Cloud-Services der Landesrechenzentren

Eine Handlungsempfehlung für die Ausschreibung, die Vergabe und den Betrieb von öffentlichen Aufträgen in der Cloud

(Entwurfspapier der Arbeitsgemeinschaft der Leiter derLandesrechenzentren)

Version: 3.1 vom 08.12.2014

1 EINLEITUNG

1.1 Motivation

Vertrauen ist gut, Kontrolle ist besser, so ein altes Sprichwort. Das gilt auch für die Nutzung neuer IT-Technologien, wie dem Cloud-Computing. Pro und Contra werden in diesem Zusammenhang auf allen gesellschaftlichen Ebenen derzeit diskutiert.

Der Bedarf, diese Technologie für öffentliche Einrichtungen nutzbar zu machen, ist klar erkennbar. Denn die Vorteile des Cloud-Computings liegen auf der Hand. Dies gilt als die Lösung der Zukunft, um große Datenmengen günstig zu speichern, Informationen orts- und geräteunabhängig zu nutzen und IT-Ressourcen aller Art bedarfsgerecht und flexibel bereitzustellen, ohne dass damit eigene Anschaffungs- und Betriebskosten einhergehen, denn die Abrechnung erfolgt verbrauchsorientiert.

Dabei muss klar sein: Die Daten und Ressourcen liegen auf fremden Servern an ggf. unterschiedlichen Standorten, die durch Weitverkehrsnetze untereinander verbunden sind. Die Nutzer greifen in der Regel via Internet darauf zu.

Wie kann aber eine öffentliche Einrichtung ihren gesetzlichen Pflichten nachkommen, wenn sich diese neuen IT-Technologien immer mehr und mehr ihrem Einflussbereich entziehen?

Mit diesem Papier soll dargestellt werden, wie die Landesrechenzentren der Länder den Kundenforderungen nach einem sicheren und rechtskonformen Cloud-Computing entsprechen können. Es zeigt, wie ein Vorgehen hinsichtlich eines Ausschreibungs- bzw. Umsetzungsvorhabens aussehen könnte und skizziert wesentliche Aspekte für die Auswahl eines Betriebsmodells.

Hinzu kommt, dass die in letzter Zeit bekannt gewordenen eklatanten Enthüllungen über geheimdienstliche Internet-Überwachungen, die sogenannte NSA-Affäre, das Vertrauen in die mehrheitlich unter US-amerikanischer Hoheit agierenden Cloud-Dienstleister gegen Null tendieren lässt. Damit wird die aus vorrangig wirtschaftlichen Aspekten getriebene Euphorie zur Nutzung von Cloud-Services merklich gebremst.

Wenn Verwaltungen aufgrund immer neuer Datenschutzskandale annehmen müssen, dass sie nicht mehr Herr der Daten sind, Bürger ausspioniert und damit sogar ihre Grundrechte verletzt werden, dann wächst das Misstrauen gegenüber den Cloud-Anbietern unweigerlich.

Für Bürger und Verwaltung ist es eben nicht leicht ersichtlich, wie gut ihre Daten bei bestimmten Cloud-Providern aufgehoben sind. Dies liegt auch an der mangelnden Transparenz, wer im Rahmen der Leistungserbringung eingebunden ist und welche Sicherheits- und Datenschutzstandards tatsächlich gewährleistet werden.

Gerade in solch komplexen IT-Infrastrukturen sind gegenseitiges Vertrauen und eine reale Kontrollmöglichkeit von größter Bedeutung. Denn schließlich sollte der Bürger darauf vertrauen können, dass seine Daten, die durch die öffentliche Verwaltung in der Umsetzung von Gesetzen und Vorschriften erhoben und verarbeitet werden, auch nach Recht und Gesetz geschützt sind.

Konsequentermaßen wird eine ausreichende Cybersicherheit erwartet, um dem wachsenden Risiko von Datendiebstahl und -missbrauch zu begegnen. Dafür sind in der öffentlichen Verwaltung und bei ihren IT-Dienstleistern seit langem umfassende Sicherheitsstandards wie IT-Grundschutz etabliert, die auch beim Cloud-Computing Maßstab sein müssen.

Und dennoch: Die Verwendung von Cloud-Services verspricht eine flexible, verbrauchsorientierte Bereitstellung von IT-Leistungen und senkt somit Aufwand und Kosten der IT-Planung (insbesondere die Planung und Bestellung ausreichender Kapazitäten) auf Seiten der Verwaltungs-

organisation und verlagert diese zumindest teilweise auf das servicegebende Landesrechenzentrum.

Im Zuge der technischen Verfügbarkeit von Cloud-Technologien, der zunehmenden Standardisierung von Prozessen in der öffentlichen Verwaltung und der gestiegenen Anforderungen an die Kosteneffizienz von IT-Dienstleistungen fordert die öffentliche Verwaltung mit Recht die Bereitstellung von Cloud-Dienstleistungen. Diese können durch ihr Landesrechenzentrum oder die Nutzung von Angeboten des Marktes in jedem Fall nach den Grundsätzen und rechtlichen Rahmenbedingungen des Bundes und der Länder erbracht werden.

Bei den möglichen Handlungsalternativen sind insbesondere die folgenden Aspekte zu berücksichtigen:

- Datenschutz und Informationssicherheit in den schwer kontrollierbaren Cloud-Infrastrukturen[1]
- Europaweites Vergaberecht auch für Cloud-Services, deren physische Ablageorte weitgehend unbekannt bzw. durch den Cloud-Dienstleister auch ohne Zustimmung des Cloud-Nutzers außereuropäisch gewählt werden können (strittiger Rechtsraum)
- Wahrung hoheitlicher Interessen und Handlungsspielräume

1.2 Grundlage, Bezug und Gültigkeitsgrenzen für die Handlungsempfehlung

Die in diesem Dokument enthaltene Handlungsempfehlung gilt für alle Landesrechenzentren im Hinblick auf Ausschreibung, Vergabe und Betrieb öffentlicher Aufträge in der Cloud und basiert auf den im folgenden genannten Referenzdokumenten.

Diese werden durch die vorliegende Handlungsempfehlung im Hinblick auf ihre Bedeutung und Umsetzung in den Landesrechenzentren der Länder konkretisiert.

Dokument	Untertitel	Ersteller	Version/vom
Whitepaper Cloud	Möglichkeiten von Cloud-Technologien in der öffentlichen Verwaltung	EURITAS (European Association of IT Service Providers)	1.0.0 / 30.10.2012
Eckpunktepapier Sicherheitsempfehlungen für Cloud Computing Anbieter	Mindestanforderungen in der Informationssicherheit	Bundesamt für Sicherheit in der Informationstechnik	Februar 2012

[1] *Unter der Prämisse der unbekannten oder unkontrollierbaren physischen Ablageorte muss prinzipiell davon ausgegangen werden, dass Verschlüsselung ggf. nur eingeschränkt wirksam ist. Nationales Recht räumt den staatlichen Organen häufig ein Recht zur Entschlüsselung und Einsicht in gespeicherte Daten ein. Ebenso kann eine Nation jederzeit den Zugriff zu den auf dem eigenen Hoheitsgebiet gespeicherten Daten verweigern, beschränken oder anderweitig kontrollieren.*

Dokument	Untertitel	Ersteller	Version/vom
Trusted Cloud Datenschutzrechtliche Lösungen für Cloud Computing	Ein rechtspolitisches Thesenpapier der AG Rechtsrahmen des Cloud Computing	Kompetenzzentrum Trusted Cloud	Oktober 2012
Orientierungshilfe – Cloud Computing		Arbeitskreise Technik und Medien der Konferenz des Bundes und der Länder	Version 1.0 / 26.09.2011
Cloud-Fahrplan für die öffentliche Verwaltung		Kompetenzzentrum Öffentliche IT am Fraunhofer-Institut FOKUS in Berlin	April 2014

Sofern weiterführende Empfehlungen von diesen Organen herausgegeben werden oder durch von diesen Organen vorangetriebene Maßnahmen verbindliche Umsetzung finden (z. B. Datenschutz-Zertifizierung von Cloud-Diensten, „Trusted Cloud“ des BMWi), wird eine Überarbeitung dieser Handlungsempfehlung erforderlich.

2 HERAUSFORDERUNGEN UND RISIKEN

Wie eingangs schon erwähnt, wird mit der Verwendung von Cloud-Diensten kundenseitig eine erhöhte Flexibilität in der Ressourcenverwendung (pay per use) sowie gleichzeitig eine signifikante Einsparung von Kosten erwartet. Die Beschränkung dieser Effekte auf hoch standardisierte Verfahren, die im Sinne einer Massenproduktion bereitgestellt werden können, werden von den Kunden weitgehend verstanden und akzeptiert.

Vereinfacht kann gesagt werden, dass die Flexibilität und die Kosteneffizienz durch zwei Faktoren bestimmt werden:

- **Unabhängigkeit vom eigentlichen Leistungserbringer**
  Über- oder Unterkapazitäten des beauftragten IT-Dienstleisters können von demselben frei gehandelt werden. Dadurch wird der Dienstleister davon befreit, große Kapazitätsreserven aufzubauen und zu finanzieren.
- **Unabhängigkeit vom spezifischen Kunden**
  Je mehr Kunden bzw. Nutzer aus möglichst unterschiedlichen Zielgruppen (d. h. mit unterschiedlichen Nutzungsmustern) die Leistung abfordern, desto größer ist der erreichbare Skaleneffekt , was die Notwendigkeit zur Vorhaltung von Reservekapazitäten und damit die Kosten weiter senkt und die Bereitstellung von Automatismen zur vollständigen Selbstadministration der Leistungen und des Leistungsbezugs überhaupt erst möglich (finanzierbar) macht.

Was alle seriösen Cloud-Anbieter zumindest versprechen, sind eine virtuelle Abgrenzung der Servicenehmer untereinander sowie eine Abschottung der Dateninhalte vor der Einsicht durch Dritte. Hier kommen unterschiedlichste Mechanismen und Sicherheitsstandards zum Einsatz, deren konkrete Umsetzung schwer nachvollziehbar ist.

Unabhängig von den jeweils eingesetzten Sicherheitstechniken senkt die einheitliche Bereitstellung von Services allerdings die Wirkung dieser Sicherheitstechniken. Vom Prinzip her gilt eine von einem potentiellen Angreifer gefundene Schwachstelle damit für alle Servicenehmer.

Entsprechend stehen bei der Auswahl eines Cloud-Modells immer folgende zwei Aspekte im Vordergrund:

- **Schutzbedarf der im Rahmen der bereitgestellten Services verarbeiteten Daten**
  Die Aussage „es gibt keine absolute Sicherheit“ gilt insbesondere im Zusammenhang mit standardisierten und industriell angebotenen IT-Services. Folgendes Spannungsfeld muss in Balance gebracht werden:
  - Je billiger (bzw. korrekterweise: allgemeingültiger) der Cloud Service ist, desto anfälliger ist dieser für Sicherheitslücken bzw. desto attraktiver ist dieser für Angreifer (das Ausloten einer Sicherheitslücke gewährt Zugang zu den Daten vieler Angriffsziele).
  - Je höher der Schutzbedarf der zu verarbeitenden Daten ist, desto höher ist der Bedarf an direkter Kontrolle der Verarbeitung durch den Dateneigentümer.
- **Rechtssicherheit im Falle eines Sicherheitsvorfalls**
  Wer haftet für den entstandenen Schaden, und kann dieser überhaupt haftbar gemacht werden? Auch hierfür gibt es ein dem vorhergenannten Aspekt recht ähnliches Spannungsfeld:
  - Je billiger (bzw. korrekterweise: örtlich unabhängiger) der Cloud-Service ist, desto unklarer ist der tatsächliche Ort, an dem die Datenverarbeitung geschieht. Die Identifikation eines Schuldigen kann sich streckenweise als unmöglich gestalten, zudem ist nicht sicher, dass der identifizierte Schuldige im Rahmen der geltenden nationalen Gesetze haftbar gemacht werden kann.
  - Je höher der potentielle Schaden eines Sicherheitsvorfalls ist, desto genauer muss in einem Servicevertrag die Haftung und die geschuldete Sicherheitsleistung beschrieben sein.

  Beispiel: Die Bereitstellung virtueller Server durch verschiedene indische oder chinesische Dienstleister gehört weltweit zu den günstigsten Angeboten. Im Falle eines durch einen Sicherheitsvorfall entstandenen Folgeschaden ist allerdings nicht zu erwarten, dass eine Entschädigung gezahlt wird.

Entsprechend der Datenschutzgesetze des Bundes und der Länder ist der Eigentümer der Daten verantwortlich für deren Schutz und muss sicherstellen, dass dem Schutzbedarf angemessene Schutzmechanismen bereitgestellt werden. Diese Verantwortung verbleibt beim Eigentümer und kann nicht abgegeben werden. Insofern muss sich der Eigentümer der Daten versichern, dass durch einen Dritten bereitgestellte Dienste durch den Dritten angemessen geschützt werden, und sollte er sich absichern, dass durch einen Sicherheitsvorfall beim beauftragten Dritten entstandene Schäden durch diesen behoben oder zumindest in angemessenem Umfang entschädigt werden können.

Das E-Government-Gesetz eröffnet in § 11 den Ländern jedoch die Möglichkeit, gemeinsame Verfahren zu nutzen, für die die Verantwortlichkeit der Dateneigentümer zwar nicht beseitigt, jedoch anders verteilt werden kann. Dabei kann die Verantwortlichkeit für einzelne Aufgabenbereiche einem Land zugeordnet werden, unabhängig davon, Daten welchen Landes verarbeitet werden und somit eine effektivere Datenverarbeitung gewährleistet werden.

Die Herausforderung besteht insgesamt darin, effizientes Cloud Computing anzubieten, dass rechtliche Randbedingungen, regulatorische Anforderungen und Informationssicherheitsstandards genügt und dann immer noch effizient ist.

3 CLOUD-BETRIEBSMODELLE IM KONTEXT DER LANDESRECHENZENTREN

Die IT-Infrastrukturen der Landesrechenzentren sind aufgrund der erhöhten Schutzbedarfsanforderungen der öffentlichen Verwaltung auf ein überdurchschnittlich hohes Sicherheitsniveau ausgerichtet und verfügen größtenteils über zertifizierte Rechenzentren. Zudem sind die Landesrechenzentren an die besonders gesicherten landesinternen und überregionalen Verwaltungsnetze sowie an die Netze des Bundes (z. B. DOI) angebunden. Ebenso sind Dienstleistungsspektrum, Abarbeitungsprozesse und IT-Verfahren auf die Bedürfnisse der öffentlichen Verwaltungen zugeschnitten. Dieses muss im Zusammenhang mit künftigen Dienstleitungsangeboten im Cloud-Computing mit dem Ziel berücksichtigt werden, bestimmte Cloud-Dienste als Shared Services im Rahmen der Kooperation der Landesrechenzentren ebenfalls anderen Landesrechenzentren anzubieten und zur Verfügung zu stellen.

Wie im vorhergehenden Abschnitt erläutert, liegt die Verantwortung für den Schutz der Daten in der Hand des Dateneigentümers, also der jeweiligen Behörde. Entsprechend kann auch (auf eigenes Risiko) entschieden werden, einen Billiganbieter zu verwenden, solange dem keine gesetzlichen Vorgaben entgegenstehen. Vor diesem Hintergrund empfehlen wir, die in folgende Kategorien eingeteilten Betriebsmodelle entsprechend der Schutzbedarfseinstufung zu betrachten.

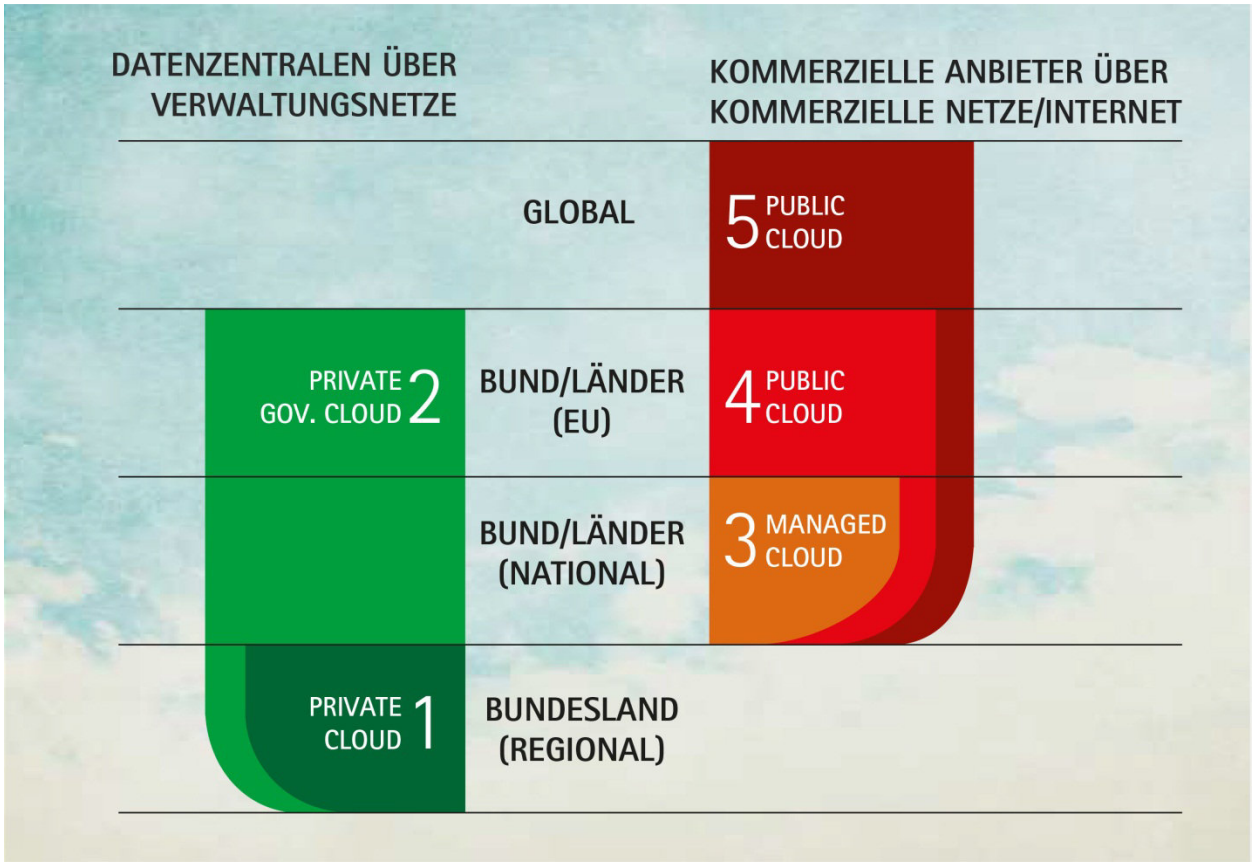


Abb. 1: Die Cloud-Kategorien im Kontext der Landesrechenzentren

3.1 Kategorie 1: Private Cloud

Bei der Private Cloud handelt es sich um einen individuell und exklusiv für einen Kunden eingerichteten Service, der genaugenommen als Managed Private Cloud anzusehen ist. Hiermit werden verschiedene Cloud-Charakteristika erfüllt, u. a.:

- Verbrauchsabhängige Abrechnung
- Selbstbedienung und freie Konfiguration
- Virtuell unbegrenzte Ressourcen

Dieses Modell bietet die besten Sicherheiten sowohl hinsichtlich Datenschutz als auch hinsichtlich Haftung und zeichnet sich üblicherweise durch einen individuellen Vertrag aus, in dessen Rahmen die Leistung bezogen werden kann und mit dem alle erforderlichen Rahmenbedingungen der Auftragsdatenverarbeitung gemäß der geltenden Datenschutzgesetze schriftlich vereinbart werden. Darüber hinaus ist die Anbindung über das landesinterne Verwaltungsnetz gewährleistet.

Die Abstufungen in diesem Modell ergeben sich aus den durch den Anbieter erfüllten Sicherheitsstandards (z. B. ISO 27001 auf Basis IT Grundschutz) sowie aus dessen speziellen Kenntnissen der Verfahren und Bedürfnisse der Landesverwaltung. In jedem Fall ist bekannt, wer (im Einzelfall sogar welche Person) die Daten handhabt und welches Gericht im Schadensfall zuständig ist.

3.2 Kategorie 2: Private Government Cloud (PGC)

Services, die bundesweit einheitlich bereitgestellt werden, können von jedem Bundesland bezogen werden. Im Rahmen der Private Government Cloud (PGC) können Skalen-Effekte realisiert werden, die dem einzelnen Land nicht möglich wären, und somit diese Art von Service kostengünstiger als ein einzelnes Rechenzentrum anbieten (Stichwort: Community Cloud).

Die Netzanbindung ist durch die verschiedenen Ebenen der Verwaltungsnetze gewährleistet.

Dieses Modell realisiert immer noch einen recht hohen Sicherheitsstandard, da Ressourcen unter vertrauenswürdigen Partnern geteilt werden, die einem definierten Sicherheitsniveau verpflichtet sind. Allerdings sind die getroffenen Sicherheitsmaßnahmen aufgrund der Tatsache der verteilten Nutzung niemals so wirksam wie in der Private Cloud.

Das Betreibermodell dieser Kategorie wird technisch und organisatorisch in folgenden Ausprägungen umgesetzt:

Nationale PGC

Hier gilt in jedem Fall deutsches Recht und somit können die Vorzüge z. B. der Bundes- und Landesdatenschutzgesetze konsequent genutzt werden.

Dieses Cloud-Modell wird von dem betreffenden Landesrechenzentrum im Rahmen des Dienstleistungsverbundes der Landesrechenzentren auch anderen Landesrechenzentren zur Nutzung für deren Kunden bereitgestellt. Das betreffende Landesrechenzentrum tritt in diesem Zusammenhang gegenüber dem Auftraggeber als Cloud-Service-Provider (CSP) auf und ist somit Auftragnehmer im datenschutzrechtlichen Sinne.

Dabei werden die folgenden Möglichkeiten der technischen Bereitstellung der Cloud-Infrastruktur unterschieden:

- **Interne National PGC**
  Bei einer „internen“ National PGC befindet sich die Cloud-Infrastruktur im „eigenen“ Rechenzentrum und unterliegt den ggf. zertifizierten Bedingungen des Landesrechenzentrums. Die Leistungen werden länderübergreifend auch anderen Landesrechenzentren sowie deren Kunden angeboten. Im Falle von Kapazitätsengpässen können Kapazitäten flexibel von „externen“ National PGC-Anbietern hinzugekauft werden.
- **Landesrechenzentren übergreifende „verwaltungsinterne“ National PGC**
  Hierbei kombinieren im „Grid-Computing-Ansatz“ mehrere Landesrechenzentren Ihren Ressourcen, um Ausfallsicherheit und Spitzenabdeckung sicher zu stellen. Durch die Koppelung mehrerer nationaler Rechenzentren können höhere Skaleneffekte bei gleichzeitig hoher Sicherheit innerhalb der Verwaltung realisiert werden.
- **Externe National PGC**
  Bei einer „externen“ National PGC befindet sich die Cloud-Infrastruktur außerhalb des „eigenen“ Rechenzentrums, wird von einem externen National PGC-Anbieter eingekauft und ggf. mit eigenen Funktionen angereichert. In diesem Fall wird die Cloud physisch von einem dezidierten externen RZ-Anbieter betrieben, dessen Standort sich in Deutschland befindet und der den im Ausschreibungsverfahren definierten Anforderungen in Bezug auf die fachlichen, organisatorischen, betrieblichen und sicherheitstechnischen Anforderungen gerecht wird.

European PGC

Dieses Modell entspricht der „Landesrechenzentren übergreifenden verwaltungsinternen National PGC“, jedoch in einer internationalen Verwaltungskooperation. Damit kann eine EU-weite Aufgabenteilung und Skalierung innerhalb der verwaltungstechnischen Rahmenbedingungen ohne Kompromisse mit sehr großen Skaleneffekten realisiert werden. Diese Abkommen können bi- oder multilateral abgeschlossen werden.

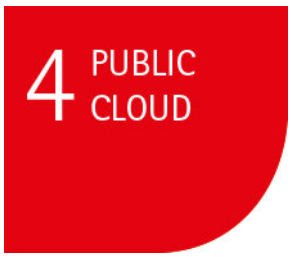
3.3 Kategorie 3: Managed Cloud kommerzieller deutscher Anbieter

Dieses Modell entspricht im Wesentlichen der Kategorie 1 mit dem Unterschied, dass es sich bei dem Anbieter um einen kommerziellen Anbieter ohne die in den Landesrechenzentren besondere Spezialisierung für die öffentliche Verwaltung handelt und die Netzanbindung nicht über ein Verwaltungsnetz erfolgt.[2]

Sicherheitsstandard und Rechtssicherheit sind vergleichsweise hoch bzw. gut im Rahmen einer Ausschreibung bewertbar. Die besonderen Regeln für den Datenschutz im Landesrecht sowie die besonderen Sicherheitsbedürfnisse der öffentlichen Hand werden aber zumeist nicht gut abgedeckt werden können, da diese Anbieter im Gegensatz zu den hierauf spezialisierten Landesrechenzentren in der Regel mit den besonderen Anforderungen der öffentlichen Hand nicht vertraut sind. Dieser Aspekt sollte im Rahmen einer Ausschreibung besondere Berücksichtigung erfahren.

[2] *Aus Sicht der Landesrechenzentren gibt es gegenwärtig keine kommerziellen Anbieter für private Clouds (Kategorie 3) außerhalb Deutschlands, die als Cloud-Anbieter für die öffentlichen Verwaltungen in Frage kommen. Insofern wird dieses nicht weiter betrachtet.*

3.4 Kategorie 4: Public Cloud kommerzieller europäischer Anbieter



Public Clouds werden von privat organisierten Firmen betrieben, wobei in den meisten Fällen unbekannt ist, von welchem Rechenzentrum die eigentlichen Cloud-Infrastrukturen bereitgestellt und betrieben werden, wo sich diese Standorte befinden und welchen Sicherheitskriterien sie unterliegen.[3] Auch hier erfolgt die Netzanbindung nicht über ein Verwaltungsnetz.

Nichtsdestotrotz kann sich sowohl aus der Firmenstruktur als auch aus den Verträgen mit solchen Anbietern ergeben, dass ausschließlich Rechenzentren im europäischen Raum zum Einsatz kommen bzw. solche, die anhand der Standardvertragsklauseln der Europäischen Kommission unter bestimmten Bedingungen den Anforderungen des deutschen Datenschutzrechts genügen sowie welche Sicherheitsstandards die einzelnen Rechenzentren mindestens einhalten.

Sofern bei solchen Betreibermodellen personenbezogene Daten verarbeitet werden sollen, wird allerdings kaum eine hinreichende Berücksichtigung der einschlägigen Vorschriften der Datenschutzgesetze der Länder erreicht werden. Insofern betrifft dieses Modell im Wesentlichen Daten ohne direkten Personenbezug wenn sicher ist, dass dieser auch nicht durch die Kombination der verarbeiteten Daten hergestellt werden kann.

Die – wie in Abschnitt 2 dargestellte – eingeschränkte Sicherheit sowie die üblicherweise ebenso eingeschränkte Haftbarkeit müssen natürlich berücksichtigt werden, ebenso wie das Fehlen von spezifischen Fachverfahren der Verwaltung.

3.5 Kategorie 5: Sonstige Public Clouds

Anbieter, deren Rechenzentren nicht an Orten stehen, die durch das Bundesdatenschutzgesetz (BDSG) als unbedenklich einzustufen sind oder deren Orte unbekannt sind, müssen als unsicher betrachtet werden.

Sie sind vergleichbar mit öffentlichen Plätzen und fallen unter die Rubrik „auf eigene Gefahr“. Das gilt also nur für solche Daten, die keinem besonderen Schutzbedarf unterliegen.

Hierunter fallen insbesondere populäre Internet-Dienste wie beispielsweise:

- Google Docs
- Dropbox
- Youtube
- Amazon Cloud (EC2)
- iCloud
- Public Mail Infrastrukturen (GMail, Yahoo, usw.)

Cloud-Services ohne individuellen Vertrag sind aus Sicht der Landesverwaltungen grundsätzlich der Kategorie 5 zuzurechnen.

[3] *Eine Differenzierung nach „deutsch“ und „europäisch“ ist nicht sinnvoll, da hier die Standortfrage des Rechenzentrums nicht mehr die entscheidend ist. Wichtig ist hier der europäische Rechtsrahmen, der auch für Deutschland und demzufolge auch für deutsche Anbieter gilt.*

Im Rahmen einer allgemeinen Ausschreibung sollte davon abgesehen werden diese Dienste für die öffentliche Verwaltung zu berücksichtigen. Entsprechend werden sie im Folgenden nicht weiter betrachtet.

3.6 Hybrid Clouds

Hybrid Clouds sind im Wesentlichen Private Clouds in einem der vorgenannten Modelle, die Belastungsspitzen in einer Public Cloud auffangen. Üblicherweise handelt es sich bei den in die Public Cloud ausgelagerten Diensten um Basisdienste (Speicher, Netzkapazität, Prozessorkapazität) und sind nur mittelbar mit dem beauftragten Service verbunden.

Die Art der verwendeten Public Cloud (gemäß Abschnitt 3.4 oder 3.5) kann ggf. festgestellt werden. Die reine Existenz dieser Fail-Over-Strategie mag aber für den beauftragten Service ein nicht akzeptables Risiko darstellen und muss entsprechend genau geprüft werden.

Im besten Fall entspricht die Hybrid Cloud dem Sicherheitsstandard einer Private Cloud der Kategorie 3, im Normalfall sind die durch den Public-Teil eingeführten Risiken so groß, dass das ganze Modell unter der Rubrik „Sonstige Public–Clouds“ der Kategorie 5 eingestuft werden muss.

4 ENTSCHEIDUNGSFINDUNG – VORBEREITUNG DER AUSSCHREIBUNG

4.1 Sicherheitseinstufung des auszuschreibenden Verfahrens

Wie in den Betrachtungen in Abschnitt 2 „Herausforderungen und Risiken“ dargestellt, geht der Entscheidung für ein geeignetes Cloud-Modell immer eine Schutzbedarfsfeststellung für das in der Cloud zu betreibende Verfahren bzw. die dabei zu verarbeitenden Daten voraus.

4.2 Compliance-Anforderungen

Zusätzlich zu der Schutzbedarfsfeststellung müssen folgende für die öffentliche Verwaltung relevanten Punkte geprüft werden:

- **Erfordert das Verfahren einen Betrieb in hoheitlicher Hand?**
  Bestimmte Anforderungen an Verfahren können es nötig machen, dass hoheitliches Handeln durch Amtsträger im Rahmen ihrer Amtspflicht ausgeführt wird. Dazu muss sich das verarbeitende Rechenzentrum gegebenenfalls im direkten Einflussbereich des bestellenden Ministeriums befinden, damit die betreffenden Daten auch tatsächlich physisch hier vorliegen.
- **Sind bei dem Verfahren Berufs- oder besonderen Amtsgeheimnisse betroffen?**
  Die Kritikalität der Daten solcher Verfahren sowie besondere Vorschriften können ein kommerzielles Betreibermodell (Kategorien 3-5) ausschließen.

4.3 Anforderungen an den Betreiber (Cloud-Service-Provider - CSP)

Im Sinne der Lieferantenstrategie der ausschreibenden Verwaltungsorganisation müssen die Kriterien an den Cloud-Service-Provider, den eigentlichen Vertragspartner, festgestellt werden.

Hier sind insbesondere Anforderungen zu folgenden Punkten zu definieren, um sie vertraglich zu vereinbaren:

- Haftung: Welche Mindesthaftung muss der CSP wahrnehmen können?
- Ausfallsicherheit: Welche Zusagen muss der CSP zu seiner Business-Continuity-Strategie treffen?
- Versicherung: Wie gut muss der CSP gegen eigene Krisen (z. B. Zahlungsunfähigkeit) abgesichert sein?

Im Weiteren wird auf die Kapitel 5 „Kriterien für eine Ausschreibung“ verwiesen.

4.4 Exit-Strategie und Datenmigration

Jeder Vertrag endet. Sei es, um den Anbieter zu wechseln, das Verfahren zu beenden oder bei Insolvenz des CSP die Daten zurückzuführen.

Es muss sichergestellt werden, dass

- im Rahmen einer Datenmigration die Daten entsprechend ihres Schutzbedarfs abgesichert sind.
- Verfahren etabliert sind, die hinreichend ausschließen, dass die Daten rekonstruiert werden können.
- das Verfahren möglichst ohne Störung des Geschäftsbetriebs überführt werden kann.

Eine maximale Interoperabilität und Portabilität von Daten und Diensten kann nur erreicht werden, wenn standardisierte Techniken zum Einsatz kommen:

- Software
- Programmiersprachen
- Datenbanken
- Schnittstellen
- Protokolle

Auf diese Weise ist der Auftraggeber möglichst unabhängig von einem einzelnen CSP und kann relativ kurzfristig die Daten und Dienste zu einem anderen Anbieter bzw. in das eigene Rechenzentrum transferieren.

5 KRITERIEN FÜR EINE AUSSCHREIBUNG

Der Bereitstellung von Cloud-Ressourcen durch den CSP im Rahmen des Outsourcings muss eine Sicherheitsarchitektur zugrunde liegen, die die Vertraulichkeit, Integrität und Verfügbarkeit der dort gespeicherten Informationen sicherstellt. In diesem Zusammenhang sind ebenso die korrespondierenden Grundwerte des Datenschutzrechts zu gewährleisten. Es sollte ein IT-Sicherheitsmanagement beim Auftragnehmer vorliegen, das auf der Grundlage ISO 27001 betrieben wird. Falls hoheitliche Aufgaben zu erledigen sind, wäre es zudem angebracht, dass das IT-Sicherheitsmanagementsystem auf den IT-Grundschutzstandards des Bundesamtes für Sicherheit in der Informationstechnik basiert, um den besonderen Complianceanforderungen des öffentlichen Dienstes in Deutschland besser gerecht werden zu können.

Das Rechenzentrum des CSP, in dem die Daten des Auftraggebers gespeichert und verarbeitet werden sollen, muss so konzipiert sein und betrieben werden, dass die Grundwerte der IT-Sicherheit (Vertraulichkeit, Integrität und Verfügbarkeit) gewährleistet sind. Dabei sind u. a. folgende Punkte zu beachten:

- Zutrittskontrolle
- Klimatisierung
- Schutz vor Feuer, Wasser, Gas
- Unterbrechungsfreie Stromversorgung

Beabsichtigt der Auftraggeber die Zertifizierung des Betriebs der Cloud-Service-Leistung in Kategorie 2-4 nach ISO 27001 auf der Basis von IT-Grundschutz, hat der Auftragnehmer seine Bereitschaft zur Mitarbeit und Zulieferung im Rahmen der Erstellung der entsprechenden Dokumente für den BSI-Baustein B1.11 Outsourcing der IT-Grundschutzkataloge in der jeweils gültigen Fassung zu erklären. Der Auftragnehmer hat weiterhin die Bereitschaft zur aktiven Unterstützung von Vor-Ort-Audits durch vom BSI bestellte Grundschutz-Auditoren im Rahmen von Zertifizierungen, Überwachungsaudits und Rezertifizierungen zu erklären.

Die in der Anlage aufgeführten Kriterien basieren im Wesentlichen auf dem Eckpunktepapier „Sicherheitsempfehlungen für Cloud Computing Anbieter“ des BSI und dem „Audit-Prüfkriterienkatalog für Cloud-Infrastrukturen - Security Audit as a Service (SAaaS)“ von Frank Dölitzscher et al. (2012), Hochschule Furtwangen. Die Kriterien beziehen sich auf alle Kommunikationsbeziehungen, die beim Übertragen von Daten in die Cloud des CSP und auch bei der Verteilung von Informationen innerhalb der Cloud des CSP entstehen. Von besonderem Interesse für das IT-Sicherheitsmanagement des Auftraggebers sind die Absicherungsmaßnahmen der bereitgestellten Cloud-Infrastruktur beim CSP gegenüber den anderen Kunden des CSP und gegen Angriffe aus dem Internet. Hier müssen vom CSP die technischen, vertraglichen, organisatorischen und infrastrukturellen Absicherungsmaßnahmen im Detail beschrieben werden. Außerdem muss offengelegt werden, welche Maßnahmen zu Datensicherung und Datenwiederherstellung getroffen wurden, wie die Systeme auf Seiten des CSP gehärtet werden, wie das Benutzermanagement in der Cloud geregelt ist und welche Security-Produkte zur weiteren Absicherung verwendet werden. Es muss sichergestellt sein, dass Ansprechpartner des CSP für IT-Sicherheit und Datenschutz vom Auftraggeber direkt kontaktiert werden können, falls es zu einem IT-Sicherheitsvorfall kommt.

Bei der Behandlung von Sicherheitsvorfällen im Zusammenhang mit der Nutzung von Cloud-Diensten, sind die jeweiligen CERTs (Computer Emergency Response Team) der Länder unmittelbar einzubeziehen. Soweit nicht bereits Meldepflichten bei Sicherheitsvorfällen bestehen, wird empfohlen die Zusammenarbeit mit dem Landes-CERT aufzunehmen. Dies wird um so dringlicher, da bspw. beim Betriebsmodell „Private Government Cloud“ sofort Behörden mehrerer Länder betroffen sein können und somit eine übergreifende Behandlung solcher Vorfälle notwendig wird. Sicherheitswarnungen, die dem CSP bezüglich der verwendeten Cloud-

Komponenten und Hilfsprodukte bekannt werden, sind dem CERT des Landes unverzüglich weiterzuleiten.

Die Basisanforderungen, die an jeden CSP gestellt werden, sind in der als Anlage beigefügten Tabelle in der gleichnamigen Spalte gekennzeichnet. Die jeweils durch die Kategorie 1 oder 2 zusätzlich zu erfüllenden Anforderungen sind ebenfalls herausgestellt. Durch den Auftraggeber der Cloud-Service-Leistung können die jeweils näher erläuterten (Ausschreibungs-)Kriterien herangezogen werden, um bspw. auf Basis des jeweiligen Schutzbedarfs die Anforderungen darzustellen und im Ausschreibungsverfahren abzufordern. Dabei sind die übergreifende Sicherheitsaspekte, die fachlichen und betrieblichen Anforderungen sowie die Datenschutzanforderungen in separaten Abschnitten dargestellt.

Zur Thematik Ausschreibungen, Vergabe und Migration von Cloud-Services ist vom Kompetenzzentrum Öffentliche IT am Fraunhofer-Institut FOKUS in Berlin die Informationsschrift „Cloud-Fahrplan für die öffentliche Verwaltung“ erstellt worden. Hier wird konkret u.a. auf die Aspekte der Wahl eines Ausschreibungsverfahrens sowie der Auftragsvergabe eingegangen. Deshalb erfolgen unter Bezugnahme auf dieses Dokument an dieser Stelle keine weiteren Ausführungen zum Thema.

6 AUSWIRKUNGEN DES SCHUTZBEDARFS AUF DIE WAHL DES CLOUD-BETRIEBSMODELLS

Anhand der Schutzbedarfsfeststellung, die für das in der Cloud zu betreibende Verfahren bzw. die damit zu verarbeitenden Daten im Vorfeld vorzunehmen ist, kann grundsätzlich entschieden werden, welches der zuvor erläuterten Betreibermodelle der Kategorien 1 bis 4 für den Verfahrensbetrieb in Frage kommt. Dabei stehen zunächst die Grundwerte Vertraulichkeit und Integrität im Vordergrund. Dies wird ergänzt durch die datenschutzrechtliche Perspektive hinsichtlich des informationellen Selbstbestimmungsrechts bei der Verarbeitung personenbezogener Daten.

Schutzbedarf zu quantifizieren ist problematisch. Selbst für solche Größen, für die konkrete Werte angegeben werden können, sind diese im Kontext der jeweiligen Organisation individuell festzulegen. Im Weiteren werden deshalb hier die vom BSI geprägten qualitativen Aussagen verwendet, mit denen der Schutzbedarf in drei Kategorien unterteilt wird:

Normal

- Schäden können zu deutlichen finanziellen Verlusten führen, bleiben aber insgesamt tolerabel.
- Die internen Ansehens- oder Vertrauensverluste können erheblich sein. Die Rufschädigung in der Öffentlichkeit bleibt gering.
- Verstöße gegen Gesetze, Vorschriften oder Verträge ziehen keine oder nur geringfügige, insgesamt tolerable Konsequenzen nach sich.

Hoch

- Im Schadensfall tritt Handlungsunfähigkeit zentraler Bereiche ein.
- Schäden bewirken beachtliche, jedoch nicht „Existenz bedrohende“ finanzielle Verluste für die Behörde selbst, ihre Vertragspartner oder die Bürger.
- Es ist mit einer erheblichen, ggf. nachhaltigen Rufschädigung in der Öffentlichkeit zu rechnen, die zu personellen Konsequenzen für die Verantwortungsträger führt.
- Verstöße gegen Gesetze, Vorschriften oder Verträge ziehen erhebliche Konsequenzen nach sich.

Sehr hoch

- Ein Schadensfall kann zur vollständigen Handlungsunfähigkeit der Behörde führen.
- Schäden bewirken extreme finanzielle Verluste für die Behörde selbst bzw. ihre Vertragspartner oder die Bürger
- Ruf, Vertrauen und Ansehen der Behörde oder gar der gesamten Landesverwaltung werden in der Öffentlichkeit landesweit extrem und nachhaltig geschädigt, so dass personelle Konsequenzen für die Behördenspitze und die Politik erfolgen müssen.
- Fundamentale Verstöße gegen Gesetze, Vorschriften oder Verträge haben ruinöse Folgen.

Zur grundsätzlichen Untersetzung werden typische Schadensszenarien verwendet, anhand derer die zu erwartenden Schäden sowie deren Folgen beim Verlust der Grundwerte bestimmt werden können. Analog dazu wird über das Schadensszenario „Verletzung des informationellen Selbstbestimmungsrechts“ die Abbildung in den einzelnen Schutzbedarfskategorien ermöglicht.

Da die Schadensszenarien kaum singulär auftreten, werden die dabei möglichen Auswirkungen hier zusammenfassend charakterisiert. Durch die nachfolgende qualitative Beschreibung wird somit eine Abgrenzung der Schutzbedarfskategorien untereinander deutlich, die allerdings letztlich durch Maßgaben des Dateneigentümers im Einzelnen präzisiert werden muss.

Normal

- Vertraulichkeit
  - Die Informationen sind zum hausinternen Gebrauch vorgesehen. Der Zugriff durch Unbefugte ist nachteilig für die Interessen der Behörde, Folgeschäden sind aber tragbar.
  - Anhand der offenbarten Informationen können die Behörde bzw. ihre Vertragspartner nicht wesentlich finanziell geschädigt werden.
- Integrität
  - Eine Manipulation, Verfälschung, Sinnänderung oder der Verlust von Informationen ist ohne oder aber mit tragbaren Folgeschäden verknüpft.
  - Die Nachweisbarkeit von Transaktionen ist zum Zwecke der Prozesskontrolle erforderlich, um eine ordnungsgemäße Abwicklung zu gewährleisten.
  - Transaktionsfehler führen zu tragbaren Folgeschäden.
- Verarbeitung personenbezogener Daten
  - Der Missbrauch personenbezogener Daten kann den Betroffenen maximal in seiner gesellschaftlichen Stellung (Ansehen) oder den wirtschaftlichen Verhältnissen beeinträchtigen, z. B. Einkommen, Grundsteuer, verwandtschaftliche Beziehungen, Verkehrs-Ordnungswidrigkeiten, Kreditauskünfte, Geschäftsbeziehungen, Kontenstände, Personalverwaltungsdaten (außer Beurteilungen).

Hoch

- Vertraulichkeit
  - Der Zugriff durch Unbefugte ist schädlich für die Interessen der Behörde. Folgeschäden sind erheblich.

- Anhand der offenbarten Informationen können die Behörde oder die Landesverwaltung bzw. Vertragspartner finanziell in erheblichem Umfang geschädigt werden.

- Integrität
  - Eine Manipulation, Verfälschung, Sinnänderung oder der Verlust von Informationen sind mit erheblichen Folgeschäden verbunden.
  - Es ist gesetzlich oder vertraglich eine Aufbewahrungs- bzw. Nachweispflicht definiert.
  - Ein Abstreiten von Transaktionen durch den Transaktionspartner bzw. eine fehlerhafte Authentisierung führen zu erheblichen Folgeschäden.
- Verarbeitung personenbezogener Daten
  - Im Falle des Missbrauchs des informationellen Selbstbestimmungsrechts sind erhebliche (schlimmstenfalls existenzbedrohliche) Auswirkungen für den Betroffenen nicht auszuschließen
  - Es sind personenbezogene Daten betroffen, die unter erhöhten gesetzlichen Schutz fallen (§ 3 Abs. 9 BDSG, Krankenhausgesetze, Amts- und Berufsgeheimnisse etc.) Dazu gehören z.B. dienstliche Beurteilungen, Patientendiagnosedaten, Straffälligkeit, Anstaltsunterbringung, schwerwiegende Ordnungswidrigkeiten, psychologisch-medizinische Untersuchungsergebnisse, der Finanzverwaltung offenbarte Steuerdaten, Schulden, Pfändungen, Konkurse, Mitgliederverzeichnisse von Parteien, Gewerkschaften oder Religionsgemeinschaften, weitere Daten, die dem Sozialgeheimnis § 35 SGB1 unterliegen wie Sozialleistungen oder Grad der Behinderung, Verkehrs-Ordnungswidrigkeiten, Kreditauskünfte, Geschäftsbeziehungen, Telefonverbindungsdaten, Kontenstände

Sehr hoch

- Vertraulichkeit
  - Der Zugriff durch Unbefugte schädigt die Behörde und das Handeln der gesamten Landesverwaltung nachhaltig. Folgeschäden sind untragbar.
  - Durch Datenpreisgabe werden die Landesverwaltung bzw. Vertragspartner der Behörde finanziell in Existenz gefährdendem Umfang geschädigt.
- Integrität
  - Eine Manipulation, Verfälschung, Sinnänderung oder der Verlust von Informationen ist mit fatalen Folgeschäden verbunden.
  - Es handelt sich um Transaktionen, die gemäß einschlägiger Gesetze der Schriftform oder einer notariellen Beglaubigung bedürfen.
  - Ein Abstreiten von Transaktionen durch den Transaktionspartner bzw. eine fehlerhafte Authentisierung führen zu untragbaren Folgeschäden.
- Verarbeitung personenbezogener Daten
  - Personenbezogene Daten, deren unberechtigte Kenntnisnahme die Persönlichkeitsrechte der Betroffenen in hohem (bis hin zu Existenz gefährdendem) Maße einschränken; dies kann bis zur gravierenden Gefährdung der körperlichen Unversehrtheit und der akuten Gefahr für Leib und Leben gehen. Hoher Schutzbedarf kann sich aus der möglichen Zahl der Betroffenen und/oder der Höhe des für den Einzelnen damit verbundenen Missbrauchsrisikos ergeben (DIN 31000)

Der hinsichtlich der Verfügbarkeit erforderliche Schutzbedarf hat sekundär auf die Auswahl des Cloud-Betreibermodells Einfluss. Da der Cloud-Nutzer bzw. Auftraggeber sich in Fragen der Verfügbarkeit jedoch in eine starke Abhängigkeit vom CSP begibt, sind diese Aspekte sehr kritisch zu behandeln. Die dazu ermittelten Anforderungen, wie die maximal erlaubte Ausfallzeit, sind jeweils durch entsprechende Service-Level-Agreements (SLA) in den vertraglichen Vereinbarungen abzusichern. Dazu muss der CSP adäquate technische und organisatorische Voraussetzungen gewährleisten.

Das BSI stellt mit dem HV-Kompendium[4] Instrumente zur Verfügung, die bei der Ermittlung der Qualitätsanforderungen angesetzt werden können und aus denen Kriterien für einen anforderungskonformen SLA abgeleitet und gegenüber gestellt werden sollten.

Fazit:

Somit ergibt sich unter Zugrundelegung der vorstehenden Ausführungen zu den Cloud-Betreibermodellen durch die Berücksichtigung der zutreffenden Schutzbedarfskategorien folgende grundsätzliche Zuordnung:

Schutzbedarf	**Kategorie 1**: Private Cloud	**Kategorie 2**: National/European Private Government Cloud	**Kategorie 3**: Managed Cloud (deutsches Recht)	**Kategorie 4**: Public Cloud (europäisches Recht)
normal	X	X	X	X*)
hoch	X	X		
sehr hoch	X			

*) *Anmerkung: Die Verarbeitung von Daten mit normalem Schutzbedarf in einer Public Cloud (Kategorie 4) ist besonders kritisch zu prüfen und kann nicht generell vorgesehen werden. Eine Verarbeitung ist nur dann akzeptabel, wenn es sich um Daten ohne Vertraulichkeitsanforderungen handelt.*

Allerdings bleibt für eine endgültige Entscheidung zu berücksichtigen, dass weitere Randbedingungen, wie beispielsweise die in Kapitel 4.2 dargestellten besonderen Kriterien, in die Überlegungen einzubeziehen sind. Dies obliegt der Verantwortung des Dateneigentümers.

[4] *https://www.bsi.bund.de/DE/Themen/weitereThemen/Hochverfuegbarkeit/HVKompendium/hvkompendium_node.html*

Dieses Dokument entstand mit freundlicher Unterstützung des

Arbeitskreises "Technische und organisatorische Datenschutzfragen" (AK Technik) der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

sowie dem

Bundesamt für Sicherheit in der Informationstechnik (BSI)