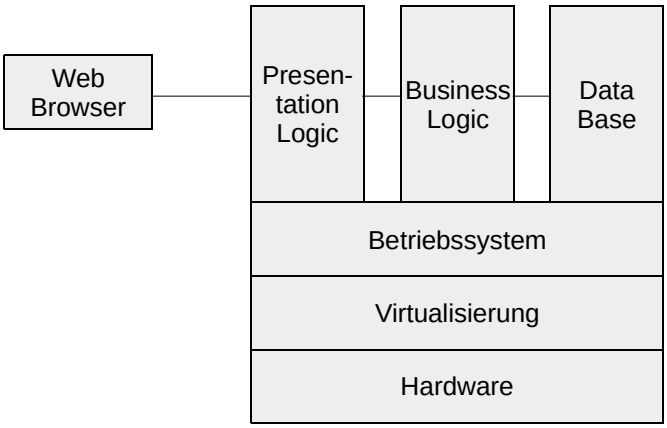

Abbildung 1 Generische 3-Tier Applikation

Während **Fehler! Verweisquelle konnte nicht gefunden werden.** die Möglichkeit zeigt, dass alle Schichten auf derselben Hardware laufen, zeigt die nachstehende Abbildung 2 die Möglichkeit, die Tiers auf verschiedene Hosts verteilt sind. Aus datenschutzrechtlicher Sicht ist auch die Darstellung von anderen Applikationen, die einem anderen Zweck dienen, wichtig.

Die Abbildung stellt im Weiteren noch vier wichtige Systemaspekte dar: Identitätsmanagement, Access Policy, Logging, und Systemintegrität. Typischerweise

wird der Zugriff auf Daten und Anwendungen auf autorisierte Anwender limitiert. Dazu benötigt man eine Systemkomponente, die die Berechtigungen von Anwendern und möglicherweise Komponenten verifiziert und verwaltet. Mittels Rechte- und Rollenkonzept (Access Policy) ist dann geregelt, wer auf welche Ressourcen (Daten, Prozesse) zugreifen kann. Diese Policy ist typischerweise in einem zentralen Ort wie einem Directory Device verwaltet. Das Logging registriert, wer wann was im System tut. Dies ist wichtig für die Revisionsfähigkeit des Systems und kann bei Verarbeitung personenbezogener Daten auch zur Erfüllung von Auskunftsansprüchen herangezogen werden.

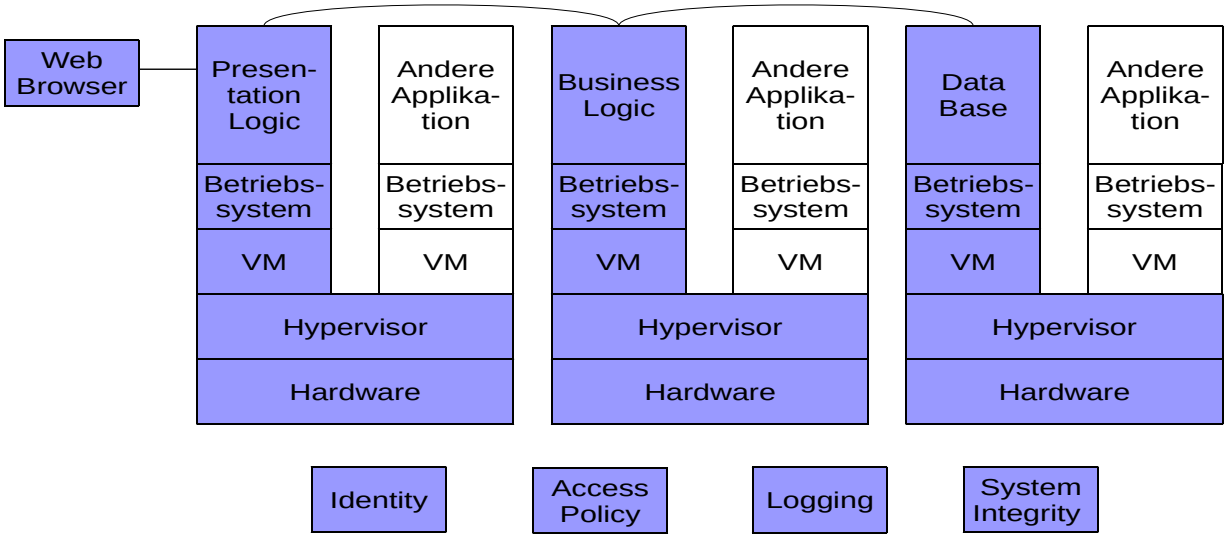

Abbildung 2 Deployment auf mehreren Hosts

2.1.2 Konkretisiertes Einsatzszenario: Dienstleistung für Energie- und Wasserversorger

Weil eine Bewertung von Systemen im Allgemeinen und die Durchführung einer Datenschutz-Folgenabschätzung im Speziellen von einem möglichst detaillierten Anwendungsfall profitiert und um die Darstellung nachvollziehbarer zu gestalten, beschreiben wir hier den Anwendungsfall, wie er den Projektpartnern während der Entwicklungsphase gedanklich als mögliche künftige Implementierung diente. Auf der mittels der SPLITCloud-Lösung gesicherten Plattform würde z.B. ein Dienst angeboten, der für lokale Wasser- und Energieversorger (im Folgenden abkürzend „Stadtwerke“) IT-Dienstleistungen von der Datenerhebung bis zur Rechnungsstellung anbietet.

Dafür besteht eine Rechenzentrums-Infrastruktur (Verantwortlicher Projektpartner für diese Aspekte: Verizon), die entsprechende Hardware und mit vorhandenen am Markt Virtualisierungslösungen enthält, um eine SPLITCloud-Anwendung zu betreiben. Hier wird die Hardware eingesetzt, die den Aufbau von vertrauenswürdigen, voneinander durch Sicherheitsmaßnahmen abgetrennten und gesicherten Teilabschnitten (Trusted Virtual Domains = TVD) ermöglicht in denen zusammengehörige Presentation Logic, Buseiness Logic und Data Base der Anwendung eines Kunden gekapselt werden. Eine entsprechend angepasste Lösung der vom Projektpartner Sirrix eingebrachten Lösung zum Erstellen und Verwalten von TVDs wurde im Projekt weiterentwickelt und angepasst. Hier setzt dann die zuvor abstrakt beschriebene drei-schichtige Architektur an. Die Business Logic enthält dabei die besonders für die Anforderungen von Stadtwerken angepasste Lösung. Diese umfassen das volle Spektrum der anfallenden Aufgaben vom Kundenmanagement, Entgegennahme der ausgelesenen Verbrauchswerte bis zur Erstellung der Rechnungen. Damit kommt es zwingend zu einer Verarbeitung von personenbezogenen Daten – denen der Stadtwerke-Kunden sowie von Mitarbeiterdaten. Mit Blick auf die gegenwärtige Entwicklung hin zu in engen Zeitintervallen messenden Stromzählen, die diese Information über das Netz an den Betreiber übermitteln (Smart Meter) können auch Daten betroffen sein, die sich zur Profilbildung eignen. Damit sind in den Messwerten nicht nur allgemein personenbezogene Daten zu sehen sondern, je nach dem Maße, in dem durch Rückschlüsse auf das Nutzungs-Verhalten der Endverbraucher detaillierte – teils gerätegenaue Profile – erstellt werden können, auch besonders sensible Informationen zu schützen. Sollen solche Angaben bei Dienstleistern verarbeitet werden, ist die verantwortliche Stelle (hier, die Stadtwerke) verpflichtet, über die gesamte Verarbeitungskette den erforderlichen Schutz sicherzustellen. Vorliegend wird daher geprüft, ob mittels SPLITCloud die Kontrolle über einzelne Verarbeitungen so umfassend zentral gehalten werden kann dass sich dabei auch der Recheninfrastrukturen Dritter bedient werden kann, mithin Cloud-Computing durch den Einsatz der SPLITCloud-Lösung erst statthaft wird oder ein bereits statthafter Einsatz maßgeblich sicherer gestaltet werden würde.

2.1.3 Akteure und betroffene Personen

Dieser Abschnitt erörtert betroffene Personen und Akteure im abstrakten Anwendungsszenario. Da das Projekt eine breit einsetzbare Technologie bereitstellt, diese aber nur in einer ganz konkreten Pilotanwendung umfassend und abschließend bewertet werden kann, wird diese Diskussion hier zunächst generisch geführt. In der vorliegenden Diskussion des Soll-Zustandes werden vorerst generische Akteure

beschrieben, wobei zwecks besserer Verständlichkeit an geeigneten Stellen Bezüge zum Musteranwendungsfall herstellt werden. Eine Spezialisierung und Diversifikation dieser Akteure ist erst in der Diskussion des Ist-Zustands möglich, nachdem die Konzepte von SPLITCloud analysiert worden sind und in der Folge eine Diversifikation von Akteuren und Rollen motiviert werden kann. Die betroffenen Personen können aufgrund des generischen Charakters dieser Evaluation nicht ermittelt werden, im konkretisierten Musteranwendungsfall sind dies die Stromkunden, deren Daten verarbeitet werden. Vielmehr wäre dies erst möglich, wenn sämtliche Informationen zur konkreten Umsetzung einschließlich der jeweiligen Datenflüsse etc. bekannt wären. Es wird an dieser Stelle daher als Grundannahme gesetzt, dass die Anwendung personenbezogene Daten von einer großen Anzahl von Personen verwaltet. Je nach Konkretisierung des Szenarios kann die Eingriffsintensität von normal bis sehr hoch variieren. Zur Kategorisierung von normalen, hohen und sehr hohen Eingriffsintensitäten verweisen wir hier auf die bewährten Eingruppierungen nach dem von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zur Anwendung empfohlenen Handbuchs zum Standarddatenschutzmodell (SDM).[9]

Die wichtigen Akteure für die abstrakte Darstellung werden im Folgenden beschrieben. Die Akteure für eine konkrete SPLITCloud-Implementierung werden erst nachstehend unter 2.5.2 bei der konkreten Bewertung des Risikos eingeführt.

Endkunden (betroffene Personen): Endkunden sind die natürlichen Personen, deren Daten verarbeitet werden und datenschutzrechtlich geschützt werden sollen. Datenschutzrechtlich sind dies die betroffenen Personen. Im Musteranwendungsfall sind dies die privaten Energiekunden.

Anwender (Verantwortlicher): Anwender als Ganzes ist die Entität, die eine zur Verfügung gestellte Softwarelösung einsetzt. Anwender bezeichnet dabei das einsetzende Unternehmen und dessen Mitarbeiter, die tatsächlich auf die Daten zugreifen. Der Anwender der Applikation benutzt einen Web Browser um die personenbezogenen Daten der Betroffenen gemäß dem Zweck der Anwendung zu verarbeiten. Der Anwender ist datenschutzrechtlich Verantwortlicher.

Hersteller der Hardware und Firmware: Die beschriebene Anwendung benötigt Hardware und damit gelieferte Firmware. Dies umfasst nicht nur die Computer wie den

[9] Siehe u.a.: https://www.datenschutz-mv.de/datenschutz/sdm/sdm.html.

Desktop des Anwenders, und die Server auf denen die Applikation läuft, sondern auch *Storage Application Networks*, *Firewalls*, und *Routers*.

Alle diese Geräte sind als Angriffsvektoren ideal geeignet. Angriffe über Firmware in einem Cloud Szenario findet man z.B. in [Gorobets u.a. 2015][10].

Hersteller der Software: Die Hersteller der verschiedenen Software sind weitere Akteure. Sie umfassen nicht nur die Hersteller der eigentlichen Applikation, sondern auch die Hersteller der Hypervisors, Betriebssysteme, Systemverwaltung wie automatisches Deployment, Migration und Überwachung, sowie Software. Daneben erfolgt die zur Unterstützung der in Abbildung 2 speziell erwähnten Funktionen wie Überwachung der Systemintegrität (z.B. Intrusion Detection), Logging, Identity Management und eventuelle Softwarekomponenten zur zentralisierten Konfiguration und Anwendung (Enforcement) von Policy.

In SPLITCloud sind die folgenden Softwarehersteller von besonderer Bedeutung:

- Hersteller der Applikationssoftware.
- Hersteller der Sicherheitssoftware, inklusive dem Trusted Server, Trusted Desktop und dem Trusted Object Manager (TOM)

Andere Softwarehersteller in SPLITCloud stellen andere Komponenten des Gesamtsystems her, inklusive den Betriebssystemen, dem Datenbankmanagement-system (DBMS) und dem Hypervisor.

Systembetreiber: Systembetreiber befassen sich mit dem technischen Betrieb der Anwendung über ihren gesamten Life Cycle hinweg. Dies beinhaltet die Installation und Wartung von Hardware und Software inklusive dem Ersetzen defekter Komponenten, Migration von Prozessen auf andere Prozessoren, Installation von neue Versionen von Software (und möglicherweise auch Firmware), Backup und Recovery von Daten, Löschen von Daten (inklusive der Tiefenlöschung von auszumusternden Festplatten), Überwachung der Systemleistung- und Sicherheit (z.B. mit Monitor Software wie Nagios[11] oder Intrusion Detection Systemen), bis hin zu forensischen Untersuchungen nach erkannten Angriffen.

[10] http://www.intelsecurity.com/advanced-threat-research/content/AttackingHypervisorsViaFirmware_bhusa15_dc23.pdf
[11] https://www.nagios.org/

Die Architektur von SPLITCloud definiert klar getrennte Rollen. Auf dieser Basis werden die folgenden Systembetreiber unterschieden:

- Server Hardware Provider, der die Server betreibt, auf denen die Applikation läuft.
- Trusted Objekt Manager Hardware Provider, der den TOM-Server betreibt.
- Applikationsbetreiber, der die eigentliche Applikation auf den oben genannten Servern betreibt.
- TOM-Administrator, der den Trusted Object Manger auf dem TOM-Server betreibt.

Unbefugte Dritte: Wie bei allen Anwendungen sind auch hier unbefugte Dritte als mögliche Akteure zu Berücksichtigen. Als unbefugt sind dabei auch Mitarbeiter der unterschiedlichen Akteure in der Leistungskette zu betrachten. Der Schutz ist also unabhängig davon zu gewährleisten, ob die Angriffe von organisationsinternen oder -externen Personen erfolgen.[12]

2.1.4 Identifikation der maßgeblichen Rechtsgrundlagen

Für die Verarbeitung personenbezogener Daten bedarf es stets einer Rechtsgrundlage, oder umgekehrt, die Verarbeitung personenbezogener Daten ohne eine genehmigende Rechtsgrundlage ist unzulässig, § 4 Abs. 1 BDSG, Art. 6 Abs. 1 Buchst. b DSGVO.[13] Dies gilt vor allem für die Verarbeitung durch den Verantwortlichen. Soweit durch den Einsatz einer Cloud-Lösung weitere Entitäten, wie Betreiber von Rechenzentren, mit der Verarbeitung der Daten betraut werden, lässt sich dies regelmäßig die Regelungen zur Auftragsdatenverarbeitung abbilden. Insoweit wird darin ein Schwerpunkt der Darstellung liegen.

Für die Datenverarbeitung durch den Cloud-Kunden selbst ergibt sich die Rechtsgrundlage gegenüber den betroffenen Personen in der Regel aus den allgemeinen datenschutzrechtlichen Normen oder spezifischen gesetzlichen Regelungen und wird konkretisiert durch die vertraglichen Beziehung zu den Endkunden. Für die Verarbeitung der zur Vertragsdurchführung erforderlichen Daten besteht regelmäßig bereits eine gesetzliche Erlaubnisnorm, vgl. § 28 Abs. 1 S. 1 BDSG, Art. 6 DSGVO. Die Regelung der DSGVO behält dabei die Grundstruktur des bereits im

[12] DSK, SDM v1.0 S. 14.
[13] Paal/Pauly Art. 6 DSGVO Rn. 7.

BDSG normierten[14] Verbots mit Erlaubnisvorbehalt, so dass jede Verarbeitung personenbezogener Daten unrechtmäßig ist, soweit keine Erlaubnisnorm vorhanden ist.

2.1.4.1 Cloud-Dienstleistung als Auftragsdatenverarbeitung

Der Datentransfer von der verantwortlichen Stelle an einen Anbieter von Cloud-Diensten kann über die Regelungen zur Auftragsdatenverarbeitung statthaft sein, soweit nicht durch eine explizite Einwilligung, z.B. als essentieller Bestandteil einer Leistung für die betroffene Person der Datentransfer schon auf anderer Rechtsgrundlage zulässig ist. Die Vorschrift des § 11 BDSG bzw. des Art. 28 DSGVO dient dabei als Rechtsgrundlage für den Datenfluss an den „verlängerten Arm" des Verantwortlichen (im Folgenden synonym auch „Auftraggeber") und gewährleistet einen Schutz betroffener Personen, deren Daten nunmehr bei einer weiteren Entität, die Hilfsaufgaben für den Verantwortlichen wahrnimmt[15], vorliegen. Letztverantwortlich für die gesamte Auftragskette bleibt stets der Verantwortliche. Dieser hat daher sicherzustellen, dass die für die Verarbeitung der Daten angemessene Schutz durch geeignete technische und organisatorische Maßnahmen beim Auftragnehmer gewährleistet ist, Art. 28 Abs. 1 DSGVO.

Eine Auftragsdatenverarbeitung privilegiert die Beteiligten in zweierlei Weise: Für den Auftraggeber stellt sie die Rechtsgrundlage für den Datentransfer an den Auftragnehmer dar, weil dieser nicht „Dritter" i.S.d. DSGVO ist,[16] für den weisungsgemäß handelnden Auftragnehmer beschränkt sich die Haftung im Vergleich zu allen anderen Verarbeitern auf Verstöße gegen die spezifischen Pflichten der Auftragnehmer. Überschreitet der Auftragnehmer demgegenüber seine Rechte, indem er selbst die Mittel und Zwecke der Verarbeitung bestimmt (sog. Funktionsexzess), haftet er wie ein Verarbeiter, Art. 28 Abs. 10 DSGVO.[17] Der Auftraggeber muss also die rechtliche Herrschaft über die Daten behalten, damit die Erlaubnisnorm greift.[18] Ob dies der Fall ist, hängt von der Ausgestaltung der Dienstleistung ab.

Wird die **Cloud als reiner Speicherdienst** genutzt, lässt sich nicht pauschal bestimmen, ob Datenübermittlungen an einen Onlinespeicher als Inanspruchnahme einer Auftragsdatenspeicherung anzusehen sind.[19] Sind Cloud-Anwender und Cloud-Diensteanbieter bestrebt, den Cloud-Dienst so auszugestalten, dass er die

[14] Gola/Schomerus, BDSG, § 4 Rn. 3.
[15] Engeler/Deibler/Hansen/Jensen/Obersteller, MonIKA, S. 28; Paal/Pauly Art. 28 DSGVO Rn. 1.
[16] Paal/Pauly Art. 28 DSGVO, Rn. 7f.
[17] Paal/Pauly Art. 28 DSGVO, Rn. 77.
[18] Zum BDSG: Gola/Schomerus, BDSG, § 11 Rn. 3; Nägele/Jacobs, ZUM 2010, 281 (290).
[19] SPLITCloud D1.1, S.15.

Anforderungen des § 11 BDSG bzw. Art. 28 DSGVO erfüllt, ist dies ohne weiteres möglich. Als „Dilemma des Cloud Computing“ wird hingegen der Umstand bezeichnet, dass das Machtgefälle zwischen Cloud-Diensteanbieter und Cloud-Anwender dem oftmals entgegensteht.[20]

Der für SPLITCloud interessantere Anwendungsfall stellt die Nutzung der Cloud für Software-as-a-Service (SaaS) dar. Dabei werden neben Datenspeicher ganze Anwendungen und ggf. weitere Ressourcen vom Nutzer in die Cloud verlagert, bzw. vom Anbieter angeboten.[21] Die Bedienung kann dann dabei oft über einen Webbrowser erfolgen, so dass sich eine lokale Installation von Software erübrigt. [22] Das angebotene Software-Paket ist regelmäßig mandantenfähig und der Anbieter übernimmt die Sorge für zeitgerechte Updates.[23] Gleichzeitig sorgt die Cloud-Speicherung für eine hohe Verfügbarkeit der verarbeiteten Daten.

Anforderungen einer Auftragsdatenverarbeitung bei SaaS-Diensten

Auch SaaS-Dienste können Auftragsdatenverarbeitung sein.[24] Maßgeblich ist, ob der Auftragnehmer über die Mittel und Zwecke der Verarbeitung (mit-)bestimmt, Art. 28 Abs. 10 DSGVO, also insbesondere davon ob der Anbieter die bereitgestellten Daten auch zu eigenen Zwecken auswerten würde.

Kommt danach rechtlich ein Auftragsverhältnis in Frage, sind die weiteren Voraussetzungen des Art. 28 DSGVO zu erfüllen. Dazu haben Auftraggeber und -nehmer einen Vertrag zu schließen, der die Weisungsbindung sicherstellt, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, Kategorien betroffener Personen und die Rechte und Pflichten des Auftragnehmers spezifiziert und insbesondere nach Art. 28 Abs. 3 vorsieht, „dass der Auftragsverarbeiter:

> „a) die personenbezogenen Daten nur auf dokumentierte Weisung des Verantwortlichen – auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation – verarbeitet, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor

[20] Schuster/Reichl, CR 2010, 38 (42).
[21] Grünwald/Döpkens, MMR 2011, 287; Nägele/Jacobs, ZUM 2010, 281.
[22] Grünwald/Döpkens, MMR 2011, 287.
[23] Sommergut, Computerwoche 2015.
[24] Bergt, in: Taeger, Law as a Service (LaaS), S. 37/138; Kompetenzzentrum Trusted Cloud, Datenschutzrechtliche Lösungen für Cloud Computing, S. 6; SPLITCloud, D1.1. S. 19:

der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet;

b) gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen;

c) alle gemäß Artikel 32 [DSGVO] erforderlichen Maßnahmen ergreift;

d) die in den Absätzen 2 und 4 genannten Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters einhält;

e) angesichts der Art der Verarbeitung den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützt, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III [der DSGVO] genannten Rechte der betroffenen Person nachzukommen;

f) unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 [DSGVO] genannten Pflichten unterstützt;

f) nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder löscht oder zurückgibt, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht,

h) dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Artikel niedergelegten Pflichten zur Verfügung stellt und Überprüfungen – einschließlich Inspektionen –, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglicht und dazu beiträgt."

Im Vergleich zu der Normierung der Auftragsdatenverarbeitung im BDSG[25] bleiben die Regelungen der DSGVO damit inhaltlich gleich und spezifizieren einige Aspekte wie die Erteilung von Unteraufträgen nunmehr genauer.[26]

[25] Zu cloudspezifischen Fragestellungen siehe SPLITCloud D1.1, S. 18 ff.
[26] Paal/Pauly, Art. 28 Rn. 79.

Rechtsfolge einer Auftragsdatenverarbeitung bei SaaS-Diensten

Sind alle Voraussetzungen gegeben, bleibt der Verantwortliche weiterhin in der Pflicht, die Ordnungsmäßigkeit der Datenverarbeitung zu gewährleisten, indem er bereits bei der Auswahl des Auftragnehmers sicherstellt, dass dieser hinreichende Garantien für geeignete technische und organisatorische Maßnahmen getroffen hat, Art. 28 Abs. 1 DSGVO[27]. Während der Auftragsverarbeiter den -geber bei der Umsetzung der Betroffenenrechte unterstützt (Art. 28 Abs. 2 Buchst. e), bleibt die verantwortliche Stelle Adressat der Pflichten. Die Haftung eines im Rahmen der Weisungen agierenden Auftragnehmers ist auf Verletzung spezifischer Pflichten für Auftragnehmer begrenzt, Art. 82 Abs. 2 DSGVO.[28] Im Ergebnis bleibt es daher eine Obliegenheit des Auftraggebers, den Auftragsverarbeiter bei der Wahrnehmung des Auftrags bei zentralen Handlungen so umfassend zu überwachen, wie dies möglich ist. Dabei sollte solchen Tätigkeiten eine erhöhte Aufmerksamkeit zukommen, die mit besonderen Risiken verbunden sind. Bei „Software as a Service"-Angeboten sind dies unter anderem:

- Das Einspielen neuer Systemsoftware: Bei einem on-premise Hosting durch den Verantwortlichen würde datenschutzrechtlich erwartet, dass neue Software erst nach erfolgreichem Absolvierens eines Prozesses für Test und Freigabe in Betrieb genommen würde. Bei SaaS-Diensten ist das Updatemanagement teilweise schon Inhalt des Angebots, der Verantwortliche bleibt jedoch rechtlich in der Pflicht.
- Die Rechtevergabe durch die Administration: Die Durchsetzung eines Rechte- und Rollenkonzeptes für den Zugriff auf die Daten obliegt weiterhin dem Verantwortlichen. Die physikalischen Systeme und auch die tatsächlichen Zugangsmöglichkeiten bestehen aber beim Dienstleister. Die Rechtevergabe sollte daher zumindest effektiv überwacht, besser noch von der verantwortlichen Stelle selbst oder durch einen gesondert Beauftragten wahrgenommen werden.
- Wechsel der Hardware und des Verarbeitungsortes: Eine Eigenschaft diverser Cloud-Architekturen besteht darin, dass die Datenverarbeitung im Container jederzeit flexibel auf andere Hardware verschoben werden kann, was eine besonders effektive Nutzung der vorhandenen Hardware ermöglicht und damit mittelbar für die Cloud-Kunden günstige Preise ermöglicht. Ein Datentransfer in

[27] Paal/Pauly, Art. 28 Rn. 19.
[28] von Albrecht/Jotzo, Teil 8, Rn. 21.

Drittstaaten sollte vermeiden werden.[29] Idealerweise sollten dabei neben der vertraglichen Zusicherung durch den Dienstleister weitere Garantien technischer Natur vorhanden sein. Normativ sieht die DSGVO dabei vor, dass die Art und Weise der Verarbeitung hinsichtlich des Gegenstands und Dauer der Verarbeitung sowie bezüglich Art und Zweck der Verarbeitung bestimmt sein müssen, Art. 28 Abs. 3 DSGVO. Daraus wird geschlossen, dass der Auftraggeber die weiteren Details des „Wie“ nicht vorgeben muss, was der arbeitsteiligen Gestaltung und den jeweiligen Expertisen der Parteien entspricht.[30]

- Nach Möglichkeit ist ein Zugriff auf die Daten durch Mitarbeiter und Administratoren des Auftragsverarbeiters auszuschließen, womit auch erzwungene Zugriffe Dritter erschwert werden.

Während nicht alle SaaS-Dienste diese besonderen Teilaspekte werden adressieren können und auch nicht müssen, sind solche Aspekte jedoch bei der Betrachtung zu berücksichtigen, sobald ein erhöhter Schutzbedarf festgestellt wird.

Auftragsdatenverarbeitung im Use Case Energieabrechnung

Im besonderen Fall der Verarbeitung von per Smart Meter erhobenen Messdaten sind neben vertraglichen Regelungen besondere Voraussetzungen für die Erhebung und Verarbeitung der Daten zu beachten. Für die Erhebung und Verarbeitung von Daten durch Messstellen sieht das Messstellenbetriebsgesetz (MsbG) vom August 2016 in den §§ 19 bis 28 entsprechende konkretisierende datenschutzrechtliche Anforderungen vor. Die Befugnis, die für die Zweckerreichung erforderlichen Daten zu verarbeiten, ergibt sich hier bereits spezialgesetzlich aus § 50 Abs. 1 MsbG. Sollen Daten über den konkret gesetzlich ausgeführten Katalog privilegierter Zwecke hinaus verarbeitet werden, ist eine Einwilligung der betroffenen Personen erforderlich, § 50 Abs. 1 und 2 MsbG. Die Berechtigung zur Verarbeitung von Messdaten wird in § 49 MsbG konkreten Stellen zugewiesen, u.a. den Energielieferanten und Netzbetreibern. Eine darüber hinaus erfolgende Übermittlung, Nutzung oder Beschlagnahme durch andere Stellen ist weder nach den Normen des Bundes noch der Länder statthaft, so dass nicht ausdrücklich genannte Stellen zur Verarbeitung einer wirksamen Einwilligung i.S.d.

[29] Die Anforderungen für einen Transfer in Drittstaaten sind in Art. 44 ff DSGVO geregelt. Im Wesentlichen bleibt es bei den Übermittlungsmöglichkeiten, die schon unter dem BDSG bekannt waren, insbesondere dass es entweder der Feststellung eines angemessenen Datenschutzniveaus im Zielland oder sonstiger geeigneter Garantien bedarf, siehe BayLDA, „XI Datenübermittlungen“.
[30] Paal/Pauly, Art. 28, Rn. 38.

Datenschutzrechts bedürfen, § 49 Abs. 1 S. 2 MsbG i.V.m. § 49 Abs. 3 Nr. 7 MsbG. Abweichend von dieser strikten Untersagung einer zweckändernden Übermittlung ist die Auftragsdatenverarbeitung i.S.d. § 11 BDSG jedoch nach § 49 Abs. 3 MsbG ausdrücklich erlaubt. Damit sind die für die SPLITCloud oben vorgeschlagenen Praxisumsetzungen auch im Bereich des Energiewesens rechtlich zulässig, soweit den Anforderungen an ein wirksames Auftragsverhältnis genügt wird (siehe nachstehend).

Daneben stellt das Messstellenbetriebsgesetz weitere datenschutzrelevante Anforderungen, die jedoch für die Betrachtung der SPLITCloud-Lösung keine besondere Relevanz aufweisen, weil sie unverändert bei einer Datenverarbeitung ohne Cloud-Kontext anzuwenden sind. So sieht das MsbG Mindestanforderungen für intelligente Messsysteme vor, die unter anderem Aspekte der Vertraulichkeit und Verfügbarkeit adressieren und schreibt eine Zertifizierung vor, § 19 Abs. 3 MsbG.

Die Normen des MsbG verweisen ausschließlich auf das BDSG und damit auf die nationale Rechtslage bis zum Wirksamwerden der DSGVO. Ab dem 25. Mai 2018 werden die Normen der DSGVO direkt anwendbar sein und die Regelungen des BDSG ablösen. Der deutsche Gesetzgeber wird im Zuge dessen das MsbG anpassen oder einen Hinweis auf die Anwendbarkeit der Art, 28 f. DSGVO in das BDSG-neu aufnehmen, Diese Normen bedürfen aufgrund der unmittelbaren Anwendbarkeit von Verordnungen gem. Art. 288 UAbs. 1 AEUV keiner eigenen Umsetzung durch den nationalen Gesetzgeber, konkret dass die Art. 28 f DSGVO zur Auftragsdatenverarbeitung vollinhaltlich zur Anwendung gelangen.

2.1.4.2 Cloud-Dienstleistung auf Basis einer informierten Einwilligung

Neben der Nutzung eines Cloud-Dienstes auf Basis einer Auftragsdatenverarbeitung besteht stets die Möglichkeit, die Verarbeitung über eine informierte Einwilligung aller betroffenen Personen zu legitimieren. Die Einwilligung ist dann Rechtsgrundlage für die Datenübermittlung an und die Verarbeitung durch den Dienstanbieter. Weil sowohl für die vertragsnotwendige Datenverarbeitung als auch für die Einbeziehung eines Dienstleisters als Auftragsverarbeiter gesetzliche Rechtsgrundlagen bestehen, wird es in der Praxis der betrachteten Anwendungsfalls nur des Rückgriffs auf eine Einwilligungslösung bedürfen, wenn eine über das Erforderliche hinausgehende Verarbeitung erfolgen soll,[31] z.B. auf Basis der Daten weitere Zusatzdienste angeboten

[31] Wobei auch bei Fällen gesetzlich gestatteter Datenverarbeitung eine Unterrichtung über Grund, Zulässigkeit und Erforderlichkeit der Datenverarbeitung zu erfolgen hat, vergl. Paal/Pauly/Frenzel, Art. 6 Rn. 7 DSGVO.

werden sollen, die nicht in unmittelbarem Zusammenhang mit der Energieversorgung stehen.

Während die Einwilligung für viele Bereiche der Datenverarbeitung gängige Praxis ist, ist sie im Bereich des Cloud-Computing kaum gangbar.[32] Eine informierte Einwilligung setzt möglichst genaue Kennnisse der betroffenen Personen von den technischen Abläufen voraus. Das widerspricht primär der meist explizit gewünschten Flexibilität des Cloud-Computing und ist herausfordernd aber durchaus praktisch umsetzbar. Wesentliche Änderungen am System bedürften darüber hinaus einer erneuten Einwilligung.[33] Schließlich müsste der Verantwortliche mit einem jederzeitigen Widerruf der Einwilligung praktisch umgehen und eine Verarbeitung für die Zukunft ausschließen können, vgl. Art. 7 Abs. 3 DSGVO. Ein solches Einwilligungs- und Widerrufsmanagement ist jedenfalls bei einer größeren Zahl betroffener Personen schwer umsetzbar und praxistauglich.

Haftungsrechtlich hat dies für den Dienstanbieter die Konsequenz, dass er nunmehr gegenüber dem Betroffenen nicht mehr als Auftragsverarbeiter auftritt und damit die besondere Beschränkung der Haftung auf die Verletzung der spezifischen Pflichten eine Auftragsverarbeiters verliert, was jedoch zumindest im Innenverhältnis zum Cloud-Kunden vertraglich geregelt werden kann. Für die betroffenen Personen hat eine solche Lösung zwar den Vorteil einer erhöhten Transparenz, da nunmehr Normen der Art. 12 ff. DSGVO unmittelbar für den Cloud-Dienst gelten, umgekehrt besteht jedoch das Risiko dass den betroffenen Personen die Einwilligung in letztlich alternativlosen Situationen abverlangt wird.[34] Insbesondere bei der Deckung lebensnotwendiger Bedürfnisse wie der Grundversorgung mit Energie und Wasser ist die Freiwilligkeit der Einwilligung sicherzustelle, denkbar z.B. vergleichbare Alternativangebote ohne Datenverarbeitung die einer Einwilligung bedarf.

Einwilligungen können damit für Daten, die nicht für die Erfüllung des Vertrages, einer Rechtspflicht oder einer öffentliche Aufgabe im Sinne des Art. 6 Abs. 1 DSGVO erforderlich sind, als Rechtsgrundlage in Betracht zu ziehen.[35]

[32] Niemann/Paul, Rn. 107.
[33] Niemann/Paul, Rn. 107.
[34] Kamp/Rost, DuD 2013, 80, 81f.
[35] Für weitere Ausführungen zur Einwilligung siehe SPLITCloud D1.1 ,S. 20 ff.

2.1.4.3 Messdaten – Bereichsspezifische Normen

Für den Muster-Anwendungsfall ergeben sich aus den bereichsspezifischen Normen geringfügig erweiterte Anforderungen. So wurde bereits nach alter Rechtslage durch die Aufsichtsbehörden vertreten, dass bei einer Auftragsdatenverarbeitung gegenüber den betroffenen Personen Verantwortliche und Auftragnehmer konkret zu benennen sind. Jedenfalls für Auftragsverhältnisse, die einer Einwilligung der Betroffenen bedürfen oder anderweitig besondere Risiken für die betroffenen Personen aufweisen wurde dies vertreten, z.B. weil die Auftragserteilung durch einen Berufsgeheimnisträger nach § 203 StGB erfolgt.[36] Für die besonders sensitiven Daten, die bei einer zeitgenauen Kommunikation von Messwerten anfallen, sieht § 54 MsbG daher als konkretisierende Transparenzanforderungen vor, dass mittels kurzem, einfach verständlichem Formblatt mitzuteilen ist, wer welche Daten von wem wie oft zu welchem Zweck erhält, § 54 Abs. 1 S. 2 MsbG. In diesem Kontext sollten nach unserer Auffassung auch die Auftragnehmer in einer Auftragskette benannt werden, einschließlich einer Information über den Adresse und Sitz der Auftragnehmer. Dafür spricht, dass künftig nach der DSGVO Auftragnehmer zusammen mit den Verantwortlichen gegenüber den Betroffenen für Schäden im Rahmen einer deliktischen Gesamtschuld haften, soweit sie auftragsverarbeiter-spezifische Pflichten verletzt haben, Art. 82 Abs, 2 DSGVO.[37] Insoweit ist es hilfreich, wenn die Betroffenen zwecks Rechtewahrnehmung auch die Adressen der Auftragnehmer zur Kenntnis erhalten.

2.1.4.4 Einwilligung zur weiteren Verarbeitung von Messdaten

Wie bereits oben dargestellt, bestehen umfassende Erlaubnisnormen für die Datenverarbeitung im Energiesektor, soweit diese zur Erbringung der Energielieferung und des Betriebes der Netze erforderlich ist. Sollen darüber hinaus auf Basis der Daten Mehrwertdienste angeboten werden, die nicht energiewirtschaftlich erforderlich sind, bedarf es einer Einwilligung.[38] Diese muss den Anforderungen hinsichtlich der Freiwilligkeit und Informiertheit genügen und auf der Einwilligung basierende Datenverarbeitung muss derart gestaltet sein, dass einem Widerruf der betroffenen Person Rechnung getragen werden kann (siehe oben 2.1.4.2).

---

[36] ULD, Mehrstufige Schweigepflichtentbindungserklärungen, online: https://www.datenschutzzentrum.de/artikel/879-.html
[37] Von Albrecht/Jotzo, Teil 8 Rn. 21.
[38] MsbG-Entwurf, BT-Drucksache 18/7555, S. 107.

2.1.5 Zusammenfassung Prüfgegenstand und Rechtsgrundlagen

Als Rechtsgrundlage für die Cloud-Nutzung bei einem Anbieter im Inland bzw. im Geltungsbereich der DSGVO wird regelmäßig für die meisten Anwendungsfälle eine Auftragsdatenverarbeitung in Betracht kommen. Dabei obliegen dem Verantwortlichen umfassende Pflichten bei der Auswahl und Überwachung des Auftragverarbeiters. Darüber hinaus sind die betroffenen Personen hinreichend zu Unterrichten. Diesen Pflichten, insbesondere der Kontrolle, kann durch den Einsatz einer SPLITLCloud-Lösung in besonderem Maße Rechnung getragen werden, dazu unten Kapitel 3.

Gegenstand der Betrachtung in diesem Dokument ist die im Projekt SPLITCloud entwickelte Architektur mit besonderem Augenmerk auf Cloud-spezifische Risiken und ob und inwieweit diese durch die SPLITCloud-Architektur adressiert werden.

2.2 Schutzbedarfsbestimmung für die Gewährleistungsziele

In dieser Sektion wird der Schutzbedarf für verschiedene Gewährleistungsziele besprochen. Im Fokus stehen jene Risiken für Gewährleistungsziele und Aspekte, die spezifisch fürs Cloud-Computing sind, insbesondere solche, bei denen Systembetreiber als Angreifer agieren können. Die Beurteilung der Artikel 29 Datenschutz-Gruppe zum Cloud-Computing[39] nennt explizit die spezifischen Risiken des Cloud-Computing[40]. Die Artikel 29 Gruppe besteht aus Vertretern der Datenschutzaufsichtsbehörden aller Mitgliedstaaten der Europäischen Union wurde nach Art. 29 der Datenschutzrichtlinie (Richtlinie 94/46/EC) gegründet und soll unter anderem zur einheitlichen Anwendung des eurpäischen Datenschhutzrechts beizutraten. Für SPLITCloud sind von den dort genannten Risiken vor allem die Folgenden relevant:

- Fehlende Vertraulichkeit durch direkte Anfragen von Gesetzeshütern an den Cloud-Provider: Wie Vertraulichkeit auch gegenüber Systembetreibern und Systembetreibern, die von Dritter Seite zu Eingriffen gezwungen werden, sichergestellt werden kann ist ein Hauptfokus der vorliegenden Analyse. Insoweit nennt die Art. 29-Gruppe explizit das Risiko von Offenbarungen von Daten gegenüber Strafverfolgungsbehörden im EU-In- und -Ausland ohne wirksame Übermittlungsbefugnis.[41] Das besondere Risiko durch Angriffe oder

[39] Art. 29 WP 196 Seiten 5 und 6.
[40] Siehe Art. 29 WP 196 Kap. 2 „Data protection risks of cloud computing“ S. 5 und 6.
[41] Art. 29 WP 196 Kap. 2.

Pflichtverletzungen von Mitarbeitern und Insidern[42] wird durch die Einschaltung weiterer Dienstleister mit weiteren Dienstleistern dabei erhöht.

- Fehlende Intervenierbarkeit, wenn durch die Dynamik von Cloud-Anwendungen weitere Komponenten und Akteure in die Outsourcing-Kette aufgenommen werden, ohne dass die verantwortliche Stelle diesbezüglich hinreichende Unterrichtung und Einflussmöglichkeiten hat. In der Folge können auch die Betroffenenrechte nicht mehr umfassend gewährleistet werden.
- Mangelhafte Isolation von personenbezogenen Daten, die durch verschiedene virtualisierte Anwendungen verarbeitet werden und dabei ggf. auf dieselben Ressourcen (Hardware) zugreifen. Eine klare Trennung der Daten mehrerer Cloud-Kunden ist dabei sicherzustellen (Mandantentrennung).
- Mangelhafte Integrität durch das Risiko einer Kombination von personenbezogenen Daten von einer Vielfalt von Quellen (z.B. mehreren Mandanten).
- Mangelnde Transparenz durch Verarbeitung der Daten in mehreren Orten innerhalb oder außerhalb der EU.

Sekundär sind diese Risiken zu nennen, die von der Art. 29-Gruppe gleichsam genannt werden:

- Mangelhafte Verfügbarkeit durch Vendor Lock-In, da das Prüfobjekt ein Standard-Datenbankmanagement System (DBMS) verwendet und einfache Backups einen Lock-In vermeiden können.
- Mangelhafte Intervenierbarkeit, da in SPLITCloud präzise definierte Applikationen (Software as a Service) zur Anwendung kommen, welche die notwendige Intervenierbarkeit durchaus anbieten können. Da die vorliegende Analyse sich nicht auf die Pilotanwendung erstreckt, wird für weitere Beurteilungen auf die jeweiligen Anwendungen verwiesen.

Die für SPLITCloud besonders relevanten Risiken werden in der Untersektion über **Vertraulichkeit** analysiert, da Cloud-Dienste bei der Vertraulichkeit spezifische Risiken aufweisen (nachstehend 2.2.4). Der Vollständigkeit halber werden die anderen Gewährleistungsziele erörtert, jedoch mit geringerer Detailtiefe. So stellen sich

[42] Vergl. die Resultate der gesponsorten Studien von Interessenverbänden und Industrie: Bitkom/Holz, Datendiebstahl S. 9; Ponemon Institute, gesponsorte Studie Closing Security Gaps, S. 2.

identische Anforderungen wie die Möglichkeit, die Betroffenenrechte zu gewährleisten, ganz überwiegend auch bei einem in-house-hosting ganz ohne Cloud-Bezug. Die Aufnahme aller Gewährleistungsziele dient vorwiegend zur Demonstration, dass die vorliegende Analyse keine wichtigen Lücken offen lässt. Zu den allgemeinen rechtlichen Anforderungen wird auf die Darstellungen im SPLITCloud-Dokument „D.1.1 Datenschutzrechtliche Anforderungen an das SPLITCloud-Framework“ verwiesen. Die Darstellung orientiert sich an der Reihenfolge der Gliederung im Standard-Datenschutzmodell.

2.2.1 Datenminimierung

Das Gewährleistungsziel der Datenminimierung entspricht der Anforderung des Normgebers in Art. 5 Abs. 1 lit. c DSGVO, dass die Datenverarbeitung inhaltlich auf ein Minimum zu beschränken ist. Dieses Gewährleistungsziel ist vorrangig vor der der Prüfung der Modalitäten und der Gestaltung der Verarbeitungsprozesse zu prüfen und ohnehin Teil der bei den gesetzlichen Rechtsgrundlagen bereits über das Erforderlichkeitskriterium zu bewertenden Zulässigkeit der Verarbeitung. Das Standard-Datenschutzmodell definiert Datenminimierung wie folgt:

> „Datenminimierung konkretisiert und operationalisiert im Verarbeitungsprozess den Grundsatz der Erforderlichkeit, der von diesem Prozess insgesamt wie auch von jedem seiner Schritte verlangt, nicht mehr personenbezogene Daten zu erheben, zu verarbeiten und zu nutzen, als für das Erreichen des Verarbeitungszwecks erforderlich ist. Datenminimierung ist als proaktives Element datenschutzfreundlicher Technikgestaltung zu berücksichtigen: beginnend beim Design der Informationstechnik durch den Hersteller, über ihre Konfiguration und Anpassung an die Betriebsbedingungen, bis zu ihrem Einsatz in den Kernprozessen des Verfahrens wie auch in den unterstützenden Prozessen zum Beispiel bei der Wartung der verwendeten Systeme, von der Erhebung der personenbezogenen Daten über ihre Verarbeitung und Nutzung bis zur Löschung oder vollständigen Anonymisierung, über den vollständigen Lebenszyklus der Daten hinweg.“[43]

[43] DSK, SDM v1.0, S. 11.

Da die Erörterung in diesem Dokument generisch geführt wird, ohne einen spezifischen Zweck und damit verbundene personenbezogene Daten zur Hand zu haben, kann keine Aussage darüber gemacht werden, ob die Kategorien der verarbeiteten und verketteten Daten und die Anzahl der gesammelten Attribute der Datenminimierung genügen. Dies ist am Maß des konkret verfolgen Zwecks der Anwendung und der anwendbaren Rechtsgrundlage zu bemessen.

Maßnahmen die auch im Cloud-Kontext zur Umsetzung geeignet sind umfassen[44]:

- Bevorzugung automatisierter Verarbeitungsprozesse, die eine Kenntnisnahme personenbezogener Daten entbehrlich machen. Anwendbar ist dies vor allem für das Update von Software. Siehe hierzu die Ausführungen im Abschnitt Vertraulichkeit oben.
- Reduzierung von Verarbeitungsoptionen in Prozessschritten, jedenfalls soweit diese sich auf den Verantwortungsbereich des Cloud-Dienstes und nicht der Applikation selbst bezieht. Regelmäßig ist dies jedoch eine Frage der Gestaltung und der Voreinstellungen der jeweiligen fachspezifischen Applikation.
- Regelungen zur Kontrolle von Prozessen und Änderung von Verfahren. Als organisatorische Maßnahmen sind diese auf der Ebene des Cloud-Anbieters zu treffen. Soweit möglich können mittels SPLITCloud-Lösung auch Teile dieser Kontrolle auf den TOM übergehen.

Datenminimierung im Sinne, dass nur befugtes Personal Kenntnis von personenbezogenen Daten erlangen kann, ist Teil der oben geführten Diskussion zu Anforderungen an die Vertraulichkeit (siehe oben 2.2.4).

Die Löschung von Daten sobald sie nicht mehr benötigt werden ist weitgehend applikationsabhängig. Die Architektur des Prüfgegenstands sieht die Verwendung eines Standard-Datenbankmanagement Systems vor. Löschung von Daten in diesem Kontext ist eine Problematik für die etablierte Lösungen existieren. Dasselbe gilt für das mögliche Weiterleben von Daten in Backups, wobei zumindest für das Rückspielen längst gelöschter Daten entsprechende Vorkehrungen anhand zu treffen sind. Die Verwendung von Daten durch Cloud-Provider oder andere Drittparteien wird durch herkömmliche Verschlüsselung verhindert.

[44] Vergl. zum generischen Maßnahmenkatalog Datenminimierung: DSK, SDM v1.0, S. 30.

2.2.2 Verfügbarkeit

Mangelnde Verfügbarkeit durch das Versagen von Hardware ist in einem Cloud-Deployment viel weniger wahrscheinlich. Dies umfasst z.B. Möglichkeiten der automatischen Migration von Applikationen weg von Hardware die die ersten Anzeichen von Versagen zeigt[45] noch bevor Daten verloren gehen. Auch relevant sind eine einfachere Realisierung von Redundanz durch erleichterte Verfügbarkeit von Rechen- (VMs) und Speicherressourcen (SANs) und eine typische geographische Verteilung, die bessere Disaster Relisilience verspricht.

Dasselbe gilt für (distributed) Denial of Service Attacks, für welche Cloud-Provider üblicherweise über bessere Schutzmaßnahmen verfügen. Ein möglicher Vendor Lock-In kann durch die Verfügbarkeit von periodischen (z.B. täglichen) Backups in einem Standardformat beim Endkunden vermieden werden.

Normativ findet die Verfügbarkeit ihren Niederschlag in Art. 32 Abs. 1 lit. c) und d) DSGVO für den Umgang mit physischen oder technischen Zwischenfällen. Das Standard-Datenschutzmodell definiert Verfügbarkeit wie folgt:

> „Das Gewährleistungsziel Integrität bezeichnet einerseits die Anforderung, dass informationstechnische Prozesse und Systeme die Spezifikationen kontinuierlich einhalten, die zur Ausübung ihrer zweckbestimmten Funktionen für sie festgelegt wurden. Integrität bezeichnet andererseits die Eigenschaft, dass die zu verarbeitenden Daten unversehrt, vollständig und aktuell bleiben. Abweichungen von diesen Eigenschaften müssen ausgeschlossen werden oder zumindest feststellbar sein, damit sie berücksichtigt bzw. korrigiert werden können. Versteht man das Gewährleistungsziel Integrität als eine Form der Richtigkeit im Sinne des Art, 5 Abs. 1 lit. d DS-GVO, resultiert daraus der Anspruch, dass zwischen der rechtlich-normativen Anforderung und der gelebten Praxis eine hinreichende Deckung besteht, sowohl in Bezug auf technische Details wie auch im großen Zusammenhang des Verfahrens und dessen Zwecksetzung insgesamt.“[46]

Aus dem besonderen Blickwinkel des Datenschutzes sind vor allem Maßnahmen zu treffen, dass datenschutzspezifischen Anforderungen, also unter anderem die

45 Z.B., abnormal hohe Temperaturen.
46 DSK, SDM v1.0, S. 13f.

Umsetzung der Betroffenenrechte auf Auskunft, Berichtigung und Löschung, in einem angemessenem Zeitfenster genügt werden kann. Daneben sind die Interessen betroffener Personen an der Verfügbarkeit der Informationen zu berücksichtigen, welche z.B. im Gesundheitsbereich deutlich gesteigert sein können. Im Übrigen wird das Gewährleistungsziel der Verfügbarkeit primär durch geschäftliche Anforderungen des Cloud-Kunden bestimmt. So sind Verfügbarkeitsanforderungen kommerziellen Cloud-Einsatz im Zentrum des Interesses und werden – nicht zuletzt als ein maßgebliches Kriterium bei der Preisgestaltung – im Rahmen von service level agreements minutiös geregelt.

2.2.3 Integrität

Das Gewährleistungsziel der Integrität bezieht sich sowohl auf Prozesse und Systeme als auch auf die Unversehrtheit, Aktualität und Vollständigkeit der Daten. Vorwiegend sind Maßnahmen zur Umsetzung auf der Ebene der Anwendung zu treffen. Das Standard-Datenschutzmodell bestimmt dazu:

> „Das Gewährleistungsziel Integrität bezeichnet einerseits die Anforderung, dass informations-technische Prozesse und Systeme die Spezifikationen kontinuierlich einhalten, die zur Ausübung ihrer zweckbestimmten Funktionen für sie festgelegt wurden. Integrität bezeichnet andererseits die Eigenschaft, dass die zu verarbeitenden Daten unversehrt, vollständig und aktuell bleiben. Abweichungen von diesen Eigenschaften müssen ausgeschlossen werden oder zumindest feststellbar sein, damit sie berücksichtigt bzw. korrigiert werden können. Versteht man das Gewährleistungsziel Integrität als eine Form der Richtigkeit im Sinne des Art, 5 Abs. 1 lit. d DS-GVO, resultiert daraus der Anspruch, dass zwischen der rechtlich-normativen Anforderung und der gelebten Praxis eine hinreichende Deckung besteht, sowohl in Bezug auf technische Details wie auch im großen Zusammenhang des Verfahrens und dessen Zwecksetzung insgesamt.“[47]

Der Prüfgegenstand benutzt Standard-Technologien zur Datenspeicherung (d.h. DBMS) die z.B. durch Transaction Management Datenintegrität schützen. Zudem werden Einflüsse von Dritten bei einer Anwendung der SPLITCloud-Lösung durch Isolation und Vertraulichkeit weitgehend vermieden, was die Integrität zugutekommt. Auf Ebene des

[47] DSK, SDM v1.0, S. 13.

Cloud-Betriebs sollen Zuweisungen von Rechte und Rollen dokumentiert sein. Software und neue Prozesse sind vor einem Einsatz zu testen.

Weitergehende Anforderungen hängen vom zu evaluierenden Einsatzszenario ab, so wären hieran höhere Anforderungen zu stellen, wenn die Daten besonderen Nachweispflichten genügen müssen, z.B. als Nachweis korrekter Rechnungslegung nach steuer- und handelsrechtlichen Normen. Mit Blick auf den Datenschutz können vor allem die Logdateien über Zugriffe und Rechteänderungen durch den TOM-Administrator erhöhten Anforderungen unterliegen. Anforderungen an die Ebene der Anwendung würden darüber hinaus Einschränkungen bei Schreib- und Änderungsrechten, Einsatz von Prüfsummen erfordern.

2.2.4 Vertraulichkeit

Vertraulichkeit reduziert die Verfügungsgewalt und Kenntnisnahme von personenbezogenen Daten auf das zur Erfüllung der Zwecke der Datenverarbeitung Erforderliche und konkretisierend innerhalb von Organisationen auch mit Bezug zur jeweiligen Aufgabe einer Person mit Kenntnisnahmemöglichkeiten. Das Standard-Datenschutzmodell definiert:

> „Das Gewährleistungsziel Vertraulichkeit bezeichnet die Anforderung, dass keine Person personenbezogene Daten unbefugt zur Kenntnis nehmen kann. Unbefugte sind nicht nur Dritte außerhalb der verantwortlichen Stelle, mögen sie mit oder ohne kriminelle Absicht handeln, sondern auch Beschäftigte von technischen Dienstleistern, die zur Erbringung der Dienstleistung keinen Zugriff zu personenbezogenen Daten benötigen, oder Personen in Organisationseinheiten, die keinerlei inhaltlichen Bezug zu einem Verfahren oder zu der oder dem jeweiligen Betroffenen haben.“[48]

Die Anforderungen gelten auch im Verhältnis zum Auftragsverarbeiter. Art. 28 Abs. 3 lit. b DSGVO bestimmt, dass alle Mitarbeiter des Auftragnehmers zur Vertraulichkeit verpflichtet sein müssen. Diese Norm setzt den Grundsatz der Integrität und Vertraulichkeit aus Art 5 (1) im Bereich der Auftragsdatenverarbeitung um.[49]

Von den oben beschriebenen Akteuren ist lediglich der Verantwortliche, also die verantwortliche Stelle nebst den jeweils zur Erfüllung erforderlichen Mitarbeitern, originär

[48] DSK, SDM v1.0, S. 13f.
[49] Paal/Pauly, Artikel 28 DSGVO Rn. 43.

dazu berechtigt auf die Daten zuzugreifen. Die Erforderlichkeit einer Kenntnisnahme durch Auftragnehmer und andere Unberechtigte sollte dabei nach Möglichkeit bereits durch und organisatorische Maßnahmen vermieden und durch geeignete technische Maßnahmen verhindert werden. Der Umfang der zu ergreifenden Maßnahmen richtet sich dabei nach Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen, Art. 32 Abs. 1 DSGVO. Sind Daten von Berufsgeheimnisträgern nach § 203 StGB betroffen (z.B. Ärzte, Rechtsanwälte) dürfen Auftragnehmer oder gesonderte Schweigepflichtenbindung nach bisheriger deutscher Rechtslage gar keine Möglichkeit zur Kenntnisnahme erhalten, was nach Auffassung vieler deutscher Datenschutzaufsichtsbehörden der Länder einer Datenverarbeitung in der Cloud durch Berufsgeheimnisträger ausschließt. Diesbezüglich wird gegenwärtig eine Änderung des § 203 StGB im Entwurf[50] erörtert, der eine Auftragsdatenverarbeitung auch für Berufsgeheimnisträger ermöglicht – in diesem Fall müssen jedoch regelmäßig hohe, ggf. auch sehr hohe, Anforderungen an die Sicherstellung des Schutzes der Gewährleistungsziele gestellt werden. Insoweit vermag eine Gestattung der Auftragsdatenverarbeitung in § 203 StGB eine Rechtsgrundlage schaffen, bei der Bewertung des Risikos sind indes die besonderen Anforderungen an das Vertrauen der Patienten, Mandanten und Klienten dieser Berufe angemessen zu gewichten.

Dem engen Wortlaut des Art. 9 DSGVO folgend würde sich eine Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Art. 9 DSGVO ausschließen. Hierzu wird in der Literatur vertreten, dass ein solches Verständnis, die vom Normgeber gewollten Vorteile und Erleichterungen in diesem Bereich aufheben würde, weil Auftragsdatenverarbeitung nur in sehr beschränkten Maße statthaft wäre.[51] Der Hinweis in Abs. 3, dass der Vertrag die Arten der personenbezogenen Daten festlegen müsse indiziere eher, dass dies gerade die besonderen Kategorien von Daten erfasse.[52] Tatsächlich entspricht diese Auslegung den Bedürfnissen der Praxis, was nicht zuletzt auch durch die Bemühungen des nationalen Gesetzgebers zur Aufnahme der Auftragsdatenverarbeitung in den § 203 StGB unterstrichen wird. Die Schaffung und einer Rechtsgrundlage im Allgemeinen und das Vorliegen im konkreten Einzelfall wirkt

[50] Entwurf des BMJV, https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/ReGE_Neuregelung_Schutzes_von_Geheimnissen_bei_Mitwirkung_Dritter_an_der_Berufsausuebung_schweigepflichtiger_Personen.pdf?__blob=publicationFile&v=2.
[51] Paal/Pauly/Martini Art. 28 Rn. 10.
[52] Paal/Pauly/Martini Art. 28 Rn. 33.

sich jedoch nicht auf die Bewertung des Risikos aus. Hier wird die Verarbeitung besonderer Kategorien von Daten regelmäßig auf hohe oder sehr hohe Schutzbedarfe hinweisen, die ggf. eine Verarbeitung dieser Daten durch einen externen Cloud-Dienst ausschließen kann.

Zur Wahrung der Vertraulichkeit bei jeglicher Verarbeitung personenbezogener Daten in Cloud-Diensten sind daher Maßnahmen zu ergreifen, um den **Zugriff Unberechtigter auf die Daten des Systems zu verhindern** insbesondere in den folgenden drei Situationen: Während der *Übertragung* von Daten zwischen Systemkomponenten, während der *Speicherung* der Daten und während der *Verarbeitung* der Daten im System. Die konkreten Konsequenzen dieser Anforderungen werden im Folgenden im Detail besprochen.

2.2.4.1 Vertraulichkeitsschutz während der Datenübertragung

Wie aus Abbildung 2 (oben S. 11) ersichtlich wird, ist das SPLITCloud System auf mehrere Prozessoren verteilt, insbesondere dem PC des Anwenders und den Servern für Presentation Logic, Business Logic, und Datenbank. Dies erfordert die Übertragung von personenbezogenen Daten zwischen diesen Komponenten.

In verschiedenen Deployment-Varianten können die Sicherheitscharakteristiken der Netzwerke, welche für die Übertragung benutzt werden, sehr verschieden sein. So kann z.B. ein internes Netzwerk verwendet werden, das von äußeren Einflüssen durch Maßnahmen wie Firewalls weitgehend gegenüber Zugriffen Dritter geschützt ist. Öffentliche Netzwerke wie das Internet sind aber weit weniger geschützt. Die meisten Systeme benutzen auch öffentliche Netzwerke, z.B. für Maßnahmen der Disaster Recovery, wo die Speicherung der Daten in einem weit entfernten Ort die Übertragung über das öffentliche Internet erfordert.

Um zu beurteilen, ob der Schutz der Datenübertragung ausreichend ist, muss die Widerstandsfähigkeit verschiedener Maßnahmen gegen Angriffe ermittelt werden. Im Regelfall basiert die Maßnahme auf Verschlüsselung der Kommunikation zusammen mit der Authentisierung der Kommunikationspartner. Eine sichere Wahl von Verschlüsselungsalgorithmus und Parameter wird hier als gegeben vorausgesetzt; im Folgenden werden kritische Eigenschaften dieses Ansatzes diskutiert:

Welcher Abschnitt der Kommunikation wird verschlüsselt? Verschlüsselung kann den ganzen Weg zwischen zwei Kommunikationspartnern abdecken (sogenannte Ende-zu-Ende-Verschlüsselung) oder nur einen Teil der Übertragungsstrecke sichern. Der gesamte Kommunikationsweg kann auch unterbrochen sein und durch mehrere verschlüsselte Kanälen hintereinander aufgebaut werden.

Ein Beispiel von Ende-zu-Ende-Verschlüsselung ist eine TLS (HTTPS) Verbindung zwischen einem Web Browser und Server. Ein Beispiel von teilweiser Verschlüsselung ist die Verwendung eines Virtual Private Networks, bei dem die Kommunikation vor dem Eingangspunkt (z.B. einem Router) und nach dem Austrittspunk (z.B. ein Router auf der Gegenseite) nicht von der Maßnahme geschützt ist. Ein Beispiel von einer – in der Regel notwendigen – unterbrochenen Verschlüsselung ist ein Web Server der die Presentation Logic ausführt und mit dem Browser des Anwenders durch einen sicheren Kanal sowie mit der Datenbank im Back End durch einen zweiten sicheren Kanal kommuniziert. Auf dem System, das die Presentation Logic ausführt, liegen die Daten jedoch zwecks Verarbeitung im Klartext vor.

Von einer Sicherheitsperspektive ergeben sich für die Varianten der Verschlüsselung folgende Abstufungen:

- **Ende-zu-Ende-Verschlüsselung:** Diese bietet den besten Vertraulichkeitsschutz.
- **Unterbrochene Verschlüsselung** die mit mehreren Kanälen den gesamten Weg verschlüsselt.
- **Unvollständige Verschlüsselung** mit teilweiser Kommunikation im Klartext. Soweit diese in Teile in internen Netzwerken, z.B. auf der Seite eines Unternehmenskunden, erfolgt kann dies mit Blick auf Transparenz und Verfügbarkeit sogar beabsichtigt sein. Entstehende Vertraulichkeits-Risiken sind durch geeignete Schutzmaßnahmen im internen Netz aufzufangen.
- **Unvollständige Verschlüsselung** mit Übermittlungen von Klartext in einem **öffentlichen Netzwerk.** Ein Bruch der Vertraulichkeit steht konkret zu befürchten, so dass von einer solchen Gestaltung bei der Verarbeitung personenbezogener Daten in Auftragsverhältnissen abgesehen werden sollte.

Wer/Was genau wird authentifiziert?

Authentisierung von verschlüsselten Kanälen ist notwendig, so dass einerseits schützenswerte Daten nicht in die falschen Hände fallen, andererseits um sicher zu stellend dass die legitime Datenquelle abgefragt wird. Insoweit ist eine gesicherte Authentisierung wesentlicher Teil einer sicheren Verschlüsselungsstrategie. Authentisierung ist auch eine Voraussetzung für die Revisionierbarkeit, indem sie Verantwortung für Transaktionen klarstellt.

Technisch existieren viele Optionen für die Realisierung der Authentisierung. Zum Beispiel können die Endpunkte der Kommunikation authentisiert werden, oder aber nur ein Teil des Weges, wie z.B. ein Virtual Private Network das zwei Organisationen verbindet. Offensichtlich unterscheiden sich verschiedene Optionen in ihrer Granularität mit der sie Verantwortung für Transaktionen zuweisen.

Um die Sicherheitsstufe eines Authentisierungsansatzes zu verstehen, betrachten wir getrennt den Datenkonsument von der Datenquelle:

Beim **Datenkonsumenten** unterscheiden wir die folgenden Stufen:

- Eine Person authentisiert nicht nur einen sicheren Kanal sondern zusätzlich jede eingreifende Transaktion. Dies ist z.B. bei Online-Banken üblich, schützt vor Angriffen die legitim authentisierte Kanäle kapern, und unterstützt die präzisest mögliche Zuweisung von Verantwortung. Beispiele für Methoden zur Authentisierung einer Transaktion umfassen die erneute Eingabe eines One Time Passworts für jede Transaktion und die elektronische Signatur der Transaktion. Datenschutzrechtlich ist hier wegen der Möglichkeit von einer Verhaltens- und Leistungskontrolle zurückhaltend Gebrauch zu machen und diese Art der Authentifizierung auf besonders risikoreiche und wichtige Aktionen zu beschränken, z.B. Geldtransaktionen oder der Zuweisung besonderer Rechte auf Systemen durch Administratoren.
- Eine Person authentisiert das Ende eines Kanals.
- Das am Kanal angeschlossene Endgerät (wie z.B. eine Arbeitsstation) wird authentisiert.
- Eine Kommunikationskomponente (z.B. ein Router oder Hardware Proxy als Endpunkt eines VPNs) wird authentisiert so dass die Verantwortung für Transaktionen lediglich der gesamten Organisation zugewiesen werden kann.

Beim **Datenquellen** unterscheiden wir die folgenden Stufen:

- Eindeutige Authentisierung der Datenquelle. In Abbildung 2 könnte dies z.B. durch Authentisierung der Presentation Logic erfolgen, angenommen dass technische Maßnahmen den Zugriff von andern Komponenten auf die dahinter liegende Datenquelle verhindern.
- Authentisierung der Organisation.

Die folgenden **Stärken der Authentisierungsmethode** sollen unterschieden werden:

- Authentisierung basierend auf einem **kryptographischen Protokoll** mit einem Schlüssel der durch ein **Hardware Security Module** (Smart Card, Trusted Platform Module) vor Replikation geschützt ist oder in einem Offline Device (wie One Time Password Generator) verwaltet wird.
- Authentisierung basierend auf einem **kryptographischen Protokoll** mit einem Schlüssel der auf einem **Filesystem** abgelegt ist.
- Authentisierung **ohne Verwendung eines kryptographischen Schlüssels.** Beachte, dass ein One Time Password Generator einen

Andere Aspekte könnten hier berücksichtigt werden, wurden aber der Einfachheit halber ausgeschlossen. Ein Beispiel dafür ist die Bindung eines Hardware Tokens an eine Person (via PIN oder Biometrik). Eine detailliertere Diskussion dieser Aspekte finden sich z.B. in den Digital Identity Guidelines der US-Standardisierungsinstitution NIST.[53].

Wie gut sind die Zufallsgeneratoren?

Mehrere Aspekte in der Verschlüsselung und Authentisierung basieren auf der Generierung von Zufallszahlen. Beispiele dafür sind Kreation von zufälligen Sessionsschlüssel von verschlüsselten Kanälen oder das zufällige Schlüsselpaar mit dem sich eine Person authentisiert oder mit der sie elektronisch signiert. Ein anderes Beispiel sind die NONCE, zufällige Werte z.B. für die Verschlüsselung von Dateien, die nicht voraussehbar sein und nur ein einziges Mal verwendet werden dürfen.

Um Zufallszahlen hoher Qualität zu generieren wird eine sogenannte Entropiequelle benötigt. Auf Arbeitsstationen werden oft die Zeitpunkte von Tastendrücken als Entropiequelle verwendet; auf Servern ist es oft schwer, gute Entropiequellen zu finden.

Hoch entwickelte Angreifer können Verschlüsselungssysteme mit Zufallsgeneratoren schlechter Qualität angreifen. Deshalb unterscheiden wir die folgenden Sicherheitsstufen:

- Systeme mit **dedizierten Hardware Entropiequellen**.
- Arbeitsstationen ohne dedizierte Hardware Entropiequelle.
- Server ohne dedizierte Hardware Entropiequelle.

53 NIST SP-800-63. https://pages.nist.gov/800-63-3/sp800-63-3.html.

Entsprechend der jeweiligen Umsetzung im konkreten Einzelfall sind die erforderlichen Maßnahmen zur Gewährleistung einer sicheren Verschlüsselung zu ermitteln. Weil hier das Standarddatenschutzmodell die technischen Lösungen bewusst nicht konkret vorgibt, sondern die geeignete Zusammenstellung von Maßnahmen neutral verlangt, können an dieser Stelle keine konkreten Maßnahmenhinweise gegeben werden. Es sind angemessene Sicherheitsstufen zu wählen, wenn die Verschlüsselung den alleinigen Schutz der Daten während des Transports über offene Netzte dar oder verlangen die betroffenen Daten einen erhöhten Schutzbedarf.

2.2.4.2 Vertraulichkeitsschutz während der Speicherung der Daten

Die folgende Diskussion betrachtet das System wenn es nicht aktiv benutzt wird, aber personenbezogene Daten speichert. Dies schließt den Normalfall aus, wo der Anwender für die deklarierten Zwecke der Anwendung auf die Daten zugreift; dieser Fall wird unten in der Sektion „Schutz während der Verarbeitung von Daten“ analysiert. An dieser Stelle betrachten wir also alle andern Akteure, die auf die gespeicherten Daten zugreifen könnten.

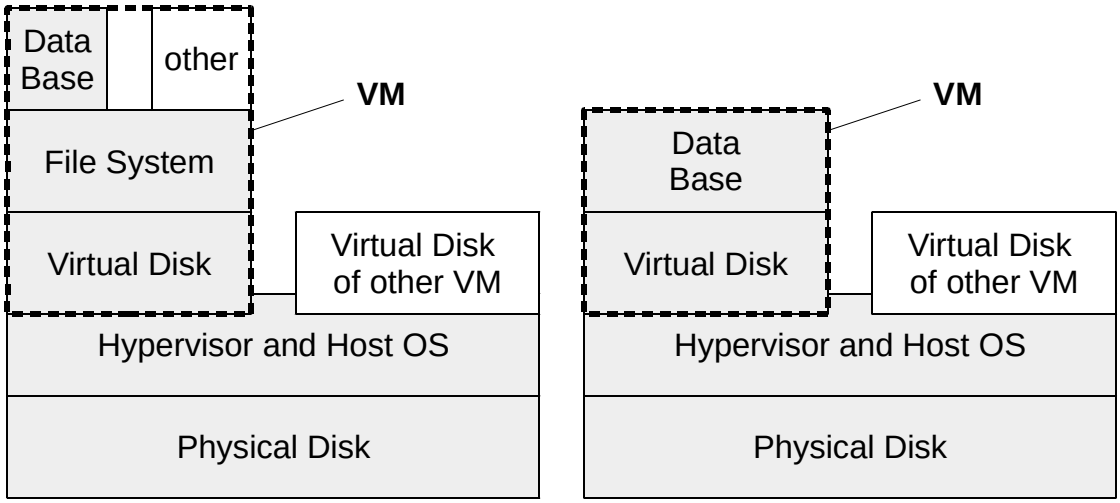

Abbildung 3 Details der Datenspeicherung

Wie in Abbildung 3 dargestellt, werden die Daten nur im Data-Base-Tier gespeichert. Zugriff auf die andern involvierten Server, wenn keine normale Verarbeitung stattfindet, ist deshalb unkritisch, da dort keine Daten gespeichert sind.

Abbildung 3 zeigt Details der Datenspeicherung. Insbesondere zeigt es zwei mögliche Architekturen, die von verschiedenen Datenbank Management Systemen (DBMS) benutzt werden: Entweder stützt sich das DBMS auf ein Filesystem (siehe links) oder es greift direkt auf einen Block Device (d.h., Festplatte oder Partition) zu (siehe rechts). In

einem Szenario mit Virtualisierung werden die Daten also entweder direkt oder indirekt auf einer virtuellen Festplatte gespeichert. Der Hypervisor abstrahiert von der physischen Festplatte und kreiert mehrere virtuelle Festplatten. Einige davon werden typisch von andern virtuellen Maschinen, die andern Zwecke dienen, benutzt.

Nicht illustriert in obiger Abbildung ist, dass in größeren Infrastrukturen die physische Disk nicht unbedingt auf dem Server belegen ist, sondern in einem über ein Netzwerk erreichbaren Storage Area Network (SAN) eingebunden sein kann. Das SAN verwaltet dabei mehrere physische Festplatten und bietet verschiedenen Servern virtualisierte Festplatten an. Wie die Daten über diese Festplatten verteilt werden wird vom SAN automatisch entschieden. Das SAN sorgt typischerweise für Redundanz und Skalierbarkeit; Festplatten können ohne Einfluss auf die darauf zugreifenden Anwendungen ersetzt und hinzugefügt werden, ohne dass Server davon betroffen sind. In einem SAN teilen sich deshalb mehrere Server und diverse Anwendungen für verschiedene Zwecke dieselbe Festplatten-Hardware.

In dieser Situation soll nun gewährleistet werden, dass keiner der Akteure auf die gespeicherten personenbezogenen Daten zugreifen kann.

Die folgenden Zugriffe sollen vermieden werden:

- **Kenntnisnahme** von personenbezogenen Daten **durch Systembetreiber**, die aber auch für legitime Zwecke Zugriff auf den (virtuellen) Datenbank-Server benötigen. Solche zulässigen aber zu schützenden Vorgänge umfassen u.a. die Folgenden:
  - Backup und Recovery der Datenbank
    - möglicherweise mit verschiedenen Prozessen für Routine-Backup und Disaster Recovery.
  - Update der DBMS Software, möglicherweise mit
    - Veränderung der Datenstruktur für die neue Version (Schema Evolution)
  - Update des Betriebssystems
  - Hardware Update, vor allem der Austausch von Festplatten
- **Kenntnisnahme** von personenbezogenen Daten **durch Unbefugte Dritte**, entweder durch
  - Zugang zum Server

- Zugang zu einer entsorgten (vielleicht defekten) Festplatten

- **Kenntnisnahme** von personenbezogenen Daten **durch Hersteller von Software**, inklusive von
  - DBMS Software
  - Betriebssystem
  - Hypervisor
  - **Kenntnisnahme** von personenbezogenen Daten **durch Hersteller von Hard- und Firmware** inklusive von Komponenten wie Server und SAN.

Die wichtigste generische Maßnahme gegen solche Kenntnisnahmen ist sicherlich die **Verschlüsselung**. Wie aus Abbildung 3 ersichtlich ist, soll diese Verschlüsselung am besten spezifisch für die Datenbank sein; wenn die Verschlüsselung erst an einer tieferen Ebene (z.B. der physischen Festplatte) angreift, bleibt die Möglichkeit, dass Prozesse, die einem andern Zweck dienen, auf die Daten im Klartext, also vor der Verschlüsselung zugreifen können. Falls die Verschlüsselung erst auf tieferen Ebenen erfolgt werden alternativ sehr starke Maßnahmen zur Isolation von Zwecken (und damit VMs) benötigt[54].

Eine sehr attraktive, aber nicht die einzig mögliche Lösung für die Verschlüsselung sind hier DBMS-spezifische Technologien wie Transparent Data Encryption,[55] welche spezifisch für den Schutz von „Data at Rest“ kreiert wurden. Diese decken sowohl die eigentliche Datenbank auf Festplatten, als auch mögliche Sicherheitskopien ab. Schlüssel können optional auch auf einem Hardware Security Module verwaltet werden.[56]

Mit solcher Verschlüsselungstechnologie können Zugriffe der meisten oben genannten Akteure verhindert werden. Die **Ausnahme** sind diejenigen Systembetreiber, welche entweder die Rolle des **Datenbank-Administrators** innehaben, oder sich diese einfach aneignen können (wie z.B. der „***root*** user“ der VM). Da der Datenbankadministrator den

54 Ein Beispiel für eine solche starke Maßnahme ist sVirt (https://rwmj.wordpress.com/2011/05/24/what-is-svirt/) das Mandatory Access Control (SELinux) für die Separation von virtuellen Maschinen einsetzt.
55 Microsoft, https://msdn.microsoft.com/en-us/library/bb934049.aspx, weitere Nachweise unter https://en.wikipedia.org/wiki/Transparent_Data_Encryption;
56 Microsoft, https://msdn.microsoft.com/en-us/library/bb895340.aspx.

Hauptschlüssel der Transparent Data Encryption kontrolliert, kann diese besprochene Technologie diese Rolle nicht effektiv von Zugriffen ausschließen (siehe z.B. Otey[57]).

Verschlüsselung auf Datenbank-Ebene bietet damit schon genügenden Schutz für einige der oben genannten legitimen Tätigkeiten durch Systembetreiber. Insbesondere umfassen diese die Updates von Hardware, Betriebssystem, und DBMS Software, da sie von einem Benutzer ohne die Rolle des Datenbank- oder Systemadministrators („*root*“) durchgeführt werden können.

Der Schutz gegen **Kenntnisnahme** von schützenswerten Daten **durch Datenbank- und Systemadministratoren** werden im Folgenden näher diskutiert. Dazu werden vorerst mögliche Schutzmaßnahmen in der Reihenfolge von aufsteigender Stärke diskutiert.

- **Organisatorische Maßnahmen:** Diese bieten den schwächsten Schutz gegen unerwünschte Kenntnisnahme von personenbezogenen Daten. Dabei werden betroffene Administratoren durch verschiedene Maßnahmen auf die Problematik aufmerksam gemacht (awareness), in den richtigen Verhaltensweisen unterrichtet und wenn möglich vertraglich zu einem korrekten Verhalten verpflichtet. Wieweit solche organisatorischen Maßnahmen, muss jeweils im konkreten Fall abgeklärt werden.
- **Überprüfbarkeit des korrekten Verhaltens und Verantwortungszuweisung bei Verstößen:** Verschiedene technische Maßnahmen dienen dazu, inkorrektes Verhalten von Akteuren nachweisen zu können und den Handelnden eindeutig identifizieren zu können, der gegen Regeln verstoßen hat.

  Der technische Grundbaustein für eine solche Maßnahme ist das „**Logging**“, d.h. die Aufzeichnung welche Aktionen von welchen Akteuren ausgeführt werden. Technische Maßnahmen sind notwendig um die Verfügbarkeit, Vollständigkeit, und Integrität dieser Aufzeichnungen (Logs) zu garantieren. In einem regelmäßigen Audit werden dann die Aufzeichnungen auf Unregelmäßigkeiten hin untersucht. Wenn möglich können Audits teilweise automatisch ausgeführt werden. Wird ein Verstoß aufgedeckt, dienen die Aufzeichnungen als Grundlage für eine forensische Untersuchung mit dem Ziel, den genauen Schaden und die Verantwortlichen zu ermitteln.

[57] Otey, SQL-FAQ, FAQ Nr . 3, “Does TDE prevent the security administrator or database administrator from seeing the data in the database?”

Verfügbarkeit, Vollständigkeit, und Integrität: Offensichtlich ist Überprüfbarkeit nicht einsetzbar, wenn Aufzeichnungen gelöscht oder modifiziert werden können, oder wenn ein zu überwachender Akteur die Aufzeichnungsmechanismen unentdeckt ausschalten kann. Verschiedene technische Maßnahmen sind möglich, um die Effizienz dieser Maßnahme zu garantieren:

- Aufzeichnungen werden von einer **vertrauenswürdigen Drittpartei** (Trusted Third Party) verwaltet. Da ein inkorrekt handelnder Akteur (und möglicherweise seine Organisation) Interesse daran hat, seine Spuren zu verwischen, ist eine Speicherung der Aufzeichnungen durch den Akteur (oder seiner Organisation) selbst nicht unbedingt sicher. Der Versand jedes Aufzeichnungselements (Log Entry) in Echtzeit an eine vertrauenswürdige Drittpartei ist daher deutlich sicherer. Die Logdateien bedürfen in der Regel ihrerseits Maßnahmen zur Sicherstellung der Vertraulichkeit z.B. durch Verschlüsselung.
- Um die Integrität von Aufzeichnungen zu unterstützen, sollten speziell dafür entwickelte **„Tamper Evidente" Formate** verwendet werden. Der Stand dieser Technologie wird in der gängigen Fachliteratur ausgiebig beschrieben.[58]
- Aufzeichnungen sind nur dann vollständig, wenn die dafür verantwortlichen Systemkomponenten (wie z.B. *auditd* und *syslogd* in Linux) ununterbrochen und in unveränderten Version und Konfiguration laufen. Dies kann z.B. durch **remote attestation** basierend auf einem **Trusted Platform Module** von einer vertrauenswürdigen Drittpartei regelmäßig geprüft werden.
- **Mandatory Access Control**: Die meisten Betriebssysteme implementieren Discretionary Access Control[59] bei denen Zugangsrechte für Ressourcen (wie z.B. Dateien) einfach modifiziert werden können. Optional ist für viele Betriebssysteme auch Mandatory Access Control[60]

[58] Siehe z.B. https://www.noao.edu/noao/staff/yao/paper.pdf, https://www.schneier.com/academic/paperfiles/paper-auditlogs.pdf, http://www.ub.utwente.nl/webdocs/ctit/1/00000099.pdf, https://www.usenix.org/legacy/event/sec09/tech/slides/crosby.pdf, http://cs.unc.edu/~fabian/courses/CS600.624/building-search.pdf

[59] https://en.wikipedia.org/wiki/Discretionary_access_control

[60] https://en.wikipedia.org/wiki/Mandatory_access_control

verfügbar. Beispiele dafür sind *Security Enhanced Linux*[61] (*SELinux*) oder *AppArmor*[62] für Linux und *Mandatory Integrity Control*[63] in Windows Vista und Server 2008. Mandatory Access Control erzwingt die Einhaltung einer zentral definierten Berechtigungs-Policy. Deshalb werden Systeme mit Mandatory Access Control auch oft als „gehärtet" bezeichnet. Gehärtete Systeme erschweren es beträchtlich, dass Zugangsverstöße nicht in den Aufzeichnungen aufgenommen werden und damit unentdeckt bleiben.

Zuweisung von Verantwortung: Genauso wichtig wie zu wissen, auf welche Daten unberechtigt zugegriffen wurde, ist zu erfahren, wer zugegriffen hat. Zentral für diese Frage sind Identitäten, sowohl von Personen (Akteuren) als auch Systemkomponenten. Die Zuweisung von Verantwortung ist dann nicht möglich, wenn Akteure falsche Identitäten annehmen können (Impersonation), entweder um sich als rechtmäßigen Nutzer zu präsentieren, oder die Verantwortung an Andere abzuschieben.

Zentral bei der Beurteilung des Identitätsmanagements in einem System ist, ob der Ausgeber der Identitäten (z.B. eine Zertifizierungsstelle für digitale Zertifikate oder ein Identity Provider im föderierten Identitätsmanagement) ein Interesse haben könnte, einen unrechtmäßigen Zugang zu vertuschen. Aus diesem Grund könnte eine Drittpartei eine bessere Wahl für diese Rolle darstellen, als den Betreiber des Systems für den auch die kritischen Akteure des Datenbank- und Systemadministrator arbeiten.

Des Weiteren sind digitale Identitäten, die von mehreren Akteuren geteilt werden können, zu vermeiden. In Unix Systemen könnte dies z.B. der „*root*" Benutzer sein, der von mehreren Systemadministratoren verwendet werden könnte.

Die stärkste Form, Verantwortung zuzuweisen, geht über die einmalige Anmeldung am System (Login) hinaus und authentifiziert jede kritische Aktion oder Transaktion separat. Dies kann z.B. durch erneute Abfrage eines One Time Passwords oder durch digitale Signatur einer Systemanfrage geschehen.

Für die Diskussion der Überprüfbarkeit des korrekten Verhaltens von Akteuren ist es auch wichtig zu wissen, welche die kritischen Aktionen sind, die aufgezeichnet

[61] https://selinuxproject.org/page/Main_Page
[62] http://wiki.apparmor.net/index.php/Main_Page
[63] https://en.wikipedia.org/wiki/Mandatory_Integrity_Controle

werden müssen. Wie oben besprochen werden die gespeicherten Daten durch Verschlüsselung schon ausreichend gegen die meisten Akteure geschützt. Eine mögliche unrechtmäßige Kenntnisnahme von Daten ist dann lediglich von Datenbank- und Systemadministratoren möglich. Deshalb müssen Datenzugriffe dieser Akteure unbedingt aufgezeichnet werden.

Darüber hinaus müssen alle Aktivitäten aufgezeichnet werden, welche die Aufzeichnung von illegitimem Verhalten verhindern könnte. Dies betrifft vor allem Aktivitäten von Systemadministratoren in Bezug auf diejenigen Systemkomponenten und deren Konfiguration, welche die Aufzeichnung regeln, welche Netzwerke (benötigt für Remote Attestation oder Logging bei Drittparteien) unterbrechen und auf Aktivitäten die Zugriffsrechte ändern.

Mögliche Aktivitäten von externen Angreifern müssen auch detailliert aufgezeichnet werden um Angriffe zu erkennen[64], abzuwehren, und den davongetragenen Schaden genau identifizieren zu können.

Insbesondere in verteilten Systemen, wie sie auch in SPLITCloud Verwendung finden, ist die absolut präzise Aufzeichnung der Zeitpunkte von Aktionen unerlässlich. Dazu müssen alle teilnehmenden Systeme über das Internet mit einer Atomuhr synchronisiert werden (z.B. durch Verwendung des *Network Time Protocol*).

- **Verwendung von automatischen Prozeduren**: Datenbankadministratoren müssen oft für legitime Zwecke auf personenbezogene Daten zugreifen. Dazu sollten aber vor allem automatisch ausführbare Prozeduren verwendet werden. Diese haben mehrere datenschutzrechtliche Vorteile:
  - Der Betreiber des Verfahrens benötigt keinen direkten Zugriff zu Daten. Aus diesem Grund kann eine Kenntnisnahme vermieden werden.
  - Wie genau auf Daten zugegriffen wird ist durch das Verfahren im Detail dokumentiert.
  - Die Funktionsweise des Verfahren kann (z.B. vor ihrem ersten Einsatz) von Dritten geprüft werden, ohne Zugang zu den Daten zu benötigen.

[64] Intrusion Detection.

Maßnahmen, mit denen man die Funktionalität eines System auf eine Menge von automatischen Prozeduren reduzieren kann, werden unten unter „Technische Verhinderung oder Begrenzung des Zugriffs“ besprochen.

- **Vier-Augen Prinzip** sieht vor, dass ein Akteur alleine keinen unrechtmäßigen Zugriff zu kritischen Daten haben darf. Wo eine Gefahr der Unrechtmäßigkeit besteht, kann deshalb mit technischen oder organisatorischen Maßnahmen erzwungen werden, dass immer mindestens zwei Akteure (also vier Augen) beteiligt werden müssen.

  Dieses Prinzip kann weiter von Personen auf Organisationen ausgeweitet werden. Dies wurde z.B. oben schon für das Logging durch eine Drittpartei verwendet. Das Verstecken eines unrechtmäßigen Zugriffs wäre dann nur durch die Zusammenarbeit zweier Organisationen möglich.

  Das Vier-Augen-Prinzip kann manchmal mit einfachen technischen Mitteln implementiert werden. Ein Beispiel ist das Verschicken von Logging Daten, mit vorhergehender Verschlüsselung mit dem öffentlichen Schlüssel (public key) des Empfängers. Ein anderes Beispiel[65] nützt eine Zwei-Faktor-Authentisierung mit dem Passwort eines Akteurs und der Handynummer eines zweiten.

  Das Vier-Augen-Prinzip erfordert aber auch oft auch eine spezifische Unterstützung in der Systemarchitektur. Insbesondere muss die Architektur eine Trennung von Rollen und Rechten ermöglichen. Die entsprechenden Systemkomponenten und damit Rollen müssen dann im Deployment den geeigneten Akteuren und Organisationen zugewiesen werden.

- **Technische Verhinderung des Zugriffs auf geschützte Daten.** Der bei weitem beste Schutz gegen unerwünschte Kenntnisnahme von personenbezogenen Daten sind technische Maßnahmen, die Zugriffe auf diese Daten verhindern. Dies ist bei gespeicherten Daten (Data at Rest) für die meisten Akteure bei geeignetem Umgang mit den Schüsseln schon durch Verschlüsselung erreichbar; die folgende Diskussion betrachtet deshalb lediglich den Zugriff durch Datenbank- und Systemadministratoren.

  Zugriff auf Daten seitens von Administratoren kann sicher dann verhindert werden, wenn diese Personen überhaupt nicht auf das System zugreifen können.

[65] http://security.stackexchange.com/questions/81916/four-eyes-authentication-for-command-execution-on-linux-os-level

Dies kann z.B. über eine Deaktivierung der Systemanmeldefunktion (Login) geschehen. In einem Unix System kann z.B. sichergestellt werden, dass in /etc/passwd keinem Benutzer eine Login-Shell zur Verfügung steht. Weiterhin können Systemanmeldungen durch Deaktivieren aller Login-Daemons (wie z.B. ssh oder telnet) vermieden werden. Zusätzlich ist es möglich, die Netzwerkzugänge des Systems so zu kontrollieren, dass ein kryptographischer Schlüssel für einen Zugriff notwendig ist. Dies kann z.B. durch Virtual Private Networks (VPNs) realisiert werden. Systemadministratoren können dann ausgeschlossen werden, indem sie keinen solchen Schlüssel erhalten.

Ein völliger Ausschluss von Administratoren vom System verunmöglicht einerseits die Kenntnisnahme von geschützten Daten, verhindert aber andererseits auch die legitimen Eingriffe auf das System seitens dieser Akteure. Aus diesem Grund ist es oft angebracht, dass eine Untermenge der Funktionalität, die einem Administrator normalerweise zur Verfügung steht, wieder zugänglich gemacht wird. Dies kann z.B. durch die Kreation einer Schnittstelle für die „Fernsteuerung“ des Systems erreicht werden. Nach Deaktivierung der normalen Systemanmeldung kann das System dann lediglich über Befehle an die Schnittstelle gesteuert werden. Diese Schnittstelle legt nur die gewünschte Untermenge der Funktionalität offen, wie z.B. eine Serie von vordefinierten Prozeduren. Dieses Prinzip wird z.B. auch von Smartcards verwendet, wo Funktionalität, wie z.B. Zugriff auf private Schlüssel, nicht über die Schnittstelle angeboten wird.

Das einschlägige technische Forum *Stackexchange*[66] nennt als zusätzlichen oder alternativen Ansatz zur Beschränkung von Administratoren das *Mandatory Access Control*. In diesem Ansatz ist eine Beschränkung von Akteuren möglich, ohne dass die Systemanmeldung deaktiviert werden muss und ohne die Realisierung einer Schnittstelle, die die gewünschte Funktionalität freilegt. Dabei wird in Policies (z.B. in *SELinux*) oder in Access Control Lists (z.B. in *grsecurity*) festgelegt, welcher Benutzer oder Prozess auf welche Ressourcen zugreifen kann. Ressourcen umfassen Entitäten wie z.B. Dateien (inklusive ausführbarer Programme), Äste eines Filesystems oder Netzwerk Ports. *Mandatory Access Control* kann alle Benutzer, inklusive *root*, den Zugang zu Ressourcen verweigern. Dies verunmöglicht einerseits den direkten Zugriff auf geschützte

[66] http://stackexchange.com/

Daten, ermöglicht aber andererseits die Ausführung von automatischen Prozeduren.

Unabhängig davon, welche Maßnahmen den Zugriff auf Daten verhindert, ist es wünschenswert zu kontrollieren, dass diese Maßnahmen aktiv und unverändert bleiben. Dies kann durch Methoden wie Trusted Boot oder UEFI Secure Boot, als auch Remote Attestation verifiziert werden.

2.2.4.3 Vertraulichkeitsschutz während der Verarbeitung der Daten

Die folgende Diskussion betrachtet das System wenn es aktiv benutzt wird. Der Anwender greift hier für zulässige Zwecke auf die Daten zu. Der Anwender ist der einzige Akteur, der rechtmäßig auf die Daten oder die zur Aufgabenerfüllung erforderlichen Daten zugreift; die personenbezogenen Daten sollten deshalb gegenüber allen andern Akteuren geschützt werden. Bei normalem Betrieb gibt es keine legitimen Zugriffe durch Systembetreiber (u.a. Administratoren, Rechenzentrumsmitarbeiter und andere Mitarbeiter des Auftragsdatenverarbeiters). Diese können nur während der Unterbrechung des normalen Betriebs stattfinden und wurden deshalb oben in der Diskussion des Schutzes während der Datenspeicherung betrachtet. Eine Beschränkung der Rechte einzelner Anwender im Rahmen der Anwendung ist an dieser Stelle nicht zu erörtern. Die Umsetzung des anwendungsinternen Rechte- und Rollenkonzepts findet auf der Ebene der Anwendung selbst statt, so dass im Musteranwendungsfall die Anwendung selbst Rechte und Rollen für den Zugriff auf die Zählerdaten und solche für fertige Rechnungen und Zahlungsdaten abbilden muss.

Um den Schutz vor unerwünschtem Datenzugriff durch Systembetreiber zu diskutieren, ist zu beschreiben, wo und in welcher Form Daten im System existieren und welche Akteure auf welche Weise zugreifen können. Dazu dient Abbildung 4. Die Figur zeigt einen der drei Tiers von Abbildung 1. Alle drei Tiers teilen dieselbe Architektur.

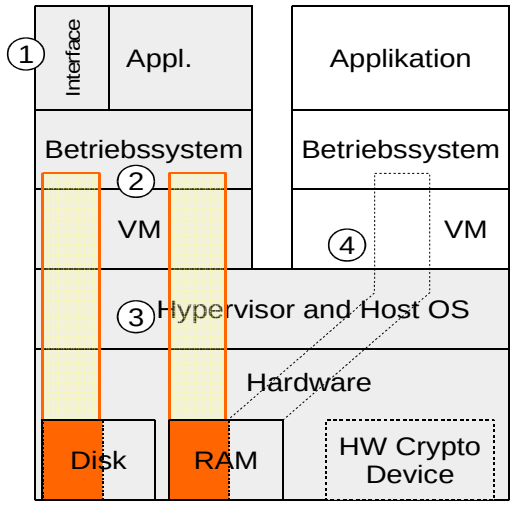

Abbildung 4 Ein Applikation-Tier während der Datenverarbeitung

Mit leicht grauer Schattierung sind die Systemkomponenten markiert, welche zur eigentlichen Applikation gehören. Die Figur deutet an, dass auf demselben Hypervisor, und somit derselben Hardware, auch andere Applikationen in anderen virtuellen Maschinen laufen können.

Personenbezogene Daten und Schlüssel sind während des Betriebs entweder im RAM oder auf der Festplatte gespeichert. Wenn Daten verarbeitet werden, müssen diese im RAM gespeichert werden. Hier ist auch eine Verschlüsselung zumindest im Moment der Verarbeitung nicht möglich. Auf der Festplatte können personenbezogene Daten auf dem Presentation- und Business-Tier als temporäre Files existieren, und auf dem Database-Tier auch als eigentliche Datenbank oder Datei. Im Gegensatz zu RAM können auf Festplatten Daten immer verschlüsselt werden.

Falls Daten verschlüsselt werden, existieren verschiedene Möglichkeiten für die Verwaltung der Schlüssel. Für die eigentliche Ver- und Entschlüsselung gibt es aber nur zwei Optionen: Entweder residiert der Schlüssel im RAM und die kryptografischen Operationen werden vom Prozessor der Plattform ausgeführt, oder der Schlüssel residiert geschützt in einem spezifischen Hardware Modul welches seinen eigenen Prozessor besitzt. Die zweite Option ist in der Abbildung mit dem „HW Crypto Device“ angezeigt.

Festplatte und RAM werden in einer wenig abstrahierten Form direkt auch in höherliegenden Softwareschichten gesehen, insbesondere im Hypervisor, der virtuellen Maschine und dem darauf sitzenden Betriebssystem. Typischerweise bilden sich die abstrahierten Festplatten und RAM aus einer Partition ihres physischen Äquivalents ab.

Offensichtlich kann diese Abbildung vom Virtuellen auf das Physische durch Strategien wie Swapping weiter kompliziert werden.

Basierend auf Abbildung 4 werden nun verschiedene Zugangswege zu den Daten identifiziert:

- Zugriffsweg 1: Der Zugang des legitimen Anwenders ist durch eine Schnittstelle der Applikation (im Presentation-Tier), die über ein Netzwerk von einem Web Browser benutzt wird. Die andern zwei Tiers haben eine ähnliche Schnittstelle, auf die der benachbarte Tier zugreift. Über diesen Weg können direkt personenbezogene Daten abgefragt werden. Während über andere Zugriffswege nur diejenigen Daten eingesehen werden können, die im Moment verarbeitet werden, sind über diesen Weg alle Daten verfügbar. Um sicher zu stellen, dass nur der rechtmäßige Anwender oder Tier Zugriff zu dieser Schnittstelle hat, muss die Applikation oder das System Nutzer oder Tier authentisieren und autorisieren. Jeder Akteur, der sich als legitimer Nutzer oder legitime Tier ausgeben kann, hat durch diesen Weg Zugriff auf die Daten.
- Zugriffsweg 2: Ein weiterer Weg ist der Zugriff auf das abstrahierte RAM und Festplatte vom Betriebssystem der Applikation her. Jeder Akteur mit Zugriff auf das Betriebssystem kann auf die Daten zugreifen. Für Zugriffe auf die Festplatte ist hier wichtig, in welcher (welchen) Softwareschicht(en) die Daten verschlüsselt werden. Geschieht dies z.B. erst im Hypervisor[67], dann sind die Daten in der Schicht des Betriebssystems unverschlüsselt zugänglich; wenn die Daten schon von der Applikation, z.B. einem DBMS, verschlüsselt werden, dann benötigt man für einen Zugriff auch den Schlüssel.
- Zugriffsweg 3: Zugriff auf die Daten kann auch vom Host Betriebssystem her erfolgen.
- Zugriffsweg 4: Ein weiterer Weg ist der Zugriff von einer andern virtuellen Maschine nach Überwindung der Isolationsmaßnahmen des Hypervisors.

Im Folgenden werden die verschiedenen Zugriffswege weiter erläutert, indem Schutzmaßnahmen gegen die Kenntnisnahme verschiedener Akteure beschrieben werden.

[67] Z.B. in Virtual Box https://blogs.oracle.com/scoter/entry/virtualbox_5_new_enhancement_and

- Zugriffsweg 1: Dieser Weg ist allen Akteuren offen. Da der Zugriff über ein Netzwerk erfolgt, wurden die meisten Schutzmaßnahmen schon oben für die Übertragung von Daten besprochen. Auch das Identitätsmanagement als wichtigste Angriffsfläche wurde schon diskutiert.

  Offensichtlich haben die Akteure, die für das Identitätsmanagement und die Zugriffs-Policy verantwortlich sind, besonders einfache Möglichkeiten für einen Zugriff. Z.B. kann ein Systemadministrator, der den Authentisierungsschlüssel des Business-Tiers besitzt, auf alle Daten des Database-Tiers zugreifen. Ähnlich kann der System- oder Datenbankadministrator, der die Zugriffsberechtigungen der Datenbank steuert sich einfach Zugriff gewähren.

  Schutzmaßnahmen sollen deshalb den Zugriff dieser privilegierten Akteure entweder technisch verhindern (tamper proof), oder sonst zumindest (durch Logging und Auditing) ersichtlich machen (tamper evident). Dies betrifft vor allem Zugriff zu Systemen und Komponenten, welche Identitäten ausgeben, Credentials (wie z.B. Schlüssel) verwalten, oder (Zugriffs-) Policy definieren.

  Schließlich können auch Schlüssel, die kopiergeschützt in einem Hardware Security Module gespeichert sind, einen Zugriff nicht verhindern. Insbesondere ist es immer noch möglich, sich in einen legitim authentisierten sicheren Kanal für illegitime Zwecke anzueignen.

- Zugriffsweg 2: Dieser Weg kann von allen Akteuren verfolgt werden, die im Guest Betriebssystem der virtuellen Maschine Zugriff auf RAM, kritische Dateien, oder (virtuelle) Festplatten haben. Die einzigen legitimen Zugriffe während des Betriebs der Applikation kommen von den Prozessen der Applikation selbst. Zugriffe von normalen Benutzern vor allem durch eine Shell sind zu vermeiden. Am wahrscheinlichsten sind solche Zugriffe seitens (i) Systemadministratoren (inklusive dem *root* user) des Guest Betriebssystems und (ii) externe Angreifer, die durch Schwachstellen der Applikation (z.B. durch den Web Server) sich Zugriff auf die Virtuelle Maschine verschaffen.

  (i) Es gibt eine Vielzahl von Maßnahmen, die vermeiden dass Benutzer, inklusive Administratoren, während des normalen Betriebs auf das System zugreifen. Diese umfassen unter anderem die Folgenden:

  - Kontrolle des Netzwerkzugriffs, um ungewollte Benutzer fernzuhalten (e.g., durch VPN)

- Maßnahmen die während des normalen Betriebs eine Systemanmeldung von Benutzern vermeiden (z.B. durch Betrieb der Applikation in einem spezifischen Unix *run level* der keine *getty* Prozesse anbietet oder durch die Vermeidung von login-fähigen Daemons wie *sshd*).
- Automatische Überwachung von Systemanmeldungen während des Betriebs und Alarmierung durch Infrastruktur Monitoring Software wie *Nagios*[68].

(ii) Schutzmaßnahmen gegen externe Angreifer zielen vor allem auf die Vermeidung von Schwachstellen in von außen zugänglichen Schnittstellen des Systems. Dies umfasst Maßnahmen wie schnelle Anwendung von sicherheitskritischen Updates und Härten (hardening) der laufenden Applikationen und des Betriebssystems. Härten umfasst Techniken wie Memory Randomization, die gegen gewisse Klassen von Angriffen schützen kann oder bessere Isolation von Prozessen, Applikationen und Benutzern durch Techniken des Mandatory Access Controls. Auch die Verwendung von Intrusion Detection Systems kann helfen, Angriffe zu entdecken und abzuwehren.

- Zugriffsweg 3: Dieser Weg ist den Systemadministratoren des Host Betriebssystems offen. Diese müssen selbst während des Betriebs der Applikation die Möglichkeit haben, den Hypervisor zu verwalten, z.B. um andere virtuelle Maschinen einzurichten, zu stoppen, oder zu starten.

  Maßnahmen, die verhindern, dass diese Systemadministratoren auf personenbezogene Daten zugreifen können, umfassen unter anderem die folgenden:

  - Automatisierung der notwendigen Verwaltungsarbeiten am Hypervisor durch vordefinierte Prozesse. Diese können z.B. durch Cloud Management Systeme wie OpenStack[69] zur Verfügung gestellt werden. Damit sind Systemanmeldungen durch den Systemadministrator unnötig.
  - Limitation der Zugriffsrechte der Administratoren (inklusive dem *root* users) auf kritische Files durch oben genannte Methoden wie Deaktivierung der Systemanmeldung oder *Mandatory Access Control* (siehe oben).

[68] https://www.nagios.org/
[69] https://www.openstack.org/

Zugriffsweg 4: Dieser Weg wird von allen Maßnahmen verhindert, die virtuelle Maschinen voneinander isolieren. Die meisten werden direkt vom Hypervisor implementiert. Darüber hinaus können Methoden des *Mandatory Access Controls* verwendet werden, um die Isolation darüber hinaus zu garantieren (siehe z.B. sVirt[70]).

Damit ist die Diskussion der möglichen Maßnahmen zur Gewährleistung der Vertraulichkeit abgeschlossen. Sie hat für Daten während der Übertragung, Speicherung und Verarbeitung analysiert, welche Akteure wie Kenntnis von personenbezogenen Daten gewinnen können. Auf dieser Basis wurden mögliche technische und organisatorische Maßnahmen gelistet, die eine Kenntnisnahme entweder erschweren oder verhindern.

2.2.5 Nichtverkettung

Das Gewährleistungsziel der Nichtverkettung spiegelt im Kern den datenschutzrechtlichen Grundsatz der Zweckbindung wieder. Konkret formuliert das Standard-Datenschutzmodell:

> „Das Gewährleistungsziel Nichtverkettung bezeichnet die Anforderung, dass Daten nur für den Zweck verarbeitet und ausgewertet werden können, für den sie erhoben werden.
>
> Datenbestände sind prinzipiell dazu geeignet, für weitere Zwecke eingesetzt zu werden und mit anderen, unter Umständen öffentlich zugänglichen Daten kombiniert zu werden. […] Rechtlich zulässig sind derartige Weiterverarbeitungen jedoch nur unter eng definierten Umständen. Die DS-GVO lässt sie nur zu für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke und fordert für diese Fälle ausdrücklich Garantien für die Rechte und Freiheiten der betroffenen Personen. […]“[71]

Für den Cloud-Bereich geeignete Maßnahmen umfassen z.B. Trennungen mittels Rollenkonzepten und abgestuft regelbaren Zugriffsrechten. [72] Eine starke Isolation zwischen unterschiedlichen Cloud-Mandanten und eine verlässliche Authentifikation ist

[70] https://rwmj.wordpress.com/2011/05/24/what-is-svirt/
[71] DSK, SDM v1.0, S. 14f..
[72] DSK, SDM v1.0, S. 31f..

dafür wichtig. Für die Anwendungen müssen hinreichende Möglichkeiten für qualitätssichernde Test- und Freigabeverfahren und zur Prüfung der Compliance, was im Cloud-Betrieb insoweit unschwer ist, als dass leicht auch temporäre Testsysteme für neue (Anwendungs-)Software aufgesetzt werden können. Ideal wäre dabei, wenn die Sicherungsmaßnahmen der unterliegenden Cloud-Infrastruktur z.B. Wartung und Updates der Anwendungs-Software ermöglichen würde ohne den damit betrauten Administratoren der der Systeme eine Möglichkeit zum Zugriff auf die verarbeiteten Daten zu gewähren.

Die starke Isolation und Vertraulichkeit in SPLITCloud verhindern ungewollte Verkettungen von personenbezogenen Daten. Insbesondere soll dies erreicht werden, indem Systembetreiber keine Kenntnis dieser Daten erlangen können. Ein Zugriff von anderen Cloud-Kunden ist durch Maßnahmen zur Mandantentrennung sicherzustellen

2.2.6 Transparenz

Das Gewährleistungsziel der Transparenz ist nicht auf die Transparenz gegenüber den Betroffenen z.B. durch die Bereitstellung einer Datenschutzerklärung beschränkt sondern adressiert auch die Organisation des Verantwortlichen und von Auftragsverarbeitern selbst. Transparenz stellt sicher, dass die Prozesse und Verarbeitungsvorgänge so dokumentiert sind, dass sie prüffähig sind, dass erforderlich werdende Änderungen tatsächlich vorgenommen werden können und dass die mit den Aufgaben des Datenschutzes und der Systemwartung in der Organisation betroffenen den notwendigen Überblick haben oder zügig verschaffen können. Konkret formuliert das Standarddatenschutzmodell:

> Das Gewährleistungsziel Transparenz bezeichnet die Anforderung, dass in einem unterschiedlichen Maße sowohl Betroffene, als auch die Betreiber von Systemen sowie zuständige Kontrollinstanzen erkennen können, welche Daten für welchen Zweck in einem Verfahren erhoben und verarbeitet werden, welche Systeme und Prozesse dafür genutzt werden, wohin die Daten zu welchem Zweck fließen und wer die rechtliche Verantwortung für die Daten und Systeme in den verschiedenen Phasen einer Datenverarbeitung besitzt. Transparenz ist für die Beobachtung und Steuerung von Daten, Prozessen und Systemen von ihrer Entstehung bis zu ihrer Löschung erforderlich und eine Voraussetzung dafür, dass eine Datenverarbeitung rechtskonform betrieben und in diese, soweit erforderlich, von Betroffenen informiert eingewilligt werden kann. Transparenz der gesamten

> Datenverarbeitung und der beteiligten Instanzen kann dazu beitragen, dass insbesondere Betroffene und Kontrollinstanzen Mängel erkennen und ggf. entsprechende Verfahrensänderungen einfordern können.“ [73]

Cloud-Implementierungen haben im Bereich der Transparenz aus dem Blickwinkel des Datenschutzes daher insbesondere das Folgende sicherzustellen:

- Klare Dokumentation der im Rahmen der Auftragsverarbeitung stattfindenden Vorgänge, einschließlich Informationen zum geografischen Ort der Verarbeitung, der konkreten Bestimmung der verwendeten Hardware, aktueller Softwarestand etc.
- Saubere Dokumentation von Test und Freigabevorgängen für neue oder Überarbeitete Prozesse.
- Neben der Protokollierung von Änderungen und Zugriffen auf Daten auf der Anwendungsebene ist die der Protokollierung der Zugriffe auf die Datenbanken und Systeme selbst, insbesondere Zugriffe durch das Personal des Auftragsverarbeiters, zwecks effektiver Umsetzbarkeit der Kontrollpflichten durch den Verantwortlichen nötig.

In SPLITCloud werden Aspekte der Transparenz dadurch adressiert, dass wesentliche Änderungen der Softwareversion, der Verwendeten Hardware etc. zentral bei der Instanz des TOM-Administrators verwaltet werden. Damit kann die Sammlung, Archivierung und Bereitstellung und der erforderlichen Informationen gegenüber dynamischeren aber dadurch auch unübersichtlicheren Cloud-Modellen erheblich verbessert werden.

2.2.7 Intervenierbarkeit

Das Gewährleistungsziel der Intervenierbarkeit umfasst alle Maßnahmen, die erforderlich sind, um betroffenen Personen die Durchsetzbarkeit und Durchsetzung ihrer Betroffenenrechte nach den Artikeln 12 bis 23 DSGVO sicherzustellen. Adressat dieser Pflichten ist jeweils der Verantwortliche, während der Auftragsverarbeiter sich vertraglich verpflichten muss, mit geeigneten technischen und organisatorischen Maßnahmen, den Verantwortlichen bei der Wahrnehmung dieser Pflichten zu unterstützen, Art. 28 Abs. 3 lit. e) DSGVO.[74] Bei Cloud-Gestaltungen sind also insbesondere sicherzustellen, dass

[73] DSK, SDM v1.0, S. 15.
[74] Gola/Klug, Art. 28 DSGVO Rn. 10.

neben der Auskunft auch die Berichtigung und Löschung durch den Verantwortlichen gewährleistet werden kann. Das Standarddatenschutzmodell definiert Intervenierbarkeit dabei wie folgt:

> „Das Gewährleistungsziel Intervenierbarkeit bezeichnet die Anforderung, dass den Betroffenen die ihnen zustehenden Rechte auf Benachrichtigung, Auskunft, Berichtigung, Sperrung und Löschung jederzeit wirksam gewährt und die verarbeitende Stelle verpflichtet ist, die entsprechenden Maßnahmen umzusetzen. Dazu müssen die für die Verarbeitungsprozesse verantwortlichen Stellen jederzeit in der Lage sein, in die Daten-verarbeitung vom Erheben bis zum Löschen der Daten einzugreifen.“ [75]

Eine Vielzahl der Maßnahmen sind auf der Anwendungsebene zu treffen, so z.B. geeignete Such- und Ausgabefunktionen für die Auskunftserteilung, Lösch- und Berichtigungsfunktionen für gespeicherte Einträge, bzw. die Möglichkeit Sperr- und Löschattribute zu setzten für Daten, die aus anderweitigen Gründen nicht sofort geändert oder gelöscht werden können. Auf der Ebene des Cloud-Systemanbieters ist erforderlich, dass Störungen und Problembeseitigungen in dokumentierter und nachvollziehbarer Weise erfolgen oder dass der Verantwortliche zur Gewährleistung der Betroffenenrechte nachvollziehbar Zugriffe auf der Systemebene erkennen kann.

Die SPLITCloud Architektur unterstützt eine Großzahl von verschiedenen Anwendungen, welche zur Intervenierbarkeit beitragen. Da das vorliegende Dokument seine Analyse nicht auf die Demoapplikation beschränkt, wird für weitere Beurteilungen auf die jeweiligen Anwendungen verwiesen.

2.3 Angreifer, Angriffsmotive, Angriffsziele

Dieses Dokument erörtert das Potential der SPLITCloud-Technologie in einem breiten Anwendungsfeld des Cloud-Computing, ohne sich nur auf die Demoapplikation zu beschränken. Aus diesem Grund ist es unbestimmt, welche Art von personenbezogenen Daten genau verarbeitet werden und somit auch wer genau welche Angriffsmotive und -ziele hat. Daher wird die Analyse in dieser Sektion generell gehalten und konzentriert sich auf die Eigenheiten des Cloud-Computing.

[75] DSK, SDM v1.0, S. 15.

Bei einem Cloud-Deployment ist zu erwarten, dass in der **Anwenderorganisation** vorwiegend Personen, die zum Zugriff auf personenbezogene Daten befugt sind, zur Applikation Zugang haben. Das Outsourcing aller anderen Funktionen vermindert das Angriffspotential innerhalb der Anwenderorganisation drastisch. Sie wird deshalb hier nicht mehr als möglicher Angreifer mit Cloud-spezifischen Risiken betrachtet. Unberührt bleiben die allgemeinen Risiken wie ein unachtsamer Umgang mit Login-Credentials durch Mitarbeiter oder vorsätzlich handelnde (ehemalige) Mitarbeiter.[76]

Üblicherweise sind **unbefugte Dritte** eine sehr wichtige Kategorie von Angreifern. Solche Angriffe und die dazu passenden Schutzmaßnahmen sind auch weithin bekannt und schon in der vorhergehenden Sektion beschrieben. In einem Cloud-Szenario kann man üblicherweise erwarten, dass ein besserer Schutz gegen Angriffe von unbefugten Dritten verfügbar ist. Insbesondere verfügt ein Cloud-Provider gegenüber vor allem kleineren Anwenderorganisationen über besser geschultes und spezialisiertem technischen Personal und ein sehr systematisches und hoch automatisiertes Vorgehen. Dies eliminiert übliche Angriffsflächen wie veraltete Softwareversionen mit bekannten Sicherheitslücken, Fehler in der Konfiguration von Software und Systemen oder mangelnde Ressourcen für systematische Intrusion Detection, Audits von Logs, etc. Unbefugte Dritte verlieren damit Wichtigkeit als Angreifer und die bekannten Schutzmaßnahmen sind meist ausreichend und können in einer Cloud-Umgebung effizienter angewandt werden.

Hersteller von Hard- und Software kommen natürlich auch als Angreifer in Frage indem sie Backdoors einrichten können um unrechtmäßigen auf personenbezogenen Daten zuzugreifen. Das größte Angriffspotential in SPLITCloud liegt sicherlich beim **Hersteller der Sicherheitssoftware** welche den Großteil der Innovation des Projekts ausmacht. Diese Möglichkeit soll in der Bewertung betrachtet werden, auch wenn die **Motivation** für einen derartigen Angriff sicherlich **sehr gering** ist. Insbesondere hängt die Marktposition des Herstellers von seinem Ruf im Gebiet der Sicherheit ab und die Aufdeckung einer Backdoor könnte den wirtschaftlichen Fortbestand des Herstellers in Frage stellen.

Die wohl wichtigsten potentiellen Angreifer, vor allem in einem Cloud-Szenario sind deshalb die **Systembetreiber**. In einem Cloud-Szenario ist relevant, dass typischer-

[76] Zur Einstufung solcher Vorfälle als reales Risiko vergl. die Resultate der gesponserten Studien von Interessenverbänden und Industrie: Bitkom/Holz, Datendiebstahl S. 9; Ponemon Institute, gesponserte Studie Closing Security Gaps, S. 2.

weise alle Funktionen des Systembetreiber vom eigentlichen Anwender an andere Organisationen ausgelagert wird. Da die physische Position der verwendeten Infrastrukturkomponenten oft nicht klar bestimmt werden kann, ist auch das Gesetz welchem die Systembetreiber unterliegen nicht immer klar identifizierbar. Viele Cloud Infrastrukturen enthalten auch Rechenzentren in Ländern, wo die Datenschutzgesetze die Privatsphäre des Einzelnen weniger schützt als es die Gesetzgebung des eigentlichen Anwenders vorsieht, z.B. in Gebieten außerhalb des Geltungsbereichs der DSGVO. Hier ist vor allem erwähnenswert, dass in einigen Ländern Anfragen von Gesetzeshütern (law enforcement agencies) Systembetreiber wirksam verpflichten können, personenbezogene Daten herauszugeben. Eine detaillierte Diskussion dieser Problematiken findet man in der Stellungnahme der Art. 29 Datenschutzgruppe zum Cloud-Computing.[77]

Die Möglichkeit dass Systembetreiber in ihrer Jurisdiktion verpflichtet sein können, personenbezogene Daten preiszugeben, die unter der Gesetzgebung des eigentlichen Anwenders geschützt werden müssen, hat großen Einfluss auf das zu betrachtende Angriffsmodell. Insbesondere ist die rechtliche Verpflichtung zur Übermittlung von Daten ein starkes Motiv für einen „Angriff“, also einen nach der Rechtauffassung der Jurisdiktion des Auftraggebers unzulässigen Zugriffs. Weiterhin bedeutet es, dass in Cloud-Szenarien Gewährleistungsmaßnahmen notwendig sind, die gegenüber Angriffen seitens Systembetreiber einen erhöhten Schutz bieten können. Organisatorische oder rechtliche Maßnahmen greifen in diesen Fällen nicht, so dass nur technische Maßnahmen, insbesondere sichere kryptografische Lösungen, solche Angriffe überhaupt wirksam begegnen können.

2.4 Bestimmung der Eingriffsintensität und des Schutzbedarfs

Um die Risiken für die Rechte der Betroffenen mit den Interessen des Verantwortlichen abwägen zu können ist es zunächst erforderlich die Intensität des Eingriffs in die Rechte der Betroffenen festzustellen. Jede Verarbeitung personenbezogener Daten durch eine Organisation stellt einen Eingriff in das Recht auf Datenschutz der Betroffenen gemäß Art. 8 Abs. 1 GRC[78] dar. Die Anforderung einer wirksamen Rechtsgrundlage für die Datenverarbeitung ist also nur eine erste Grundbedingung, die erfüllt sein muss und wurde für SPLITCloud bereits oben (vgl. 3.1.4) geprüft. Darüber hinaus muss eine

[77] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf

[78] Kingreen, in: Calliess/Ruffert, EUV/AEUV, 5. Aufl. 2016, EU-GRCharta Artikel 8, Rn. 12.

Organisation aber auch nachweisen, dass sie diesen Eingriff in die Rechte der Betroffenen auf das erforderliche Maß beschränkt und dadurch die Intensität des Eingriffs minimiert, so wie es beispielsweise von Art. 5 Abs. 2 und 24 Abs. 1 DSGVO gefordert wird. Eine Rechtfertigung besteht gem. Art. 8 Abs. 2 und Art. 52 Abs. 1 GRC, wenn die Datenverarbeitung auf einer Rechtsgrundlage beruht, die verhältnismäßig ist. Die Anforderungen an die rechtfertigenden Gründe steigen in Abhängigkeit von der Schwere des Eingriffs.[79] Im Rahmen dieser Verhältnismäßigkeitsprüfung lässt sich eine Einteilung nach der von *Alexy* entwickelten triadischen Skalierung vornehmen: dabei werden drei Stufen (leicht, mittel, schwer) unterschieden.[80] Die Intensität des Eingriffs lässt sich nur jeweils für einen konkreten Anwendungsfall ermitteln.[81]

Im diskutierten Use Case Energieabrechnung besteht der Eingriff in der Übermittlung von Daten der Endverbraucher an den Cloud-Betreiber. Dabei wird es sich in der Regel um personenbezogene Daten des Endverbrauchers als Kunden der Stadtwerke handeln, also die Vertragsdaten (Name, Kontaktdaten, ggf. Zahlungsinformationen) sowie die Verbrauchsdaten handeln.

Bezüglich der Eingriffsintensität ist insbesondere zu beachten, dass Smart Meter eine Vielzahl von personenbezogenen Daten erheben. Messwerte aus dem häuslichen Bereich und auch technische Daten wie die Stamm- und Netzzustandsdaten, fallen darunter.[82] Aus diesen Daten lassen sich mitunter detaillierte Rückschlüsse auf das Verhalten der Endverbraucher ziehen, z.B. wann dieser aufsteht und zu Bett geht, wie er Mahlzeiten zubereitet (in der Mikrowelle, im Ofen oder auf dem Herd) und wie häufig Elektrogeräte wie Waschmine, etc. laufen.[83] Nach einer vielzitierten Studie ist es sogar möglich bei sekundengenauen Ablese-Intervallen, das eingeschaltete Fernsehprogramm auch beim gleichzeitigen Laufen weitere Verbraucher noch zu identifizieren.[84] Dies verdeutlicht, dass für die Bewertung eines konkreten Use Cases zur Energieabrechnung nach datenschutzrechtlichen Gesichtspunkten die Ausgestaltung der Übermittlungszeiträume von herausgehobener Bedeutung ist. Die Eingriffsintensität steigt in diesem Zusammenhang mit der Häufigkeit der Übermittlung

[79] Jarass, Charta der Grundrechte der EU, 3. Aufl. 2016, Rn. 34-36.
[80] Alexy, Die Gewichtsformel, S. 777 ff.
[81] Alexy, Die Gewichtsformel, S. 778.
[82] Lüdemann/Ortmann/Pokrant, RDV 2016, 125, 127.
[83] Güneysu/Vetter/Wieser, Intelligenter Rechtsrahmen für intelligente Netze (Smart Grids), DVBl. 2011, 870, 872.
[84] Greveler/Justus/Löhr, Forensic Content Detection through Power Consumption, IEEE International Workshop on Security and Forensics in Communication Systems, Ottawa, Kanada, 2012; abrufbar unter: http://1lab.de/pub/ieee_forensics2012.pdf.

der Verbrauchsdaten. Diese sind in Einklang mit den Prinzipien der Datenvermeidung und Datenminimierung auf das erforderliche Maß zu beschränken. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der Düsseldorfer Kreis schlagen eine jährliche oder monatliche Übermittlung vor.[85] Insoweit die Verbrauchsdaten in einem solchen Intervall aggregiert übermittelt werden, lassen sich kaum nennenswerte Rückschlüsse über das Verhalten des Endverbrauchers ziehen, so dass der Eingriff durch die Übermittlung der Daten nur ein leichtes Gewicht hat. Dieses steigt jedoch, je feingranularer die Intervalle werden. Sobald Rückschlüsse über einzelne Verhaltensweisen des Endverbrauchers möglich sind, steigt die Eingriffsintensität und das Gewicht des Eingriffs wird mittel bis schwer.

Aus der Eingriffsintensität ergibt sich der Schutzbedarf. Nach dem Standard-Datenschutzmodell wird der Schutzbedarf in drei Kategorien unterteilt:

„*Schutzbedarfskategorie „normal“*

Da jede Verarbeitung personenbezogener Daten einen Eingriff in die Grundrechte der betroffenen Person darstellt, kann der Schutzbedarf gemäß SDM niemals niedriger als „normal“ sein. Deshalb ist grundsätzlich davon auszugehen, dass jedes personenbezogene Verfahren mindestens normalen Schutzbedarf aufweist. Weniger schutzbedürftig können folgerichtig nur Verarbeitungen mit nichtpersonenbezogenen Daten sein.

Schutzbedarfskategorie „hoch“

Folgende beispielhaft aufgeführte Verarbeitungsszenarien implizieren eine Eingriffsintensität, welche einen höheren als normalen Schutzbedarf zur Folge haben kann:

- Verarbeitung nicht veränderbarer Personen-Daten, die ein Leben lang als Anker für Profilbildungen dienen können bzw. zuordenbar sind (z. B. biometrische Daten, Genomdaten),
- Verbreitung eindeutig identifizierender, hoch verknüpfbarer Daten (z. B. lebenslang gültige Krankenversichertennummer, Steuer-ID),

[85] DSK, OH Smart Metering S. 12.

- gesetzlich begründete oder anderweitig zu erklärende Intransparenz der Verfahrensweisen für Betroffene (z. B. Verfassungsschutz, Schätzwerte im Scoring),
- Verarbeitung von Daten in einem Verfahren mit möglichen gravierenden, finanziellen Auswirkungen für Betroffene,
- Verarbeitung von Daten in einem Verfahren mit möglichen Auswirkungen auf das Ansehen/die Reputation des Betroffenen,
- Verarbeitung von Daten in einem Verfahren mit möglichen Auswirkungen auf die körperliche Unversehrtheit des Betroffenen,
- Verarbeitung von Daten, die realistischer Weise zu erwartende Auswirkungen auf die Grundrechtsausübung einer Vielzahl Betroffener haben können (z. B. bei zunehmend flächendeckender, öffentlicher Videoüberwachung),
- Gefahr von Diskriminierung, Stigmatisierung (z. B. durch Algorithmen, intransparentes Zustandekommen von Entscheidungen über einen Betroffenen),
- Eingriffe in besonders geschützten inneren Lebensbereich eines Betroffenen.

Hoher Schutzbedarf für ein personenbezogenes Verfahren besteht darüber hinaus dann, wenn Betroffene von den Entscheidungen bzw. Leistungen einer Organisation abhängig sind (etwa in der. Leistungsverwaltung oder im medizinischen Bereich) und wenn eine Organisation

- mit einer weitreichenden Eingriffsintensität Daten verarbeitet, was zu erheblichen Konsequenzen für den Betroffenen führen kann,
- Daten verarbeitet, welche gesetzlich als besonders schutzwürdig ausgewiesen sind,
- keine real nachweislich funktionierenden Möglichkeiten der Intervention und des Selbstschutzes für Betroffene bereitstellt.

Ein hoher Schutzbedarf besteht auch dann, wenn es ist nicht möglich ist, dass Konflikte unter realistisch zu bewältigenden Bedingungen für den Betroffenen vor Gericht geklärt werden können (Bsp. Anbieter von Telekommunikationsdienstleitungen ohne Niederlassung vor Ort). […]

Schutzbedarfskategorie „sehr hoch“

Von sehr hohem Schutzbedarf ist auszugehen, wenn ein Betroffener von den Entscheidungen bzw. Leistungen der Organisation unmittelbar existentiell abhängig ist und zusätzliche Risiken für den Betroffenen nicht bemerkbar sind.“[86]

Soweit die Verbrauchsdaten, etwa zu Abrechnungszwecken, in aggregierter Form jährlich übermittelt werden, gehen die Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der Düsseldorfer Kreis davon aus, dass ein normaler Schutzbedarf besteht. Allerdings steigt der Schutzbedarf bei häufigerer Übermittlung, etwa im Fall täglicher Übermittlungsintervalle nach § 35 Abs. 1 Nr. 2 bei variablen Stromtarifen i.S.v. § 40 Abs. 5 EnWG an Energielieferanten und Netzbetreiber, da diese feingranularen Daten eine Profilbildung erlauben.

Beispielhaft sollen an dieser Stelle zwei Use Cases aus der Orientierungshilfe der Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der Düsseldorfer Kreis aufgegriffen werden: Die Abrechnung der Netzentgelte des Energielieferanten gegenüber dem Letztverbraucher und die Ermittlung des Netzzustands durch den Verteilnetzbetreiber.[87]

- Unterscheidung Zählerdaten: Was ist nötig für Netzmanagement und was für Abrechnung? Für Abrechnung erforderliche Daten können aggregiert in die Cloud übermittelt werden. Wenn Abrechnung Zeitinervallabhängig
- OH ist älter als Messstellengesetz

2.5 Bewertung des Risikos

Während oben eine generische Architektur und Soll-Schutzmaßnahmen für typische Cloud-Gestaltungen diskutiert wurden, wird hier jetzt konkret auf den Ist-Zustand von SPLITClound eingegangen. Insbesondere werden im Folgenden die spezifische Architektur, Schutzmaßnahmen und eine von der SPLITCloud-Architektur ermöglichte Rollenverteilung beschrieben. Es wird weiter erörtert wie verschiedene Akteure andere Akteure beschränken und kontrollieren können. Auf dieser Basis wird ein Soll-Ist Vergleich der Schutzmaßnahmen vorgenommen.

[86] DSK, SDM v1.0 S. 37 f.
[87] DSK, OH Smart Metering S. 26 f und S. 37 f.

2.5.1 Beschreibung der SPLITCloud-Architektur und der Schutzmaßnahmen (Ist Zustand)

Abbildung 5 zeigt schematisch die SPLITCloud-Architektur anhand welcher nachstehend die Schutzmaßnahmen aufgezeigt werden.

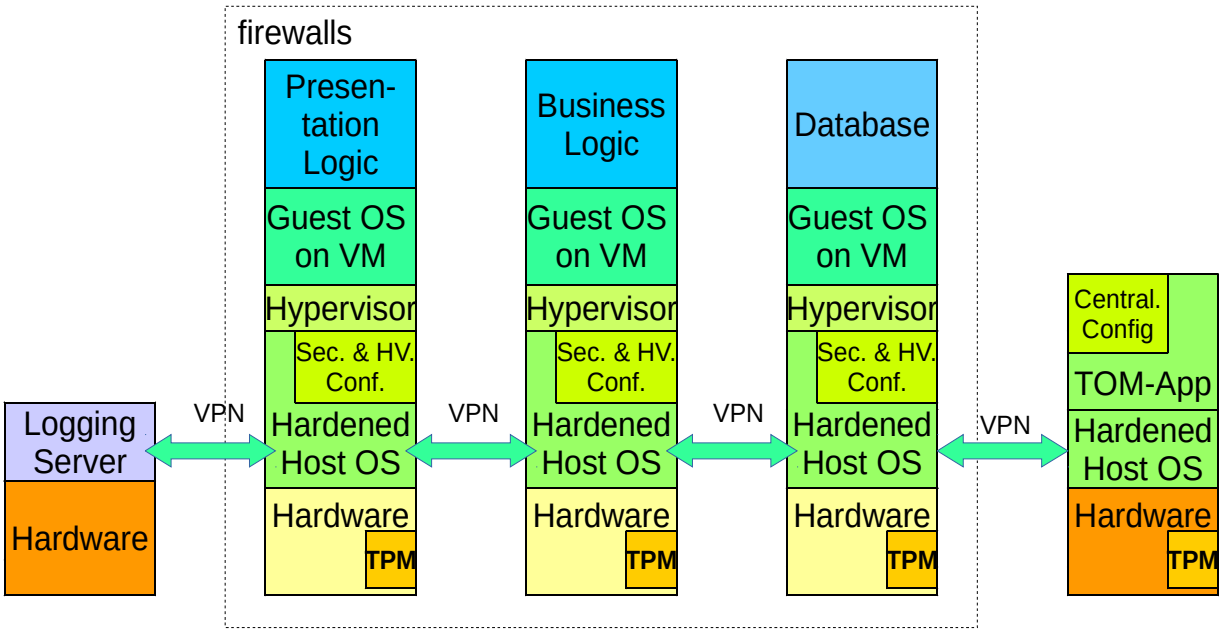

Abbildung 5 SPLITCloud-Architektur

Die drei Tiers der Demoapplikation laufen auf **Trusted Servern** (Blades) in einem Cloud-Datenzentrum (blasses Gelb). Diese Server verfügen alle über ein **Trusted Platform Module** (TPM, dunkles Gelb). Andere Server, möglicherweise außerhalb des Cloud-Datenzentrums, werden für den Betrieb des Trusted Object Managers (TOM) beziehungsweise eines zentralisierten Logging Servers verwendet. Der TOM-Server ist gleichsam mit einem TPM ausgerüstet und den Trusted Servern sehr ähnlich.

Die Trusted Server und der TOM-Server werden durch ein **gehärtetes Host Betriebssystem** verwaltet. Die Härtung (hardening) wird durch einen Linux Kernel Patch „**grsecurity**“[88] realisiert.

Das gehärtete Host Betriebssystem realisiert einige für die Sicherheit wichtige Schutzmechanismen, die in Abbildung 6 illustriert sind.

[88] https://grsecurity.net/

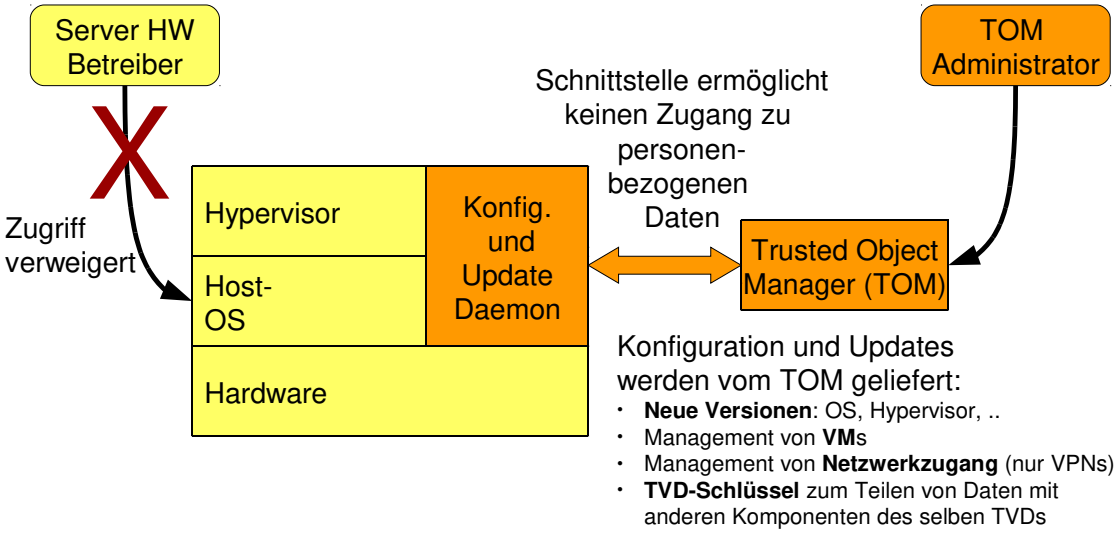

Abbildung 6 Schutzmaßnahmen auf den Trusted Servern

- Dem ***root* user** des gehärteten Host-Betriebssystem wird das Login durch die folgenden Maßnahmen verweigert:
  - Die Systemanmeldung von *root* und allen anderen Benutzern ist deaktiviert. Insbesondere hat kein Benutzer eine Login Shell in /etc/passwd und alle Daemons zur Systemanmeldung (ssh, telnet, etc.) sind ebenfalls deaktiviert.
  - Netzwerkzugriffe auf den Server sind nur durch VPNs möglich, die sich mit einem kryptografischen Schlüssel autorisieren können, die vom TOM autorisiert sind. Diese Kontrolle des Netzwerkzugriffs wird verwendet, um für alle Benutzer, einschließlich *root*, den Zugang zum Server zu steuern.
  - Sollte gegen alle Erwartungen trotzdem ein Angreifer Zugriff zum Server gewinnen, dann verunmöglicht oder erschwert die *Address Space Layout Randomisation* von *grsecurity* eine Rechteausweitung (root escalation) die notwendig wäre, um Kenntnisnahme von geschützten Daten zu erlangen.
  - Die normalerweise von *root* übernommene **Konfigurationsarbeit** wird durch einen „Konfigurations- und Update Daemon“ des gehärteten Betriebssystems übernommen und vom TOM ferngesteuert. Die Schnittstelle dieses Daemons limitiert die Funktionalität, die auf dem Server ausgeführt werden kann. Insbesondere vermeidet die angebotene Funktionalität jegliche Kenntnisnahme von geschützten Daten. Die vom TOM ferngesteuerte Konfiguration steuert die folgenden Aspekte: Virtuelle Maschinen (in SPLITCloud auch „Compartments“ genannt), die auf dem Hypervisor laufen.

- Autorisierte Virtual Private Networks, die auf ein Compartment zugreifen können.
- TVD-Schlüssel, Schlüssel die von mehreren Compartments (typisch auf verschiedenen Servern) einer sogenannten Trusted Virtual Domain (TVD) geteilt werden und eine auf Verschlüsselung basierte vertrauliche Kommunikation-Tiers.

Die Fernsteuerung ermöglicht im Weitern sichere Updates des gehärteten Betriebssystem selbst sowie des Hypervisors.

- Das gehärtete Betriebssystem und seine Services garantieren, dass Daten, die ein Compartment verlassen, wenn nötig automatisch **verschlüsselt** werden. Insbesondere ist dies der Fall wenn das empfangende Compartment nicht zur selben TVD gehörenden. Die Schlüssel (der TVDs) werden vom TOM verwaltet und nur innerhalb derselben TVD verfügbar gemacht. Außerhalb einer TVD sind Daten damit wegen Verschlüsselung nie zugreifbar. Dies stellt einen wichtigen Schutz dar, der verunmöglicht, dass geschützte Daten eine TVD-Umgegung verlassen können. Tiers
- Das gehärtete Betriebssystem garantiert auch, dass **Daten**, die auf die **Festplatte** geschrieben werden, mit einem an den TPM gebundenen Schlüssel **verschlüsselt** werden. Kopierte Daten sind damit außerhalb der sicheren Umgebung des gehärteten Betriebssystems unbrauchbar.
- Für die Zukunft ist denkbar, dass das gehärtete Betriebssystem mit Mechanismen des Mandatory Access Controls die Isolation zwischen virtuellen Maschinen auf demselben Hypervisor garantiert. (Vergleiche dazu sVirt.[89])

Die **TPMs** auf den Trusted Servern und dem TOM unterstützen einen **Trusted Boot,** der es bezweckt zu verunmöglichen, einen andern als den vorgesehenen gehärteten Kernel zu laden. Der **TPM** ist weiterhin die Basis für eine **Remote Attestation**[90] durch den TOM, der die Präsenz und Konsistenz aller vorgesehenen Schutzmechanismen im gehärteten Host Betriebssystem überprüft bevor er die zum Datenzugriff notwendigen Schlüssel freigibt.

---

https://rwmj.wordpress.com/2011/05/24/what-is-svirt/, http://danwalsh.livejournal.com/30565.html

90 https://en.wikipedia.org/wiki/Trusted_Computing#Remote_attestation.

Gebündelt mit dem gehärteten Host Betriebssystem kommt ein handelsüblicher und nur leicht modifizierter[91] **Hypervisor** (VirtualBox)[92]. Dieser kann mehrere virtuelle Maschinen betreiben und wird, wie oben beschrieben, aufgrund der zentralisierten Konfiguration des TOMs konfiguriert.

Auf den VMs läuft ein beliebiges **Guest Betriebssystem** (für die Demoanwendung wird Windows verwendet). Verschiedene Guest Betriebssysteme werden vom Hersteller der Security Software zur Verfügung gestellt. Sie werden vom TOM über sichere Kanäle heruntergeladen und den Konfigurations- und Update Daemon des gehärteten Host Betriebssystems auf den VMs installiert.

Auf drei dieser Guest Betriebssystemen, möglicherweise auf verschiedenen Trusted Servern, laufen drei Tiers der eigentlichen Anwendung.

Abbildung 7 Beschränkung des Zugriffs auf virtuelle Maschinen (Compartments) zeigt die Schutzmaßnahmen zur Regelung des Zugriffs auf virtuelle Maschinen, die SPLITCloud-Compartments repräsentieren.

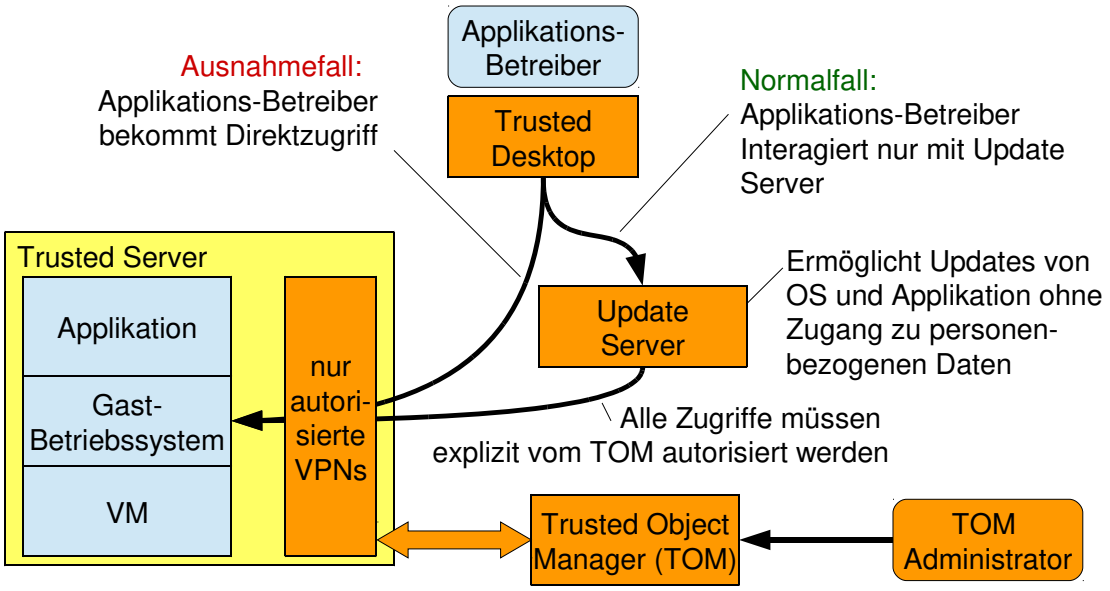

Abbildung 7 Beschränkung des Zugriffs auf virtuelle Maschinen (Compartments)

91 Insbesondere ist das Clipboard modifiziert, so dass auch hier keine Daten das TVD ohne Verschlüsselung verlassen können.
92 https://www.virtualbox.org/

Der Applikationsbetreiber, also der *root* Benutzer des Gastbetriebssystems auf der VM, hat in der SPLITCloud-Architektur zwei verschiedene Zugriffsmöglichkeiten:

Im **Normalfall** greift er nur indirekt durch einen Update Server auf den Trusted Server zu. Der Update Server bietet eine Systemumgebung, die dem Trusted Server entspricht. Sie unterstützt damit das ausführliche Testen von neuen Versionen von Software (sowohl Betriebssystem wie Applikation) bevor sie auf dem Trusted Server in Produktion gehen. Der einzige Unterschied der Umgebung sind die Daten der Applikation. Während auf dem Trusted Server reale, personenbezogenen Daten verwendet werden, verfügt der Update Server lediglich über Testdaten. Der Update Server gehört auch zu einer andern TVD als die eigentliche Applikation um einen möglichen Datenaustauch zu unterbinden. Wenn eine neue Version der Software erfolgreich getestet worden ist, veranlasst der TOM-Administrator, dass die Software vom Update zum Trusted Server übertragen wird.

Obwohl der Update Server die erwartete Konfigurations- und Instandhaltungsarbeiten des Applikationsbetreibers abdecken, kann vom TOM-Administrator im **Ausnahmefall** ein direkter Zugriff auf das Gastbetriebssystem gewährt werden.

Dies ist relativ unkritisch für den Presentation- und Business-Tier, da hier während Wartungsunterbrüchen keine personenbezogenen Daten vorliegen. Der Zugriff zu dem Compartment (VM) des Datenbank-Tiers ist kritischer und erfordert entsprechende Schutzmaßnahmen.

Die obige Abbildung 7 Beschränkung des Zugriffs auf virtuelle Maschinen (Compartments) illustriert dass Applikationsbetreiber im Ausnahmefall über einen Trusted Desktop zugreifen können. Dies ermöglicht es, vom TOM gesteuerte Schutzmaßnahmen zu realisieren.

Um einen Zugriff zu ermöglichen, muss der TOM-Administrator für die Dauer der Intervention eine VPN zwischen dem Trusted Desktop und dem Trusted Server autorisieren. Diese Autorisation kann von einer organisatorischen Realisierung des Vier-Augen-Prinzips abhängig gemacht werden, so dass vorgenommene Handlungen des Applikationsbetreibers dem TOM-Administrator zur Kenntnis gelangen. Der Trusted Desktop beim Applikationsbetreiber muss für diesen Vorgang kurzzeitig auch derselben TVD zugeordnet werden.

Das TVD Konzept mit seiner automatischen Verschlüsselung aller Daten, die die TVD verlassen, schützt vor unerwünschtem Kopieren von Daten. Insbesondere werden Daten die auf Speichermedien oder übers Netzwerk kopiert werden, und damit die TVD

verlassen, durch Verschlüsselung mit dem TVD-Schlüssel für andere Zwecke unbrauchbar gemacht. Kenntnisnahme von personenbezogenen Daten ist somit allenfalls über den Bildschirm möglich. Solche Kenntnisnahme kann aber durch ein organisatorisches Vier-Augen-Prinzip verhindert werden (siehe oben).

Abbildung 5 zeigt weiter, wie auf einem separaten Server zentralisiert alle wichtigen **Logs** (Protokolle) gesammelt werden. Diese müssen periodisch auf Unregelmäßigkeiten untersucht werden. Teile solcher Untersuchungen können dabei automatisch erfolgen. Ein manuelles Audit ist aber meist trotzdem noch notwendig.

2.5.2 Akteure in SPLITCloud

Die Diskussion des Soll-Zustands am Anfang dieses Dokuments basierte auf der generischen Architektur einer Applikation mit drei Tiers. Bei den Akteuren wurde deshalb ein generischer *Systembetreiber* verwendet. Im Ist-Zustand der hier diskutiert wird gibt es nun verschiedene konkrete Systemkomponenten und Funktionen. SPLITCloud macht es möglich, dass die Kontrolle von Komponenten und Funktionen in den Händen von verschiedenen Organisationen liegt. Deshalb muss man das Konzept von Systembetreiber in eine Mehrzahl von Akteuren diversifizieren.

Insbesondere unterscheiden sich die folgenden Hauptakteure:

- Der **Server Hardware Provider** (Infrastructure Provider) stellt die für die drei Tiers der Applikation verwendete Hardware zur Verfügung. Dies ist typisch ein Cloud-Provider mit der entsprechenden Economy of Scale.
- Der **Sicherheitssoftware Hersteller**, der die gehärteten Host Betriebssysteme des Trusted Servers und Desktops, als auch die Trusted Object Manager (TOM) Software zur Verfügung stellt.
- Der **TOM-Administrator,** der die Sicherheitskomponenten des Gesamtsystems über den TOM konfiguriert.
- Der **TOM-Hardware-Provider**, der den physischen TOM-Server zur Verfügung stellt.
- Der **Applikationsbetreiber**, der die Applikation, inklusive der Datenbank, betreibt.
- Der **Logging Betreiber**, der die Logging Software betreibt, Protokolle sicher sammelt und deren Inhalt automatisch und manuell in Audits auf Unregelmäßigkeiten untersucht.

Darüber hinaus gibt es auch die folgenden Nebenakteure:

- Der **Logging Hardware Provider**, der den physischen Logging Server zur Verfügung stellt.
- Der **Hypervisor Hersteller**.
- Der **Applikationshersteller**, der die Presentation- und Business Logic Software herstellt.
- Der **Datenbank Management System** (DBMS) **Hersteller**.
- Der **Logging Software Hersteller**.

2.5.3 Notwendigkeit einer Gegenseitige Beschränkung oder Kontrolle zwischen Systembetreibern

Wie aus der Erörterung in 2.2 „Schutzbedarfsbestimmung für die Gewährleistungsziele“ hervorgeht, ist in einem Cloud-Setting vor allem die Gewährleistung der Vertraulichkeit schwierig. Die Diskussion von Angreifern und Angriffsmotiven zeigt weiterhin, dass das Bedrohungsmodell klar Angriffe von Insidern, also Systembetreibern, umfassen muss. Insiderangriffe sind wesentlich schwieriger abzuwehren als die von andern Akteuren. Zudem stellt der Schutz von Insidern neue Herausforderungen, die noch nicht so gut verstanden werden, wie Schutzmaßnahmen von den „guten“ Insidern gegen „böse“ Outsidern. Während dieses Paradigma in einer „klassischen“ Systemumgebung einer Organisation vielleicht aufrechterhalten werden kann, ist es unverändert nicht auf eine Cloud-Umgebung übertragbar.

Ob und wie ein Insider-Akteur andere Akteure überwachen kann ist deshalb äußerst relevant für die Diskussion von Schutzmaßnahmen. Dies ist ersichtlich in der Tatsache, dass typischerweise Systembetreiber selbst Schutzmaßnahmen realisieren. In vielen Szenarien werden dann Schutzmaßnahmen lediglich zu einer Selbstbeschränkung oder Selbstkontrolle, die dann natürlich auch (temporär) wieder aufgehoben werden können. Mit andern Worten kann eine Selbstbeschränkung oder -Kontrolle für rein interne Zwecke hinreichend sein, sie ist indes kein effektiver Schutz zur Wahrung von Rechten Drittbetroffener – seien dies Cloud-Kunden oder betroffene Personen.

Beispiele für Selbstbeschränkungen sind Unix Zugriffsrechte auf Dateien, die zwar auch für den *root* User gelten, von ihm aber jederzeit abgeändert werden können. Ähnlich kann ein Protokollieren (logging) von kritischen Aktivitäten des *root* Users nicht zur

Aufdeckung von Missbrauch nutzen, wenn *root* selbst den Logging Daemon betreibt oder die Logs selbst editieren kann.

In SPLITCloud gibt es nun Schutzmaßnahmen, die von einem Akteur (d.h. Systembetreiber einer Organisation) realisiert werden und einen andern Akteur (d.h. Systembetreiber einer andern Organisation) beschränken oder kontrollieren können. Eine Beschränkung verunmöglicht ungewollte Eingriffe mit technischen Mitteln; eine Kontrolle macht es möglich, ungewollte Eingriffe aufzudecken und die Verantwortlichen zur Rechenschaft zu ziehen.

Um eine derartige Beschränkung oder Kontrolle von einem Akteur zu einem Andern umgehen zu können, müssten jeweils beide Akteure zusammenwirken. Damit bleibt eine Schutzmaßnahme effektiv, solange sich mindestens einer der betroffenen Akteure regelgerecht verhält.

2.5.4 Gegenseitige Kontrolle zwischen Hauptakteuren in SPLITCloud

Im Folgenden wird nun konkret die Möglichkeit der gegenseitigen Beschränkung oder Kontrolle in SPLITCloud analysiert. Das Ziel der Diskussion ist zu erkennen, welche Akteure genügend technisch beschränkt und von andern Akteuren kontrolliert werden können, und welche noch unaufdeckbare Rest-Angriffsmöglichkeiten haben und deshalb sehr vertrauenswürdig sein müssen.

Wie in „4 Bewertungsmaßstäbe anhand von Schutzzielen“ ersichtlich ist, sind die schwierig abwehrbaren Angriffe diejenigen, wo ein Systembetreiber als *root* User auf einen Server zugreift. Die folgende Diskussion betrachtet deshalb diese Art von Angriffen der Hauptakteure und wie die von andern Akteuren durch Beschränkung technisch verhindert oder durch Kontrolle aufgedeckt werden können.

2.5.4.1 Angriffe durch den Server Hardware Provider

Die in Abschnitt 2.2 durchdeklinierten datenschutzrechtlichen Gewährleistungsziele verlangen, dass der Server Hardware Provider, der in traditionellen Cloud-Umgebungen *root* Zugang zu den Servern hat, keine Kenntnis von personenbezogenen Daten erhalten kann. Dies kann durch die in Abbildung 6 visualisierten Beschränkungen und Kontrollen voll erreicht werden.

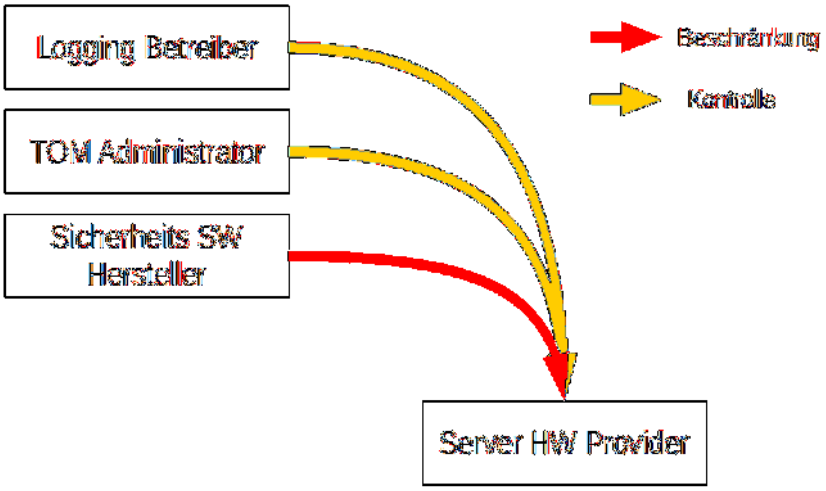

Abbildung 8 Beschränkungen und Kontrollen, die andere Akteure dem Server Hardware Betreiber auferlegen

Insbesondere werden **vom Hersteller der Sicherheitssoftware** dem Server Hardware Provider starke **Beschränkungen** auferlegt:

- Systemanmeldung als *ro*ot auf den Servern ist verunmöglicht.
- Alle normalerweise von *root* getätigte Konfiguration auf dem Server ist automatisiert und wird vom TOM gesteuert.
- Da die Sicherheitssoftware TPM-basierten Trusted Boot und Remote Attestation unterstützt, ermöglicht sie die Kontrolle durch andere Akteure, dass die Beschränkungen intakt und aktiviert sind. Eine genaue Protokollierung von Aktivitäten hat einen ähnlichen Effekt.

Der **TOM-Administrator** und der **Logging Betreiber** können somit die Präsenz und Integrität der Beschränkungsmechanismen gegenüber dem Server Hardware Providers verifizieren.

2.5.4.2 Angriffe durch den TOM-Hardware-Provider

Eine sehr ähnliche Situation ergibt sich für den TOM-Hardware-Provider. Wieder sind die Beschränkungen vom Sicherheitssoftware Hersteller realisiert und werden durch den TOM-Administrator und den Logging Betreiber überwacht.

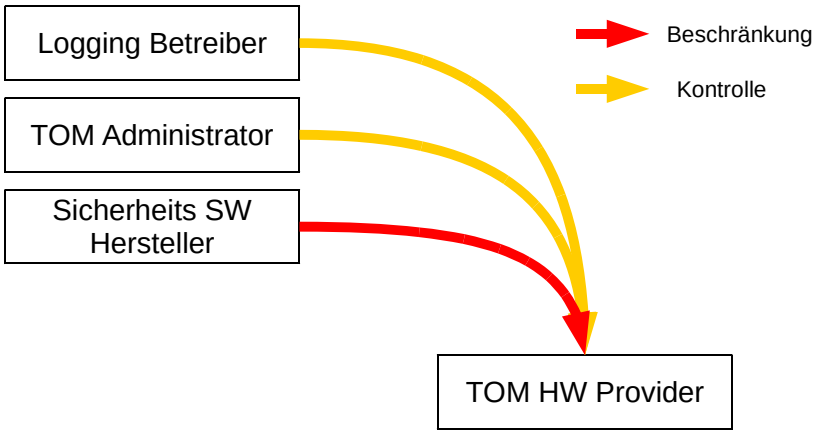

Abbildung 9 Beschränkungen und Kontrollen, die andern Akteuren dem TOM-Hardware-Betreiber auferlegen

2.5.4.3 Angriffe durch den Applikationsbetreiber

Um den *root* Zugang zu den Servern von Seiten des Applikations-Betreibers zu verhindern, werden die **vom Sicherheitssoftware Hersteller realisierten Beschränkungsmöglichkeiten** genutzt. Diese müssen aber **vom TOM-Administrator explizit konfiguriert** werden. Damit ergibt sich die folgende Situation:

- Der Applikationsbetreiber hat im Normalfall keinen *root* Zugang auf die Gastbetriebssysteme da der TOM-Administrator keine Netzwerkzugänge für den Applikationsbetreiber öffnet.
- Applikationssoftware wird durch den Update Server installiert und aktualisiert. Dieser automatisierte Prozess bietet dem Applikationsbetreiber keinerlei Zugang auf Daten. Jeder Update muss explizit vom TOM-Administrator während eines Unterbruchs des normalen Betriebs autorisiert werden.
- Sollten die vorgesehenen automatisierten Administrationstätigkeiten unerwarteter Weise nicht genügen, kann der TOM Administrator temporär ein VPN konfigurieren, über das der Applikationsbetreiber einen sicheren *root* Zugang zum Guest Betriebssystem erhalten. Um die Kenntnisnahme von Daten dabei zu vermeiden, wird wie folgt vorgegangen:
  - Bei Arbeiten am Präsentation- oder Business-Tier wird der normale Betrieb der Applikation unterbrochen, so dass keine personenbezogenen Daten auf den entsprechenden Servern präsent sind. Damit ist eine unerwünschte Kenntnisnahme ausgeschlossen.

- Beim **Datenbank-Tier** ist dies nicht möglich. In solchen Fällen soll mit **organisatorischen Maßnahmen** ein **Vier-Augen-Prinzip** implementiert werden. Der Zugang zu personenbezogenen Daten ist durch die SPLITCloud TVD Technologie auf visuelle Kenntnisnahme auf dem Bildschirm beschränkt.

Alle Routine- und Ausnahmezugriffe auf das Guest Betriebssystem müssen gelogged werden, so dass der Logging Betreiber Unregelmäßigkeiten im Betrieb erkennen kann und die erforderlichen Maßnahmen zur Evaluation, Folgenbeseitigung und Verhinderung künftiger Ereignisse ergreifen kann.

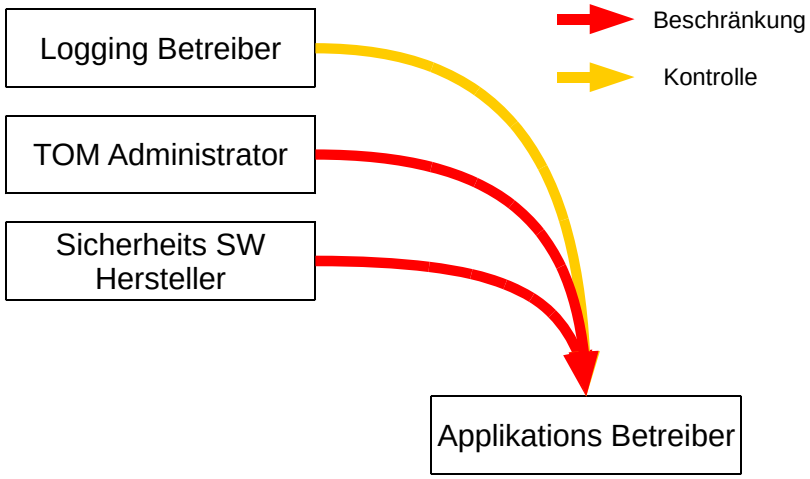

Abbildung 10 Beschränkungen und Kontrollen, die andern Akteuren dem Applikationsbetreiber auferlegen

2.5.4.4 Angriffe durch den TOM-Administrator

Wie oben beschrieben hat der TOM-Administrator eine zentrale Rolle in der Kontrolle des Zugangs zu (personenbezogenen) Daten der Applikation. Insbesondere könnte er eine VPN und TVD konfigurieren, die seinen eigenen Secure Desktop Zugriff zu den Servern und Daten gewähren. Es gibt keine Möglichkeiten in den Händen anderer Akteure, dies zu durch eine Beschränkung technisch zu verhindern.

Der Sicherheitssoftware Hersteller kann hingegen die sichere Protokollierung aller relevanten Aktionen des TOM-Administrators gewährleisten. Der TOM-Administrator ist damit **schwach durch den Logging Betreiber kontrolliert**. Da nur eine schwache Kontrolle möglich ist, muss der TOM-Administrator von einer **vertrauenswürdigen Organisation** zur Verfügung gestellt werden.

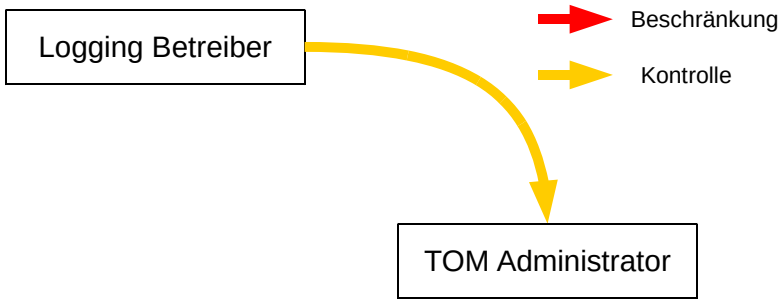

Abbildung 11 Beschränkungen und Kontrollen, die andern Akteuren dem TOM-Administrator auferlegen

2.5.4.5 Angriffe durch den Sicherheitssoftware Hersteller

Die wichtigsten Schutzmaßnahmen zur Beschränkung und z.T. auch Kontrolle des *root* Zugriffs anderer Akteure stützt sich auf der Sicherheitssoftware von SPLITCloud, also den Trusted Server, Desktop, und Object Manager. Diese Software hat durchaus Zugriff zu allen Daten. Es wäre deshalb theoretisch möglich, dass der Hersteller eine Backdoor einbauen könnte, die sehr schwierig zu entdecken wäre. Da auch die Protokollierung von kritischen Aktionen von der Sicherheitssoftware gewährleistet wird, ist eine Kontrolle weitgehend unmöglich.

Das Gesamtsystem legt daher viel Vertrauen in den Hersteller der Sicherheitssoftware.

Faktoren, die das Vertrauen in den Sicherheitssoftware Hersteller erhöhen können, umfassen die folgenden:

- Der Hersteller soll in einem Gesetzesraum mit strengen Datenschutzgesetzen operieren, und vorzugsweise denselben Gesetzen wie der verantwortliche Anwender unterliegen.
- Es soll verifiziert werden, dass der Hersteller keine Motivation zum Kompromittieren personenbezogener Daten hat.
- Es wäre denkbar, den Source Code der Software bei einem Dritten, wie einem Notar, zu hinterlegen um bei dringendem Verdacht der Existenz einer Backdoor die Frage abklären zu können.
- Es wäre denkbar, dass der Hersteller von einer vertrauenswürdigen Drittpartei die Software auditieren und zertifizieren lassen könnte.

2.5.4.6 Wie kann SPLITCloud auf Organisationen verteilt werden?

Um besser zu verstehen, wie SPLITClound Komponenten und Funktionen auf Organisationen abgebildet werden können, ist es wichtig zu verstehen, welche

Begrenzungs- und Kontroll-Abhängigkeiten existieren. Dies ist in Abbildung 12 dargestellt.

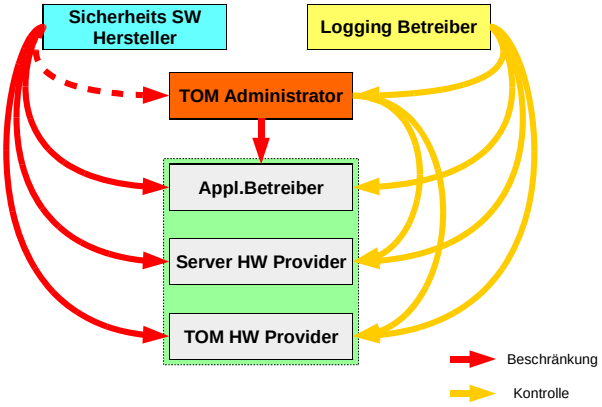

Abbildung 12 Begrenzungs- und Kontroll-Beziehungen zwischen Akteuren

Funktionen in SPLITCloud können dann kombiniert, d.h. von derselben Organisation ausgeführt werden, wenn keine gegenseitige Beschränkungs- oder Kontrollfunktion existiert. Bei der Kombination von andern Funktionen würde man wieder Selbstbeschränkung oder -Kontrolle einführen, die die SPLITCloud Architektur versucht zu vermeiden.

Von der Abbildung ist es ersichtlich, dass zwischen den Funktionen des Server Hardware Providers, TOM-Hardware-Providers und Applikationsbetreibers keine gegenseitigen Abhängigkeiten existieren. Eine Trennung dieser Funktionen bringt deshalb keinen Mehrwert unter dem Gesichtspunkt des Datenschutzes und könnte auch jetzt schon von einer einzelnen Organisation übernommen werden.

Aus der Abbildung sind gleichsam die Akteure ersichtlich, die nach obigen Ausführungen nicht genügend von andern beschränkt oder kontrolliert werden können. Dies sind vor allem der Sicherheitssoftware Hersteller, in den das System bzw. alle Beteiligten volles Vertrauen legen müssen. Weitere zentrale Stelle ist der TOM-Administrator, gegenüber dem der Sicherheitssoftware Hersteller lediglich die Protokollierung gewährleisten kann und der Logging Betreiber nur eine schwache Kontrolle ausüben kann. Dass der Logging Betreiber nicht von andern Akteuren überwacht werden kann ist demgegenüber nicht relevant, da er nach dem Konzept keinen Zugriff auf personenbezogenen Daten haben soll.

Abbildung 12 Begrenzungs- und Kontroll-Beziehungen zwischen Akteuren deutet farblich an, welche Funktionen getrennt ausgeführt werden sollen. Dies bedeutet aber nicht, dass ein absolut vertrauenswürdiger Akteur nicht verschieden eingefärbte

Funktionen trotzdem kombinieren könnte. Z.B. der eigentliche Anwender der Applikation, der auch rechtmäßigen Zugriff auf die personenbezogenen Daten hat, könnte natürlich alle Funktionen übernehmen.

2.5.5 Soll-Ist Vergleich

Im Folgenden werden die Schutzmaßnahmen von SPLITCloud mit den Soll-Maßnahmen von Sektion 2.2 verglichen. Die Diskussion konzentriert sich vor allem auf Vertraulichkeit 2.2.4 und folgt derselben Struktur.

2.5.5.1 Schutz während der Datenübertragung

Im Folgenden werden kurz die Maßnahmen von SPLITCloud zum Schutz der Datenübertragung beschrieben und dann mit den Anforderungen von Sektion 2.2.4.1 verglichen.

Alle Kommunikationskanäle in SPLITCloud sind mit Virtual Private Networks (VPNs) geschützt. Die Konfiguration dieser VPNs und wer wo Zugang hat wird zentral vom TOM-Administrator verwaltet. Die VPN Software ist ein integraler Bestandteil der gehärteten Host Betriebssystemen aller Server, inklusive der Trusted Servern, des TOM-Servers und des Trusted Desktop welcher von Administratoren benutzt werden kann. Zusätzlich sind VPN Devices verfügbar, die dasselbe gehärtete Betriebssystem beinhalten. Endkunden der Applikation benutzen diese oder Trusted Desktops um sich mit dem Web Server des Presentation Tiers zu verbinden.

Die Authentisierungsschlüssel dieser VPN Komponenten sind jeweils durch das Trusted Platform Module geschützt. Weiterhin kann durch Trusted Boot und Remote Attestation die Konsistent der VPN Software verifiziert werden.

Im Verglich zu den Anforderungen von Sektion 2.2.4.1 ist die Verschlüsselung in mehrere Teilkanäle unterbrochen. Jeder Teilkanal ist ein verschlüsseltes VPN. Zwischen diesen VPNs werden Daten im Klartext auf Rechnern verwaltet, die durch ein gehärtetes Betriebssystem besonders gegen Angriffe geschützt sind.

Eine Schicht der Authentisierung ist basiert auf den VPNs und identifiziert entweder Server, Desktops, oder VPN Endgeräte. Im letzteren Fall ist typischerweise ein Desktop PC direkt und ohne alternative Netzwerkverbindungen in das Endgerät gesteckt. Dies vermeidet eine unnötige Angriffsoberfläche bevor der Schutz durch das VPN beginnt.

Zusätzlich zu der Authentisierung von Rechnern (durch die VPN) ist auf Trusted Desktops auch eine Smartcard-basierte Authentisierung von Benutzern möglich. Dies ist vor allem wichtig für die verschiedenen Systemadministratoren.

Die eigentlichen Anwender der durch SPLITCloud geschützten Applikationen, melden sich zusätzlich mit der von der Applikation vorgesehenen Methode an. Auch wenn dies auf der Anwendungsebene mit einem Benutzername und Passwort geschieht, ist es immer noch sicher, weil das VPN schon alle Benutzer außerhalb der Anwenderorganisation effektiv ausschließt und damit ein vergleichbarer Schutzumfang besteht wie im internen Netz der Organisation. Ob dieses dem Schutz genügt, ist im Einzelfall zu prüfen. Sollte dies bei höherem Schutzbedarf nicht genügen, ist es immer möglich, jeden Anwender mit einem Trusted Desktop mit Smartcard Login auszustatten.

Da alle wichtigen Systemkomponenten mit Trusted Platform Modules mit Zufallszahl-Generatoren ausgestattet sind, sind überall dedizierte Hardware Entropiequellen verfügbar.

Damit bietet SPLITCloud eine lückenlose, starke Verschlüsselung und Authentisierung bei allen Datenübertragungen. Eine allenfalls ungenügende Sicherheitsstufe in der Authentisierung der Applikation kann mit SPLITCloud Maßnahmen auf den höchsten Stand gebracht werden.

2.5.5.2 Schutz während der Speicherung von Daten

Im Folgenden werden die Schutzmaßnahmen von SPLITCloud für Daten während der Speicherung beschrieben und mit den Anforderungen von Sektion 2.2.4.2 verglichen.

Die Anforderungen betrachten vorerst eine Verschlüsselung der Festplatten, die gehen die meisten Akteure effektiv ist und dann den Schutz vor Systembetreibern, die üblicherweise über die Schlüssel verfügen können.

Während Applikationen auf SPLITCloud eine Verschlüsselung (wie z.B. die Transparent Data Encryption eines DBMS) durchführen können, bietet SPLITCloud einen alternativen oder zusätzlichen Schutz für jede Art von Applikation an. Dies geschieht notwendigerweise auf der Ebene des Host Betriebssystems und verwendet somit denselben Schlüssel für mehrere virtuellen Maschinen und damit Verarbeitungszwecke. Aus diesem Grund verwendet SPLITCloud Methoden[93] um die zusätzlich notwendige starke Isolation von virtuellen Maschinen zu garantieren. Zusätzlich wird der Schlüssel sicher im TPM gespeichert. Mit diesem Ansatz kann selbst auf dieser tiefen Ebene der Verschlüsselung ein effektiver Schutz der gespeicherten Daten gegenüber Angriffe der meisten Akteure geboten werden.

[93] Derzeit ist eine Weiterentwicklung von SPLITCloud in Arbeit, die Mandatory Access Control für eine Verstärkung der Isolation verwendet.

Die obige Maßnahme ist ein effektiver Schutz gegen alle Akteure außer der Systemadministratoren des Host Betriebssystems und dem Datenbank- und Systemadministratoren der Guest Betriebssysteme, da diese Zugang zum Schlüssel haben, beziehungsweise Zugang zu den unverschlüsselten Daten auf einer Ebene über der Verschlüsselung haben. SPLITCloud bietet gegen unerwünschte Zugriffe dieser Administratoren den folgenden Schutz:

- Durch oben beschriebenen Maßnahmen, immer aktiv und überprüfbar durch Trusted Boot und Remote Attestation, wird die Rolle des Systemadministrators auf dem Host Betriebssystem eliminiert.
- Normalerweise durch den Systemadministrator ausgeführte Eingriffe werden von einem Daemon übernommen, der seine Konfiguration durch sichere Kanäle vom TOM-Server erhält.
- Updates des gehärteten Host Betriebssystem werden vom Sicherheitssoftwarehersteller zur Verfügung gestellt und durch den TOM-Server geladen.
- Administratoren des Guest Betriebssystems sind normalerweise in der TOM-basierten Konfiguration der VPNs vom Zugriff auf die Server ausgeschlossen.
- Routinewartung wird durch den Update Server von SPLITCloud automatisiert. Dabei haben die Administratoren keinen Zugriff auf die Server.
- Falls unerwarteter Weise die vorgesehene Routinewartung nicht ausreichen sollte, kann der TOM-Administrator vorzugsweise eine bereitgestellte Prozedur (script) ausführen oder ansonsten kurzfristigen Zugriff der Administratoren auf die Server erlauben, aber dabei durch eine organisatorische Vier-Augen Kontrolle die Möglichkeit von ungewollter Kenntnisnahme von personenbezogenen Daten ausschließen. Kenntnisnahme ist nur visuell vom Bildschirm möglich.

SPLITCloud bietet damit effektive Schutzmaßnahmen gegen Kenntnisnahme von gespeicherten Daten seitens aller möglichen Akteure. Der Schutz geht weit über den bisherigen Stand der Technik hinaus und setzt sich sehr deutlich von der Situation des herkömmlichen Cloud-Computings ab. Es ist aber wichtig zu beachten, dass ein Großteil der oben beschriebene Schutz direkt vom korrekten Verhalten des TOM-Administrators abhängt.

2.5.5.3 Schutz während der Verarbeitung von Daten

Im Folgenden werden die Schutzmaßnahmen von SPLITCloud für Daten während der Verarbeitung beschrieben und mit den Anforderungen von Sektion 2.2.4.3 verglichen.

Die Anforderungen beschreiben verschiedene Zugriffswege für die mögliche Kenntnisnahme von personenbezogenen Daten. Betreffend dem Zugriffsweg 1, durch die Netzwerkschnittstelle der Applikation, bietet SPLITCloud mit seinen VPNs weitgehenden Schutz um alle illegitimen Akteure fernzuhalten. Kombiniert mit den Möglichkeiten einer starken Authentisierung (Smartcard Login) und schwer-kompromitierbaren Terminals (Secure Desktop) bietet SPLITCloud optimalen Schutz.

Zugriffsweg 2 ist geschützt, da während des Betriebs keinerlei Zugriff auf die Guest Betriebssysteme gewährt wird. Dies wird vom TOM-Server her gesteuert und ist effektiv, da Zugriff nur über VPNs erfolgen kann.

Zugriffsweg 3 ist durch die Elimination der Rolle des Administrators des Host Betriebssystems geschützt (siehe Details oben). Das mit *grsecurity* gehärtete Host Betriebssystem bietet zudem den mit dem heutigen Stand der Technik möglichen Schutz gegen Angriffe mit dem Ziel, *root* Zugang zu erhalten.

SPLITCloud wird derzeit durch zusätzliche Verwendung von Methoden des Mandatory Access Controls zur Durchsetzung der Isolation zwischen virtuellen Maschinen untereinander und mit dem Hypervisor erweitert. Damit wird es dem Stand der Technik entsprechenden Schutz des Zugriffwegs 4 bieten.

SPLITCloud bietet damit auch im Bereich der Verarbeitung von Daten den mit der heutigen Technologie möglichen maximalen Schutz. Es ist aber wichtig zu beachten, dass ein Großteil der oben beschriebene Schutz direkt vom korrekten Verhalten des TOM-Administrators abhängt.

3. Bewertung von SPLITCloud

Nach dem obigen Soll-Ist-Vergleich der Datenschutz-Anforderungen bewertet diese Sektion SPLITCloud als Ganzes. Nach einem einleiten Blick auf die durch SPLITCloud adressierten zentralen Herausforderungen (3.1), wird der Einsatz der SPLITCloud-Lösung in unterschiedlichen vertraglichen Gestaltungen und mit Verortung des TOM-Administrators bei unterschiedlichen Akteuren auf Vorteile für den Datenschutz untersucht (3.2) und schließlich die Mehrwerte eines Einsatzes einer SPLITCloud gegenüber einer konventionellen Cloud für die einzelnen Gewährleistungsziele durchdekliniert (3.3)

3.1 Adressierte Herausforderungen

Ein großer Teil des Schutzbedarfs von Cloud-Anwendungen im Bereich Software as a Service überdeckt sich mit dem von „herkömmlichen“, also on-premise gehosteten Anwendungen und kann daher auch mit herkömmlichen Gewährleistungsmaßnahmen bereits auf der Anwendungsebene und im organisatorischen Bereich abgedeckt werden. Die vorliegende Analyse hat diese Aspekte und Gewährleistungsziele meist nur kurz erwähnt und hat sich stattdessen auf die neuen Herausforderungen des Cloud-Computings konzentriert, bei dem Daten in den Verfügungsbereich von Dritten gelangen. Die rechtliche Entsprechung dieser Sachverhalte ist regelmäßig eine Auftragsdatenverarbeitung (siehe oben **Fehler! Verweisquelle konnte nicht gefunden werden.**), so dass im Folgenden die besondere Eignung für die Absicherung einer Auftragsdatenverarbeitung evaluiert wird.

Im Folgenden sind die wichtigsten Aspekte dieser Herausforderung zusammengefasst:

1. Im Grundsatz erhöht jede Auslagerung von IT-Aufgaben das abstrakte Risiko eines unberechtigten Zugriffs durch weitere Personen. Das Angreifermodell umfasst daher vermehrt Angriffe von Insidern und Systemoperatoren bei externen Stellen, insbesondere durch den Cloud-Provider, dessen Führung, Mitarbeiter und ggf. durch Dritte, die Zwang auf den Cloud-Provider ausüben können. Mit einer Beauftragung Externer geht daher regelmäßig auch ein Kontroll- und Transparenzverlust für den Verantwortlichen einher. Dem steht indessen nicht entgegen, dass eine Auslagerung von Aufgaben an professionelle Dienstleister in der Gesamtbetrachtung sicherer sein kann, als eine Eigenbetreib von IT gerade in kleinen Einheiten ohne sachkundige Betreuung. Dennoch bleibt es zumindest bei einer abstrakten Erhöhung des Risikos.

- Eine unkontrollierte geographische Verteilung der Datenverarbeitung bringt rechtliche Unsicherheiten. Dies weniger im Bereich der Anwendbarkeit des Datenschutzrechts, die nunmehr nach Art. 3 Abs. 2 DSGVO zugunsten des Marktortes geregelt ist. Damit unterfallen Datenverarbeitungen durch Verantwortliche und Auftragnehmer ohne Sitz oder Niederlassung im Geltungsbereich der DSGVO dennoch derselben, soweit Waren oder Dienstleistungen Unionsbürgern angeboten werden oder deren Verhalten beobachtet wird. Allerdings ist gegenüber Stellen in Drittstaaten mit einem Durchsetzungsproblem zu rechnen.[94] Damit sind Verantwortliche Stellen umso mehr gehalten, Auftragsverarbeiter in Drittstaaten zu kontrollieren, soweit eine Auswahl derselben nach Artikeln 28 und 44 ff DSGVO überhaupt in Betracht kommt. Unabhängig von dem Geltungsanspruch der DSGVO auch gegenüber Entitäten in Drittstaaten können die betroffenen Stellen Regelungen der jeweils lokal anwendbaren Rechtsordnungen sein. In Betracht kommen u.a. Rechtsordnungen am Ort des Sitzes,[95] der Niederlassung oder der Standortes der Hardware, so dass z.B. auf Grundlage lokaler Strafprozessordnungen, Geheimdienstgesetze, Zivilprozessordnungen oder auch schlicht durch ungesetzlichen Zwang Druck auf Auftragsverarbeiter in Drittstaaten ausgeübt werden kann und wird.

Da in solchen Situationen bloße organisatorische Maßnahmen oft ungenügend sind bzw. im Falle von externen Zwang auf Auftragnehmer gar nicht wirken können, müssen technische Beschränkungen gefunden werden, mit denen eine Kenntnisnahme von personenbezogenen Daten seitens dieser Akteure effektiv verhindert und hilfsweise zumindest gegenüber dem Verantwortlichen im Sinne der Transparenz offengelegt werden kann.

---

[94] Gola/Pilz Art. 3 DSGVO Rn. 26.

[95] So hat das US District Court für den südlichen District von New York die Auffassung vertreten, dass Microsoft auch solche Daten herausgeben müsse, die in Irland gespeichert wären, solange nur aus den USA auf diese Daten zugegriffen werden könne. Diese Entscheidung wurde vom zuständigen Appallationsgericht aufgehoben, https://www.heise.de/downloads/18/2/1/2/9/8/4/7/14-2985-Microsoft-US-no-rehearing.pdf. Die Ermittlungsbehörden halten an der bisherigen Rechtsauffassung fest, die auch von einem Federal District Court in Pennsylvania gegenüber Google ausgeurteilt wurde, https://www.washingtonpost.com/news/volokh-conspiracy/wp-content/uploads/sites/14/2017/02/Opinion.pdf?tid=a_inl. Damit muss auch dann mit behördlichen Zugriffen gerechnet werden, wenn sämtliche Hardware in der EU belegen ist aber der Sitz des Unternehmens oder ein relevanter Teil in den USA belegen ist.

SPLITCloud adressiert diese Herausforderungen mit einem innovativen Ansatz. Im Folgenden sind die Hauptelemente zusammengefasst:

- Basierend auf dem Konzept der Trusted Virtual Domains kreiert SPLITCloud eine starke Trenning („split“) der verschiedenen Rollen von Systembetreibern.
-
- Die Trennung ermöglicht eine gegenseitige Beschränkung und Kontrolle von Akteuren. Diese geht weit über die ansonsten übliche Selbstbeschränkung von Administratoren hinaus.
- Die Kenntnisnahme von personenbezogenen Daten durch alle Systemadministratoren kann mittels kryptographischer Maßnahmen sicher vermieden werden.
- Der TOM-Administrator ist dabei zwar durch die Sicherheitssoftware des Systems beschränkt, hat aber dennoch die Möglichkeit der Kenntnisnahme von geschützten Daten. Die Rolle des TOM-Administrators muss deshalb von einer vertrauenswürdigen Partei übernommen werden. Umgekehrt können durch den TOM-Administrator alle wesentlichen Datenverarbeitungen hinreichend kontrolliert werden.

Die Trennung von Rollen durch SPLITCloud öffnet neue Möglichkeiten der Auftragsdatenverarbeitung. Insbesondere kreiert SPLITCloud zusätzliche Möglichkeiten in der Wahl, wer welche Rolle übernehmen soll.

3.2 Gestaltungen zur Verortung der TOM-Administrators bei Auftragsdatenverarbeitung

Wie oben unter 2.5.4.6 dargestellt hat der TOM-Administrator eine wesentliche Rolle als Kontrolleur und die Fähigkeit viele Aktionen und Datenzugriffe wirksam zu beschränken. Es ist daher eine wesentliche Gestaltungsfrage, bei welcher Organisation der TOM-Administrator bzw. die TOM-Administratoren angesiedelt sind. Dem eingangs geschilderten Musteranwendungsfall folgend gibt es vier grundsätzliche Möglichkeiten, den TOM-Administrator zu verorten:

1. beim Anwender (Verantwortlichen), also dem Kunden des Applikationsbetreiber wahrgenommen durch eigenes Personal,
2. beim Applikationbetreiber (Auftragsdatenverarbeiter) als Teil der Dienstleistung für den Anwender,

3. beim Infrastruktur-Provider als Dienstleistung oder
4. als eigenständiger Dienstleister, z.B. als Teil eines IT-Sicherheitsdienstes.

Auf diese Gestaltungen wird in den folgenden Abschnitten eingegangen.

3.2.1 Verortung des TOM-Administrators beim Anwender (Verantwortlichen)

Eine Verortung direkt beim Anwender als datenschutzrechtlich Verantwortlichen wäre im Hinblick auf die Möglichkeit zur Wahrnehmung der Verantwortung wünschenswert. Ein solches System ist in Abbildung 13zur Illustration skizziert:

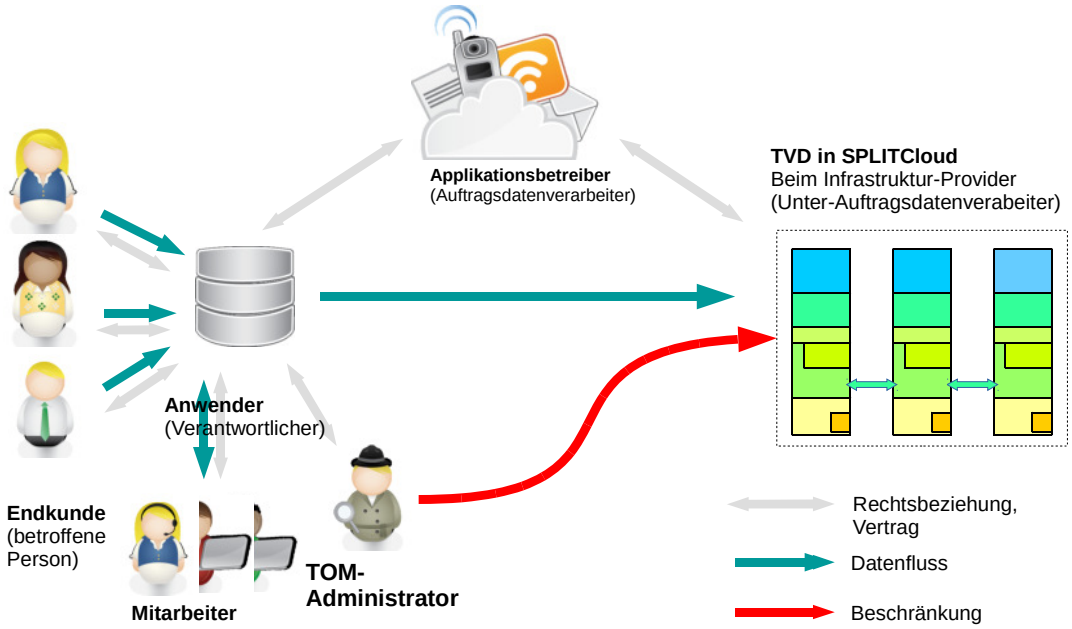

Abbildung 13 TOM-Administrator beim Anwender

Der Anwender nimmt hier im Rahmen des spezifischen (Vertrags-)Verhältnisses Daten von den Endkunden entgegen und leitet diese über die VPN gesicherte Verbindung zur weiteren Verarbeitung in die SPLITCloud weiter. Im Musteranwendungsfall ist dies die Datenübermittlung der ausgelesenen Smart Meter, die durch die Stadtwerke an den Applikationsbetreiber übertragen werden.

Die Administration der zugehörigen TVD erfolgt durch den TOM-Admin direkt beim Verantwortlichen. Als Geschäftsmodell ist dies denkbar für Anwender, die zwar die spezialisierte Software des Applikationsbetreiber, z.B. Brachnenlösungen, beziehen wollen und teilweise auch IT-Dienstleistungen auslagern möchten aber die nötigen

Ressourcen in Gestalt geschulten IT-Personals im eigenen Hause vorhalten. Die TOM-Administration kann dann durch die eigene IT-Abteilung übernommen werden. Zu Bedenken ist, dass bei Updates der Anwendungssoftware oder nötigen Änderungen in der Cloud-Konfiguration ein ggf. kurzfristiges Mitwirken des TOM-Administrators erforderlich werden kann. Diese Mitwirkung ist daher, entsprechend der festgestellten Anforderungen an die Verfügbarkeit der Systeme, durch Vertretungsregelungen und Erreichbarkeitsanforderungen an das mit dieser Rolle betraute Personal sicherzustellen.

Alle Freigaben für die Hinzunahme, den Wechsel von Hardware oder Änderungen der Systemsoftware durch den Infrastruktur-Provider sowie alle Änderungen an der Anwendungssoftware werden durch den TOM-Administrator veranlasst. Der Applikationsbetreiber kann dabei Updates für die Anwendungssoftware zur Verfügung stellen und in einer gesonderten TVD testen. Das Einspielen in die TVD mit Echtdaten kann jedoch nur durch den TOM-Administrator erfolgen. Damit ist eine effektive Kontrolle sowohl gegenüber dem Infrastuktur-Provider als auch gegenüber dem Applikationsbetreiber gewährleistet.

3.2.2 Verortung des TOM-Administrators beim Applikationsbetreiber

Die zweite grundsätzliche Gestaltung verortet den TOM-Administrator beim Applikationsbetreiber wie schematisch dargestellt in Abbildung 14:

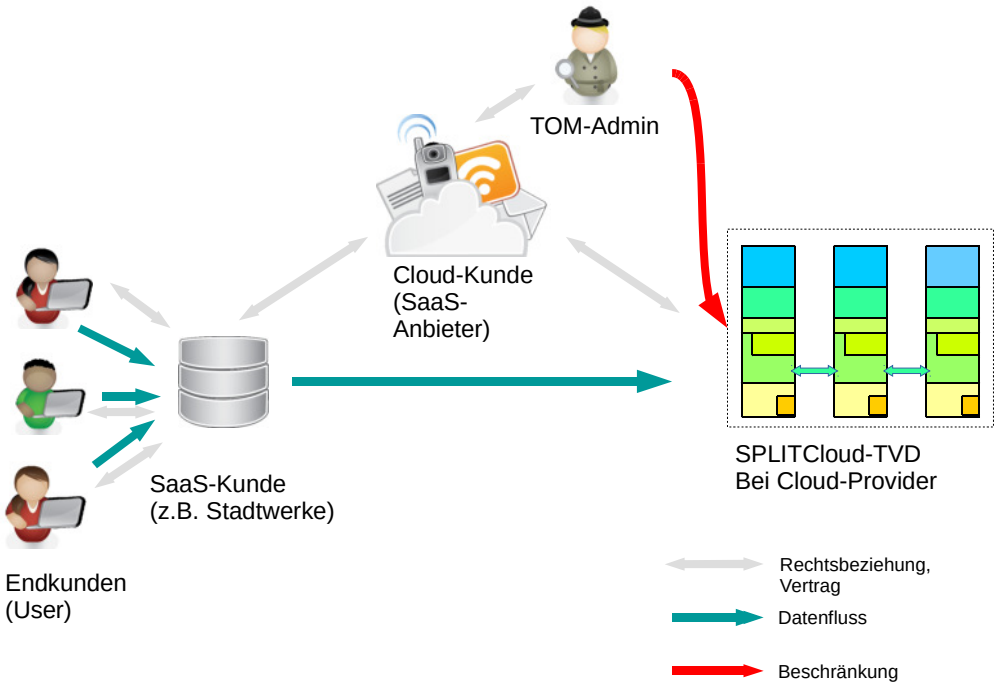

Abbildung 14 TOM-Administrator beim Applikationsbetreiber

Diese Gestaltung kommt als Geschäftsmodell von Applikationsbetreibern in Betracht, die viele vor allem kleinere Kunden betreuen, die keine eigene IT-Abteilung mehr selbst vorhalten oder vorhalten wollen. Dem Kunden wird so die Bereitstellung einer Spezial- oder Branchensoftware in Paket mit der Beauftragung und Überwachung eines geeigneten Cloud-Dienstes angeboten. Der Applikationsbetreiber bedient sich dabei seinerseits des Infrastruktur-Anbieters für die Bereitstellung der nötigen Hardware nebst Sicherheits- und Systemsoftware. Damit werden die komplexen Aufgaben jeweils in die Hand einer spezialisierten Entität verlegt. Innerhalb dieses Unterauftragsverhältnisses ist der Applikationsbetreiber verantwortlich für die Einhaltung der datenschutzrechtlichen Anforderungen und haftet gegenüber dem Anwender als (Haupt-)Verantwortlichen für die Datenverarbeitung, Art. 28 Abs. 4 DSGVO. Für das Rechtsverhältnis gelten dabei die allgemeinen Regelungen für Auftragsdatenverarbeiter. Gegenüber dem Applikationsbetreiber ist jede Beauftragung von weiteren Auftragnehmern, wie den Infrastuktur-Providern gesondert zu genehmigen oder bei einer allgemeinen Genehmigung im Vertrag zum Anwender diesem gegenüber zumindest rechtzeitig vorab anzuzeigen. Dies soll dem Kunden die Möglichkeit geben, den Infrasturkur-Provider abzulehnen, denn sowohl der Anwender als Verantwortlicher als auch der

Applikationsbetreiber als (Ober-)Auftragnehmer haften für erlittene Schäden aus der Datenverarbeitung gegenüber den Endkunden.[96]

Im Verhältnis zum Anwender ist vertraglich die Übernahme der TOM-Administration als Gegenstand der Auftragsdatenverarbeitung zu definieren. Als generelle Weisungen können bereits Erlaubnisse für das Aufspielen neuer Softwareversionen der Anwendungssoftware, insbesondere zwecks patchens kritischer Fehler, eingeräumt werden. Weitere Freigaben des TOM-Administrators können durch Richtlinien im Vertrag oder im konkreten Bedarfsfall durch Einzelgenehmigung gestattet werden.

Der TOM-Administrator kann auf diese Weise die Verarbeitung durch den Cloud-Provider überwachen. Diese Beschränkung der Befugnisse und Kontrolle des Dienstleisters dient zur Umsetzung der eigenen Verantwortung aus dem Auftragsverhältnis. Die Kontrolle und die Beschränkungsmöglichkeiten des Applikationsbetreiber entfallen bei dieser Gestaltung jedoch. Damit sind je nach Schutzbedarf weitere organisatorische Maßnahmen beim Applikationsbetreiber zu treffen. Insbesondere muss die Aufgabe der TOM-Administration organisationsintern von der operativen Systembetreuung und den für die Programmierung und Testung der angebotenen Software getrennt sein. Denkbar sind zudem weitere Lösungen zur Sicherstellung der Transparenz, wie Protokollierung aller Aktivitäten der TOM-Administratoren und ein gesichertes 4-Augen-Prinzip.

Damit ist diese Gestaltung eine ebenfalls sehr sichere Umsetzung eines SPLITCloud-Einsatzes, die jedoch ergänzende organisatorische Maßnahmen erfordern kann. Sie bietet den Vorteil, dass sie für die in der Praxis relevanten Zielgruppe kleinerer Unternehmen mit spezifischen Softwarebedarf aber ohne Ressourcen für eignes spezialisiertes IT-Personal eine im Vergleich zu einer IT-Selbstverwaltung durch Laien deutlich sicherere Datenverarbeitung anbieten kann und so zu einer Anhebung des Schutzniveaus in der Breite beitragen kann.

3.2.3 Verortung des TOM-Administrators beim Cloud-Provider

Die dritte grundsätzliche Gestaltung verortet den TOM-Administrator beim Cloud-Anbieter. Hier besteht ein erhöhtes Risiko, da der Infrastuktur-Provider und dessen Mitarbeiter gerade Teile der zu kontrollierenden Personen darstellen und eine Verortung des TOM-Administrators beim Infrastuktur-Provider gerade die durch die SPLITCloud-Technik ermöglichten Vorteile der funktionalen Trennung nicht nutzt. Damit diese

[96] Paal/Pauly/Martini Art. 28 DSGVO, Rn. 66.

Lösung gegenüber einer bloßen Selbstbeschränkung durch interne Kontrollmechanismen noch Mehrwerte bietet, bedarf es daher zwingend des Einsatzes ergänzender organisatorischer und technischer Maßnahmen.

Zunächst ist die personelle Trennung zumindest organisationsintern sicherzustellen. Der TOM-Administrator darf daher nicht mit der Administration der Hard- oder Software betraut sein. Von dem operativen IT-Geschäft ist die Funktion vielmehr hinreichend zu trennen. In Betracht kommt eine Verortung als Teil der Datenschutzabteilung. Dies bietet bei Übernahme die Vorteile, dass bereits durch technische Notwendigkeit eine Einbeziehung des TOM-Administrators und damit der Datenschutz-Expertise bei der Neu- und Umgestaltung von Systemen und Prozessen erfolgt, so dass die Kontroll-Aufgaben nach Art. 39 Abs. 1 lit. b DSGVO optimal wahrgenommen werden können.

Gegenüber den zuvor ebenfalls genannten Zugriffen durch externe Dritte, einschließlich durch Vollzugsbehörden aus Drittstaaten bietet eine Gestaltung mit TOM-Administrator beim Infrastruktur-Betreiber ebenfalls weniger Möglichkeiten, da der TOM-Administrator kaum organisationsintern eine derart gefestigte Rechtsstellung erlangen kann, die ihn von datenschutzwidrigen Weisungen der Unternehmensführung befreien kann. Gegebenenfalls könnte sogar ein temporäres Abstellen bestehender der Protokollfunktionen von Dritter Seite verlangt und mit Hilfe des TOM-Administrators ermöglicht werden. Daher sind an dieser Stelle kreative Gestaltungen erforderlich und im Einzelfall auf Umsetzbarkeit zu prüfen. Denkbar wären z.B. technische Maßnahmen wie eine revisionssichere Protokollierung, automatisierte Mitteilungen über das Verändern von Kerneinstellungen und Protokollierungsfunktionen oder organisatorische Maßnahmen wie eine höchstmögliche Unabhängigkeit in der Person des TOM-Administrators auch von Einflüssen Dritten durch einen Standort in der EU und vertragliche ggf. durch Dritte garantierte Zusicherungen und direkten unabdingbaren (Berichts-)Pflichten gegenüber den Auftragnehmer. So könnte der TOM-Administrator auch ein externer IT-Berater – idealerweise mit Lokation im Sitz-Staat des Verantwortlichen (des Anwenders oder zumindest des in einem Mitgliedsstaat ansässigen Applikationsbetreibers) – sein, der über einen Vertrag zugunsten Dritter im Auftragsdatenverarbeitungsvertrag Pflichten direkt gegenüber dem Anwender zur Wahrung von dessen Interessen unabhängig von Weisungen des Rechenzentrumsbetreibers erhält.

Eine solche Konstellation wurde nachstehend in Abbildung 15 skizziert:

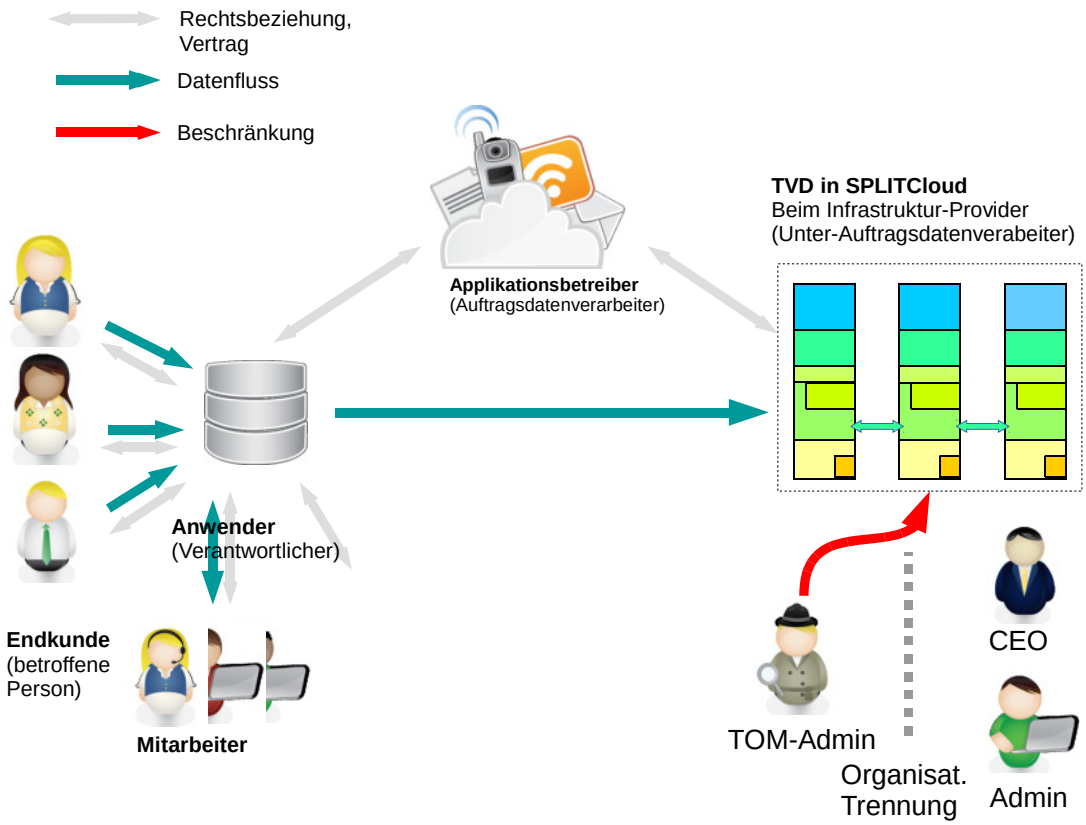

Abbildung 15 TOM-Administrator beim Infrastruktur-Provider

Zusammenfassend bleibt für diese Konstellation zu vermerken, dass wesentliche Vorteile der SPLITCloud-Architektur nicht genutzt werden. Möglicherweise stellt sie jedoch für Infrastruktur-Provider von Kunden mit gehobenem Bedarf oder Anbietern (Infrastruktur-Providern oder Applikationsbetreibern) mit Sitz in Drittstaaten eine geeignete Möglichkeit dar, erhöhten Schutz und Transparenz anzubieten. Ob dies möglich ist, hängt jedoch stark von den Bedingungen des Einzelfalls einschließlich der Rechtslage an Sitz, Niederlassung und Serverstandort ab.

3.2.4 TOM-Administrators als eigenständige Dienstleistung

Die genannten grundsätzlichen Verortungen des TOM-Administrators können schließlich auch jeweils in Kombination mit einer Beauftragung eines internen oder externen IT-Sicherheitsbeauftragten verbunden werden.

Es ist absehbar, dass sich in der Praxis auch die Frage nach der Übertragbarkeit dieser Aufgabe an einen Datenschutzbeauftragten stellen wird. Die Möglichkeit der Bestellung externer Datenschutzbeauftragter hat sich bereits unter der Anwendung des BDSG

bewährt und bleibt auch unter Anwendung der DSGVO möglich, Art. 37 Abs. 6 DSGVO.[97] Das Recht sieht also explizit vor, dass spezialisierte Aufgaben der Überwachung an Externe vergeben werden können. Der Datenschutzbeauftragte ist allerdings gesetzlich von Weisungen bei der Ausübung seiner Tätigkeit frei zu halten, Art. 38 Abs. 3 S. 1 DSGVO. Die unter dem BDSG erörterte Frage eines Ausschlusses der Bestellung wegen einer Interessenskollision als Unterfall der mangelnden Zuverlässigkeit[98] findet sich im Normtext der DSGVO nicht mehr und die zum Redaktionsschluss vorliegende Kommentarliteratur spart diese Frage gleichsam aus.[99]

Insoweit sind zwei mögliche Auslegungen denkbar:

Mit Blick auf den Gesetzestext kann einerseits vertreten werden, dass in der Wahrnehmung der Aufgabe eines TOM-Administrators kein Konflikt mit der Wahrnehmung der Aufgaben eines Datenschutzbeauftragten liegt. Dies wird durch die Beobachtung gestützt, dass der im Art. 35 Abs. 6 DSGVO-Entwurf von 2012[100] noch explizit genannte Ausschlussgrund eines Interessenskonfliktes mit sonstigen beruflichen Pflichten in der finalen Fassung der DSGVO nicht mehr enthalten ist. Die Entwurfsfassung sah vor, dass andere berufliche Pflichten mit denen, die ihm in der Funktion als Datenschutzbeauftragter obliegen, vereinbar sein müssen und zu keinen Interessenkonflikten führen. Eine derartige Vereinbarkeit wäre hier indes gegeben. Die Position des TOM-Administrators ist nicht die eines IT-Verantwortlichen oder der einer zum Betrieb der IT bestellten Person. Vielmehr überwiegen die für einen Datenschutzbeauftragten typischen Tätigkeiten der Kontrolle und Freigabe, was im Gleichlauf mit den entsprechenden Pflichten steht.

Umgekehrt kann andererseits bereits in der Entscheidung über die Freigabe von Ressourcen und Zugriffsmöglichkeiten ein Interessenkonflikt gesehen werden – so wohl die Auffassung unter Geltung des BDSG. Eine beschränkte Übertragung der TOM-Rolle für Zwecke der Kontrolle wäre danach statthaft, soweit keine weitergehende Möglichkeiten der Rechtefreigabe bestünden und diese Aufgabe an eine weitere Person delegiert würde.

---

[97] Kühling/Buchner/Bergt, Art. 37 DSGVO Rn. 30; Paal/Pauly/Paal Art. 37 DSGVO Rn. 15.
[98] Siehe Gola/Schomerus § 4f BDSG Rn. 24.
[99] Kühling/Buchner/Bergt, Art. 37 DSGVO Rn. 33ff; Gola/Klug Art. 37 Rn. 18.
[100] Siehe KOM 2012/0011 (COD), online: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_de.pdf.

Letztlich wird diese Frage aus der Kontroll- und Beratungspraxis der Aufsichtsbehörden heraus zu beantworten sein. Diesbezüglich ist zu wünschen, dass die vorstehenden Argumentationslinien in den Erwägungen Berücksichtigung finden, insbesondere die in der Person des TOM zur Verfügung stehenden Kontrollmechanismen der internen und externen Datenschutzaufsicht eröffnet bleiben.

3.2.1 Zusammenfassung

Die Auswahl des beteiligten Akteurs zur Verortung des TOM-Administrators hat maßgeblich Einfluss auf die Effektivität der ermöglichen Kontrollen und Beschränkungen regelwidriger Verarbeitungen durch eine SPLITCloud. Im Grundsatz ist es besser, je näher der TOM-Administrator dem Verantwortlichen steht.

Durch die Ausstattung des TOM-Administrators mit den erforderlichen Freiheiten von einer Organisationseinheit im Drittstaat kann eine sorgfältig wahrgenommene Aufgabe eines TOM-Administrators ggf. auch Risiken von Drittstaatenbezügen teilweise kompensieren. Die Evaluation ist dabei im Einzelfall durchzuführen, der Einsatz einer SPLITCloud-Lösung ist als technische und organisatorische Maßnahme entsprechend zu würdigen. Der räumlichen und organisatorischen Verortung des TOM-Administrators ist bei der Würdigung umfassend zu berücksichtigen.

3.3 Mehrwerte für einzelne Gewährleistungsziele

Durch die mittels eines Einsatzes einer SPLITCloud begründeten Trennung von der Administration und der unterliegenden Soft- und Hardware von Aufgaben der Kontrolle und Beschränkung der Berechtigung ergeben sich für die unterschiedlichen Gewährleistungsziele Vorteile, die nachstehend im Abgleich mit der oben erfolgten Schutzbedarfsbestimmung (oben 2.2) erörtert werden sollen

Wie bereits dargestellt, ist ein zentrales Problem der Nutzung von Cloud-Infrastrukturen, die durch Dritte bereitgestellt werden, der Schutz der Vertraulichkeit der verarbeiteten Informationen – seien es personenbezogene Daten von Kunden oder Geschäfts-geheimisse. Der Einsatz einer SPLITCloud vor allem auf eine Verbesserung der Vertraulichkeit als Schutz vor unbefugten und unbeobachteten Zugriff durch Insider bei den mit der Verarbeitung betrauten Stellen sowie Zugriffe Externer.

Nachstehend werden die Effekte eines Einsatzes der SPLITCloud-Lösung für die unterschiedlichen Gewährleistungsziele betrachtet.

3.3.1 Datenminimierung

Wie oben dargelegt (2.2.1) setzt das Gewährleistungsziel der Datenminimierung die Anforderung des Normgebers aus Art. 5 Abs. 1 lit. c DSGVO um, dass die Datenverarbeitung inhaltlich auf ein Minimum zu beschränken ist.

Ganz zentral setzt die SPLITCloud den Aspekt der Datenminimierung um, dass nur befugtes Personal im Rahmen der erforderlichen Zugangsmöglichkeiten zu personenbezogenen Daten erhalten soll. Bei korrekter Implementierung wird Administratoren der Hardware im weiten Umfang der Zugang entzogen.

Der Prozess zum Testen und Updaten von Software durch den Applikationsbetreiber setzt zudem die Anforderung um, dass Verarbeitungsprozesse bevorzugt automatisiert erfolgen sollen und so die Kenntnisnahme von Daten durch Personen verunmöglicht werden soll. Die Software wird dabei in einer gesonderten Test-TVD validiert und nur der TOM-Administrator kann ein Überspielen der getesteten Software in die geschützte TVD veranlassen. Damit wird schließlich die Einbeziehung in den Prozess der Freigabe forciert.

3.3.2 Verfügbarkeit

Bereits der Cloud-Einsatz an sich bietet durch die Möglichkeit redundante Systeme zu nuten hohe Verfügbarkeitsressourcen. SPLITCloud relativiert diesen Gewinn, als dass nicht alle zur Verfügung stehenden Ressourcen in Form von Hardware oder virtuellen Maschinen spontan und durch automatisierte Entscheidung genutzt werden können. Vielmehr muss der TOM-Administrator die Installation der TVD auf einer neuen Maschine freigeben, so dass die zur Verschlüsselung erforderlichen Schlüssel auch auf dieser Maschine installiert werden. Denkbar ist, dass bereits im Vorwege bei der Installation der TVD einige Ressourcen „in Reserve“ für die Aufnahme einer TVD vorkonfiguriert werden, so dass die Möglichkeit, auf redundante Systeme zurückzugreifen, erhalten bleibt. Die verbleibende Einschränkung, Daten nicht Standortübergreifend und weltweit verschieben zu können ist indessen keine beachtenswerte Einschränkung sondern eine explizit aus Datenschutzperspektive wünschenswerte Eigenschaft. Der TOM-Administrator erlangt insoweit in wünschenswerter Weise eine wesentliche Kontrolle über den Standort der Datenverarbeitung.

3.3.3 Integrität

Die Integrität der Daten, Prozesse und Systeme wird durch den Einsatz einer SPLITCloud-Lösung inhärent verbessert. Durch die gewährleistete Isolation und Vertraulichkeit werden Einflüsse Dritter weitgehend vermieden, was die Integrität

zugutekommt. Die gewünschte Gewährleistung der Einschränkung von Schreib- und Änderungsrechten[101] ist zwar überwiegend auf Ebene der jeweiligen Anwendungen zu implementieren, wird durch SPLITCloud jedoch auch gegenüber Mitarbeitern des Applikationsbetreibers und des Infrastruktur-Providers sichergestellt. Auch die Dokumentierte Zuweisung von Rechten und Rollen[102] wird ermöglicht, wobei hierzu zwar bereits Lösungen für sichere Logging bestehen, mit der SPLITCloud durch die zwingende Einbindung des TOM-Administrators, der idealerweise beim Verantwortlichen zu verorten ist (dazu unten) über bloße Protokollierungen hinausgegangen wird.

3.3.4 Vertraulichkeit

Das Gewährleistungsziel Vertraulichkeit bezeichnet die Anforderung, dass keine Person personenbezogene Daten unbefugt zur Kenntnis nehmen kann, was auch gegenüber dem Auftragsdatenverarbeiter und dessen Mitarbeitern gilt.[103]

Die obige Darstellung (2.2.4) unterscheidet dabei für die Vertraulichkeit der Daten bei der Datenübertragung, der Speicherung und der Verarbeitung. Die Bewertung der Risiken bei Einsatz der SPLITCloud in diesen Kategorien ist positiv. So werden Daten im Transfer umfassend verschlüsselt und auch eine schwache Authentifikation auf der Ebene der Anwendung kann durch den Einsatz des zur SPLITCloud gehörenden VPN und zum Teil auch Secure Desktops aufgefangen werden (2.5.5.1). Für die Vertraulichkeit gespeicherter Daten ergeben sich Mehrwerte, die über eine reguläre Verschlüsselung der Daten hinaus und über die herkömmlichen Maßnahmen im Bereich des Cloud-Computing weit hinausgehen (2.5.5.2), was jedoch vom korrekten und sorgfältigen Agieren des TOM-Administrators abhängig ist. Zum Zeitpunkt der Verarbeitung der Daten bietet eine SPLITCloud-Lösung gleichsam Vertraulichkeits-schutz, indem Zugriffe sowohl seitens Unbefugter als auch Systembetreiber auf die Netzwerkschnittstelle durch das VPN weitgehend verhindert werden (siehe 2.5.5.3).

Der Einsatz einer SPLITCloud hat erhebliche Vorteile im Bereich der Vertraulichkeit. Dabei ist die Vertraulichkeit für den Einsatz von Cloud-Diensten, die nicht vollständig unter der Kontrolle des Verantwortlichen stehen, von hervorgehobener Bedeutung.

3.3.1 Nichtverkettung

Das Gewährleistungsziel der Nichtverkettung sichert den Grundsatz der Zweckbindung auf der Ebene der Gewährleistungsziele. Der Einsatz einer SPLITCloud-Lösung stellt in

[101] DSK, SDM v1.0, S. 31.
[102] DSK, SDM v1.0, S. 31.
[103] DSK, SDM v1.0, S. 13f.

diesem Kontext die konkrete Umsetzung einer Maßnahme zur Einschränkung von Verarbeitungs-, Nutzungs- und Übermittlungsrechten[104] dar. Ein Zugriff von anderen Cloud-Kunden und die Verkettung mit Daten unterschiedlicher Mandanten ist durch eine effektive Mandantentrennung sicherzustellen. Dies ist bei SPLITCloud bereits durch die Verschlüsselung der einzelnen TVD weitgehend sichergestellt. Dennoch sollten parallel die Standard-Maßnahmen zur Mandantentrennung auf Systemebene vorhanden sein. Ein SPLITCloud-Einsatz unterstützt effektiv solche Maßnahmen.

Die starke Isolation und Vertraulichkeit in SPLITCloud verhindern ungewollte Verkettungen von personenbezogenen Daten. Insbesondere wird dies erreicht, indem Systembetreiber keine Kenntnis dieser Daten erlangen können.

3.3.2 Transparenz

Das Gewährleistungsziel der Transparenz ist wie beschrieben (2.2.6) nicht auf die Transparenz gegenüber den Betroffenen z.B. durch die Bereitstellung einer Datenschutzerklärung beschränkt sondern adressiert auch die Organisation des Verantwortlichen und von Auftragsverarbeitern selbst. Durch einen SPLITCloud-Einsatz werden Zugriffe und Änderungen am System prüffähig gemacht. So kann klar nachvollzogen werden, welche Softwareversionen aufgespielt wurden und welche Änderungen am System erfolgt sind. Wird die Rolle des TOM-Administrators dabei in beim Verantwortlichen verortet, ist die SPLITCloud eine sehr effektive Maßnahme zur Sicherstellung der Transparenz.

Eine gewisse Herausforderung wird die Dokumentation des Systems für die Kenntnisnahme durch Dritte, z.B. für prüfende Aufsichtsbehörden, darstellen. Hier ist die Funktionsweise der SPLITCloud ebenso darzulegen wie die getroffenen Systementscheidungen (Überantwortung der Aufgabe der TOM-Administration, Ablageort und Sicherung von Verschlüsselungsschlüsseln, etc.). Generell geht diese Verantwortung nicht über die anderer Systeme hinaus. Vielmehr wird durch die klare Darlegung der getroffenen Sicherungsmaßnahmen die Prüfung nach Art. 32 Abs. 1 DSGVO, ob geeignete technische und organisatorische Maßnahmen getroffen wurden, um ein angemessenes Schutzniveau zu gewährleisten vereinfacht. Zudem ist die Herstellung der Transparenz für den rechtskonformen Betrieb einer Datenverarbeitungsanlage erforderlich.[105]

---

[104] DSK, SDM v1.0, S. 31f.
[105] DSK, SDM v1.0, S. 15.

Test- und Freigabevorgänge sind sauber zu dokumentieren. Eine SPLITCloud unterstützt diesen Prozess, indem sämtliche wesentlichen Systementscheidungen vom TOM-Administrator zu treffen sind (2.2.6).

Indem SPLITCloud die Kenntnisnahme von personenbezogenen Daten seitens des Infrastruktur-Providers und des Applikationsbetreibers verhindert, löst es mittelbar eines der wichtigen Transparenzprobleme des Cloud-Computing, indem es hilft zu dokumentierten, auf welchen Systemen, mit welche Zugriffsrechten die Daten verarbeitet werden und diese Kontrolle in eine andere Hand als die des agierenden Auftragnehmers gegeben werden kann. Indem SPLITCloud daneben verschiedene Funktionen von Systembetreibern unterscheidet und es ermöglicht, dass ein Betreiber (d.h. Organisation) den andern beschränkt oder kontrolliert (siehe Bewertung in Sektion 6), erhöht es wesentlich die Revisionierbarkeit im Gesamtsystem.

3.3.3 Intervenierbarkeit

Das Gewährleistungsziel der Intervenierbarkeit umfasst alle Maßnahmen, die erforderlich sind, um betroffenen Personen die Durchsetzbarkeit und Durchsetzung ihrer Betroffenenrechte nach den Artikeln 12 bis 23 DSGVO sicherzustellen (oben 2.2.7). Zugleich ist sicherzustellen, dass der Verantwortliche die Mittel zur Beherrschung der von ihm veranlassten Datenverarbeitung hat.

Der Einsatz einer SPLITCloud verlagert wesentliche Entscheidungen über die Systemgestaltung an den TOM-Administrator. Wird dieser beim Verantwortlichen verortet stellt der Einsatz einer SPLITCloud inhärent eine weitreichende Umsetzung der Intervenierbarkeit dar. Insbesondere gewinnt so der Verantwortliche jenseits der bloßen Weisungsbefugnis gegenüber dem Auftragsdatenverarbeiter auch durch technische Maßnahmen weitreichende Einflussmöglichkeiten auf die für ihn durchgeführte Datenverarbeitung.

Es ist nicht ersichtlich, inwiefern der Einsatz einer SPLITCloud die Umsetzung der Betroffenenrechte auf Auskunft, Berichtigung oder Löschung erschwert, hier sind vielmehr alle Funktionen verfügbar, die die jeweilige Applikation z.B. für die Suche nach Daten zu einer anfragenden betroffenen Person bereitstellt. Nach der DSGVO ist bei einer Auskunft an die betroffene Person auch über Empfänger oder Kategorien von Empfängern Auskunft zu erteilen, Art. 13 Abs. 1 lit. e; Art. 14 Abs. 1 lit. e und Art. 15 Abs. 1 lit. c DSGVO. Während unter Geltung des BDSG noch unklar war, ob eine Auskunft auch die Nennung von Auftragnehmern einschließt ist dies durch klarstellende

Definitionen in der DSGVO nunmehr geklärt. So sind Empfänger alle Stellen, denen personenbezogene Daten offengelegt werden, unabhängig davon ob es sich um einen Dritten handelt, Art. 4 Nr. 9 DSGVO.[106] Auftragsverarbeiter werden dagegen von Begriff eines Dritten ausgeschlossen, Art. 4 Nr. 10 DSGVO. Damit ist klar, dass auch über konkrete Empfänger unterrichtet werden muss. Durch den Einsatz einer SPLITCloud kann kontrolliert und verhindert werden, dass Daten an Dritte übermittelt oder weitere Unterauftragnehmer – auch temporär – in Anspruch genommen werden. Zugleich wird gegenüber dem Verantwortlichen transparent erkennbar, welche konkreten Systeme eingesetzt werden. Damit unterstützt der Einsatz mittelbar auch die Gewährleistung der Intervenierbarkeit.

Als weiteres Element der Intervenierbarkeit ermöglicht die SPLITCloud, dass die Daten unverfügbar gemacht werden, da die Gewalt über die erforderlichen kryptographischen Schlüssel beim TOM-Administrator liegen – konkret liegen die Schlüssel auf dem TOM-Server, so dass dessen Kontrolle genügt, um die Daten für den Infrastruktur-Provider im Regelfall unverfügbar zu machen.

Der Einsatz einer SPLITCloud unterstützt die Sicherstellung der Intervenierbarkeit in hohem Maße im Vergleich zu einem üblichen Cloud-Einsatz.

3.3.1 Zwischenergebnis

Insgesamt profitiert eine Verarbeitung personenbezogener Daten in Rahmen einer Cloud-Infrastruktur erheblich vom Einsatz einer SPLITCloud-Lösung. Eine Abschließende Wertung bedarf der Entscheidung im konkreten Einzelfall.

Bei Datenübermittlungen ins Ausland auf der Basis verbindlicher interner Datenschutzvorschriften nach Art. 47 DSGVO ist der Einsatz einer SPLITCloud-Lösung kann zentraler Teil der Datenschutzvorschriften sein um die Anforderungen nach Abs. 2 lit. d) DSGVO zu erfüllen:

> „d) die Anwendung der allgemeinen Datenschutzgrundsätze, insbesondere Zweckbindung, Datenminimierung, begrenzte Speicherfristen, Datenqualität, Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, Rechtsgrundlage für die Verarbeitung, Verarbeitung besonderer Kategorien von personenbezogenen Daten, Maßnahmen zur Sicherstellung der

[106] Gola/Gola Art. 4 DSGVO Rn. 61.

Datensicherheit und Anforderungen für die Weiterübermittlung an nicht an diese internen Datenschutzvorschriften gebundene Stellen

Der Einsatz stellt eine Maßnahme zur Sicherstellung der Datensicherheit dar und verhindert effektiv die Weiterübermittelung an nicht durch die Datenschutzvorschrift gebundene Stellen. Durch geeignete Gestaltungen kann zudem ein hinreichend unabhängig gestellter und strikt den Regelungen der DSGVO und des lokalen Rechts unterworfener TOM-Administrator solche Übermittlungen weitgehend verhindern. In der Gesamtwürdigung für die Genehmigung nach Art. 47 Abs. 1 DSGVO wäre die Selbstverpflichtung zu einem Einsatz einer SPLITCloud-Lösung mit umfassender Kontrolle durch einen TOM-Administrator in einem EU-Mitgliedstaat daher nach hiesiger Auffassung deutlich positiv zu werten. Ob dies jedoch schon eine hinreichende Bedingung für die Genehmigung der Nutzung einer Cloud im Drittstaat darstellt kann nur im konkreten Einzelfall entschieden werden.

Schließlich kann als Anreiz für Infrastruktur-Provider und Applikationsbetreiber zum Einsatz fehlt, kann neben allgemeinen datenschutzrechtlichen Erwägungen, die auf Seiten der

4. Abschließende Empfehlungen für künftige Forschungs- und Entwicklungsarbeiten

SPLITCloud demonstriert schon in seiner jetzigen Version einen innovativen Ansatz für die Verbesserung des Datenschutzes durch technische Umsetzung der Kontrolle durch den Verantwortlichen im Rahmen einer Auftragsdatenverarbeitung beim Cloud-Einsatz. Weiterführende Ausarbeitung der folgenden Aspekte würde die Position von SPLITCloud und die Einsatzfähigkeit der entwickelten Lösung weiter stärken:

- Um die Kontrolle von Akteuren weiter zu verstärken, wird eine Protokollierung benötigt, die nicht vom Kontrollierten selbst beeinflusst werden kann. Weiterführend kann daher sein, bestehende und künftige Forschungen zu Fragen des *Mandatory Access Control,* verteilten Transaktionen, und ähnlichen Konzepten im Zusammenhang mit SPLITCloud zu betrachten. Gleiches gilt für Lösungen die Protokollierungen durch eine Drittpartei (remote logging) resistent gegen Netzwerk-Unterbrechungen machen. Eine solche könnte die gegenseitige Kontrolle, vor allem die Kontrolle des TOM-Administrators, verstärken.
- Eine Kontrolle des TOM-Administrators durch einen anderen Akteur wird stärker, wenn automatische Prozeduren fürs Auditing verwendet werden können. Die Entwicklung solcher Prozeduren wäre ein interessantes Thema weiterführender Forschungsbestrebungen.
- Der umfassende Einsatz von *Mandatory Access Control* für die Isolation von virtuellen Maschinen untereinander und gegenüber dem Host Betriebssystem kann den von SPLITCloud gebotenen Schutz weiter ausbauen. Entsprechende Initiativen sind vorhanden. Weitere Forschung auf diesem Gebiet wäre wünschenswert.
- Die Integration der SPLITCloud-Technologie mit Cloud-Management-Systemen wie z.B. *OpenStack*[107] könnte den Eintritt der Technologie in den Markt weitgehend vereinfachen.
- Weil eine Migration einer virtuellen Maschinen als Teil einer TVD die Mitwirkung des TOM-Administrators bedarf ist eine rein durch die Infrastruktur veranlasse Migration nicht trivial möglich, im Bereich des Cloud-Computing aber üblich und

[107] https://www.openstack.org/

oft gewünschte Eigenschaft (z.B. für Load Balancing oder Ersetzen von Hardware). Wie eine Migrationen von virtuellen Maschinen, automatisch und ohne Eingriff des TOM-Administrators (der typischerweise in einer andern Organisation tätig ist) durchgeführt werden könnte, ohne dabei die durch die Trennung für Kontrolle und Transparenz gewonnenen Mehrwerte zu verlieren stellt eine weitere Forschungsfrage.

Auf der rechtlichen Seite sind durch die Neuerungen der DSGVO insgesamt noch eine Reihe wesentlicher Vorfragen zu klären. Hier bestünde Anschlussfähigkeit im Rahmen einer möglichen Zertifizierung von konkreten Gestaltungen. Auch das – jedenfalls für die deutschen Rechtsanwender – noch unvertraute Rechtsinstitut der gemeinsam Verantwortlichen (joint controllers) kann im Kontext der Cloud-Datenverarbeitung weitere Fragen aufwerfen. So ist Verantwortlicher, wer „allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung […] entscheidet“, Art. Nr. 7 DSGVO. Auch wenn Auftragsverarbeitern ein gewisser Entscheidungsspielraum zukommt,[108] kann die Abgrenzung zwischen Cloud-Infrastruktur-Providern und Applikationsbetreibern schwierig werden. Für die Unternehmen geht ein Wechsel der Rollen von einem Auftragsverarbeiter mit stark eingeschränktem gegenständlichem Haftungsumfang zum Verarbeiter mit voller Haftung einem erheblichen Risiko einher. An dieser Stelle sind neben einer rechtlichen Bewertung auch die technischen Maßnahmen zu erörtern, mit denen sich die Anbieter möglichst weitgehend der Einflussmöglichkeit auf die Verarbeitung entäußern können, um die Haftung zu begrenzen. SPLITCloud kann dazu eine entsprechende Lösung darstellen. Dies bedarf für einen Praxiseinsatz weitergehender Betrachtungen im Kontext konkreter Musterfälle.

Insgesamt stellt SPLITCloud damit weitere Ansätze für anschließende Forschung und Entwicklung sowohl im technischen als auch im juristischen Bereich.

[108] Kühling/Buchner/Hartung Art. 28 DSGVO Rn. 28.

5. Literaturverzeichnis

Alexy, Die Gewichtsformel, Robert Alexy, Die Gewichtsformel, in Joachim Jickeli, Peter Kreutz, Dieter Reuter, Gedächtnisschrift für Jürgen Sonnenschein, Berlin, 2003, S. 777 ff.

Art. 29 WP, WP 196: Art. 29 Data Protection Working Party, “Opinion 05/2012 on Cloud Computing“, Adopted July 1st 2012, Working Paper 196, Doc. 01037/12/EN, online: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf.

BayLDA, „XI Datenübermittlungen“ Bayerisches Landesamt für Datenschutzaufsicht; „EU-Datenschutz-Grundverordnung (DS-GVO) – Das BayLDA auf dem Weg zur Umsetzung der Verordnung, XI Datenübermittlungen in Drittstaaten nach der DS-GVO“, online: https://www.lda.bayern.de/media/baylda_ds-gvo_11_international_transfer.pdf.

Bitkom/Holz, Datendiebstahl: Bitkom/Winfried Holz, Studie "Datendiebstahl, Spionage und Sabotage in der Industrie", Folienpräsentation, 25. April 2016, Hannover, online: https://www.bitkom.org/Presse/Anhaenge-an-PIs/2016/April/Bitkom-Charts-PK-IT-Sicherheit-in-der-Industrie-25-04-2016-final.pdf

BMJV, Entwurf eines Gesetzes zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen, online: https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/ReGE_Neuregelung_Schutzes_von_Geheimnissen_bei_Mitwirkung_Dritter_an_der_Berufsausuebung_schweigepflichtiger_Personen.pdf?__blob=publicationFile&v=2

DSK, OH Cloud Computing: Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises, „Orientierungshilfe – Cloud Computing“, Version 2.0, Stand 09.10.2014, online: https://www.datenschutz-mv.de/datenschutz/publikationen/informat/cloud/oh_cloud.pdf.

DSK, OH Smart Metering, Konferenz der Datenschutzbeauftragten des Bundes und der Länder und Düsseldorfer Kreis, Orientierungshilfe datenschutzgerechtes Smart Metering, 12; online: https://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/Orientierungshilfe_SmartMeter.pdf.

DSK, SDM v1.0: Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, „Das Standard-Datenschutzmodell – Eine Methode zur

Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele“, V.1.0 – Erprobungsfassung, November 2016, online: https://www.datenschutz-mv.de/datenschutz/sdm/sdm.html.

Engeler/Deibler/Hansen/Jensen/Obersteller: MonIKA – Monitoring durch Informationsfusion und Klassifikation zur Anomalieerkennung, Deliverable D5.1, online: https://www.datenschutzzentrum.de/uploads/projekte/D5.2_MonIKA_Datenschutz-Ausarbeitung_Anomalieerkennung_Final_pub_v1.1.pdf.

Gola/Schomerus, BDSG: Peter Gola, Rudolf Schomereus, Bundesdatenschutzgesetz Kommentar, München, 2015.

Gola: Peter Gola, Datenschutz-Grundverordnung, München 2017.

Greveler/Justus/Löhr, Ulrich Greveler, Benjamin Justus, Dennis Löhr, Forensic Content Detection through Power Consumption, in IEEE International Workshop on Security and Forensics in Communication Systems, Ottawa, Kanada, 2012; online: http://1lab.de/pub/ieee_forensics2012.pdf.

Güneysu/Vetter/Wieser, Sindy Güneysu, Miriam Vetter, Matthias Wieser, Intelligenter Rechtsrahmen für intelligente Netze (Smart Grids), in DVBl. 2011, 870, 872.

Jarass, Charta der Grundrechte der EU, 3. Aufl. München 2016, Rn. 34-36.

Kamp/Rost DuD 2013, 80: Meike Kamp, Martin Rost, Kritik an der Einwilligung – Ein Zwischenruf zu einer fiktiven Rechtsgrundlage in asymmetrischen Machtverhältnissen, DuD 2013, S. 80-83.

Kingreen, in: Calliess/Ruffert, EUV/AEUV, 5. Aufl. 2016, EU-GRCharta Artikel 8, Rn. 12.

Lüdemann/Ortmann/Pokrant, Volker Lüdemann, Manuel Ortmann, Patrick Pokrant, Datenschutz beim Smart Metering, in RDV 2016, 125, 127.

MsbG-Entwurf, Gesetzentwurf der Bundesregierung, Entwurf eines Gesetzes zur Digitalisierung der Energiewende, BT-Drucksache 18/7555, online: http://dip21.bundestag.de/dip21/btd/18/075/1807555.pdf.

Nägele/Jacobs, Thomas Nägele, Sven Jacobs, Rechtsfragen des Cloud Computing, in ZUM 2010, S. 281 – 292.

Niemann/Paul: Fabian Niemann, Jörg-Alexander Paul, Rechtsfragen des Cloud Computing, Berlin, 2014.

NIST SP-800-63: National Institute for Standards and Technology, “DRAFT NIST Special Publication 800-63-3 – Digital Identity Guidelines”, 2017, online: https://pages.nist.gov/800-63-3/sp800-63-3.html.

Otey SQL-FAQ, Michael Otey, “Transparent Data Encryption FAQs”, Webseite SQL-Server Pro, 2013, online: http://sqlmag.com/sql-server/transparent-data-encryption-faqs.

Paal/Pauly, Boris P. Paal, Daniel Pauly, Datenschutz-Grundverordnung: DS-GVO, München 2017.

Ponemon Institute, gesponsorte Studie Closing Security Gaps: Ponemon Institute, gesponsorte Studie "Closing Security Gaps to Protect Corporate Data: A Study of US and European Organizations", 2014, online: https://info.varonis.com/hubfs/docs/research_reports/Varonis_Ponemon_2016_Report.pdf.

Schuster/Reichl, CR 2010, 38: Fabian Schuster, Wolfgang Reichl, Cloud Computing & SaaS: Was sind die wirklich neuen Fragen? in CR 2010, S. 38 – 43.

Sommergut, Was Sie über die Cloud wissen müssen – FAQ Cloud Computing, in Computerwoche 2015, online: http://www.computerwoche.de/a/was-sie-ueber-die-cloud-wissen-muessen,2504589,2.

SPLITCloud D1.1 „Datenschutzrechtliche Anforderungen an das SPLITCloud-Framework“, Kiel 2015, online: http://www.splitcloud.de/?page_id=10

von Albrecht/Jotzo: Jan Philipp von Albrecht, Florian Jotzo, Das neue Datenschutzrecht der EU, München 2017.