Annika Selzer

Die Kontrollpflicht nach § 11 Abs. 2 Satz 4 BDSG im Zeitalter des Cloud Computing

Alternativen zur Vor-Ort-Kontrolle des Auftragnehmers durch den Auftraggeber

Nutzt ein Unternehmen etwa für die Verwaltung von Kunden- bzw. Mitarbeiterdaten einen Cloud Computing Service, so handelt es sich in der Regel um eine Auftragsdatenverarbeitung nach § 11 BDSG. Das Unternehmen ist als Auftraggeber dazu verpflichtet den Auftragnehmer vor Beginn der Datenverarbeitung und sodann regelmäßig im Hinblick auf die Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu kontrollieren und das Ergebnis zu dokumentieren. Eine Vor-Ort-Kontrolle scheint im Zeitalter des Cloud Computing nicht realistisch umsetzbar. Dieser Aufsatz beschäftigt sich daher mit Alternativen zur Vor-Ort-Kontrolle.[1]

1 Problemstellung

§ 11 BDSG regelt die Auftragsdatenverarbeitung. Eine Auftragsdatenverarbeitung liegt dann vor, wenn der Auftragnehmer personenbezogene Daten im Auftrag des Auftraggebers erhebt, verarbeitet oder nutzt und der Auftraggeber die vollen Weisungsbefugnisse bezüglich dieser Vorgänge besitzt.[2] Hierfür muss kein Erlaubnistatbestand für eine Übermittlung vorliegen[3] und der Auftraggeber bleibt verantwortlich für die personenbezogenen Daten.[4]

1.1 Kontrollpflichten des Auftraggebers

§ 11 Abs. 2 BDSG regelt, dass der Auftragnehmer unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen ist. § 11 Abs. 2 Satz 4 BDSG regelt, dass der Auftraggeber sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen hat und das Ergebnis zu dokumentieren ist.

1.2 „Prüftourismus"

Ob der Auftraggeber dieser Kontrollpflicht persönlich und vor Ort nachkommen muss, ist umstritten.[5] Geht man von der Notwendigkeit einer persönlichen Vor-Ort-Kontrolle des Auftragnehmers durch den Auftraggeber aus, so ist fraglich, ob und wie sich diese Kontrolle im Zeitalter des Cloud Computing[6] sinnvoll

1 Es handelt sich um einen Beitrag, der im Rahmen des Projekts CloudCycle entstanden ist. CloudCycle wird vom BMWi auf Grund eines Beschlusses des deutschen Bundestages im Förderschwerpunkt Trusted Cloud gefördert.

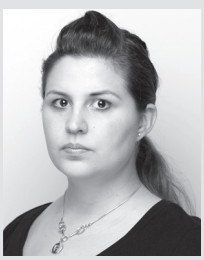
2 Vgl. § 11 Abs. 1 Satz 1 (1. Teilsatz), Abs. 3 BDSG; *Peter Gola / Rudolf Schomerus*, BDSG Kommentar, 11. Auflage, München 2012, § 11 Rdnr. 1 f. Im Gegensatz dazu liegt eine Funktionsübertragung vor, wenn der Dienstleister über eigene Entscheidungsbefugnisse verfügt.

3 Dieses Privileg beschränkt sich auf Auftragnehmer innerhalb des Europäischen Wirtschaftsraumes. Vgl. § 3 Abs. 8 Satz 3, Abs. 4 Satz 2 Nr. 3 BDSG.

4 Vgl. § 11 Abs. 1 Satz 1 (2. Teilsatz) und 2 BDSG;

5 Vgl. *Georg Borges et al.*, Datenschutzrechtliche Lösungen für Cloud Computing, S. 7, über: http://www.trustedcloud.de/documents/Thesenpapier_Datenschutz.pdf, besucht am 15.1.2013; *Eurocloud Deutschland_eco e.V.*, Leitfaden Cloud Computing und Compliance, S. 15, über: http://www.eurocloud.de/2010/12/02/eurocloud-lei tfaden-recht-datenschutz-compliance/, besucht am 15.1.2013; *Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder*, Orientierungshilfe Cloud Computing, S. 9, über: http://www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf, besucht am 15.1.2013; *Thilo Weichert*, Cloud Computing und Datenschutz, über: https://www.datenschutz zentrum.de/cloud-computing/20100617-cloud-com puting-und-datenschutz.html, besucht am 15.1.2013.

6 Cloud Computing stellt die Möglichkeit dar, verschiedene IT- Ressourcen (z.B. Rechenressourcen, Speicherkapazitäten und Datenbestände) miteinander zu ver-



Annika Selzer

Wissenschaftliche Mitarbeiterin am Fraunhofer-Institut für sichere Informationstechnologie.

E-Mail: annika.selzer@sit.fraunhofer.de

umsetzen lässt. Problematisch ist hierbei primär, dass der Cloud Nutzer („Auftraggeber der Auftragsdatenverarbeitung") in der Regel eine Vielzahl verschiedener Datenverarbeitungsdienste in Anspruch nehmen und immer wieder flexibel an seine Bedürfnisse anpassen will, ohne sich dabei in der Anzahl von Cloud Betreibern („Auftragnehmer der Auftragsdatenverarbeitung") oder bezüglich der geographischen Distanz zwischen Cloud Nutzer und Cloud Betreiber festlegen zu müssen. Muss der Cloud Nutzer jedoch eine persönliche Vor-Ort-Kontrolle vornehmen, so müsste er sich entweder sehr stark in seiner Auswahl an Cloud Betreibern (hinsichtlich Anzahl und geographischer Distanz zwischen dem Sitz des Cloud Nutzers und Cloud Betreiber) einschränken oder aber in Kauf nehmen, dass die Vor-Ort-Kontrollen der entsprechenden Cloud Betreiber in einen regelrechten „Prüf-Tourismus"[7] ausarten könnten, der zudem gem. § 11 Abs. 2 Satz 4 BDSG regelmäßig zu bewältigen wäre. Eine wie oben stehend beschriebene Einschränkung bezüglich der Auswahl der Cloud Betreiber passt jedoch nur sehr eingeschränkt mit den Vorteilen des Cloud Computing, dass die Dienste jederzeit, flexibel, unkompliziert und kostensparend erbracht werden, zusammen. Demgegenüber ist zu bezweifeln, dass der Cloud Nutzer einen wie oben beschriebenen Prüf-Tourismus wirtschaftlich und tatsächlich handhaben kann.[8] Der Artikel beschäftigt sich daher mit möglichen Alternativen zur Vor-Ort-Kontrolle.

2 Kontrolle nach § 11 Abs. 2 Satz 4 BDSG

Der folgende Abschnitt gibt zunächst einen Überblick über die in § 11 Abs. 2 Satz 4 BDSG geregelte Kontrolle des Auftraggebers durch den Auftragnehmer.

2.1 Kontrollinhalte

Den inhaltlichen Schwerpunkt der Kontrolle bilden die in § 9 BDSG bzw. der zugehörigen Anlage beschriebenen zu treffenden technischen und organisatorischen Maßnahmen zum Schutz der durch den Auftragnehmer verarbeiteten personenbezogenen Daten.

Der Auftragnehmer hat entsprechend der Anlage zu § 9 BDSG Folgendes sicherzustellen:[9]

- Zutrittskontrolle: Unbefugten ist der körperliche Zutritt zu Datenverarbeitungsanlagen zu verwehren. U.a. können Berechtigungsausweise zur Erfüllung des Kriteriums beitragen.
- Zugangskontrolle: Verhinderung der unbefugten Nutzung von Datenverarbeitungsanlagen. U.a. können Verschlüsselungsverfahren zur Erfüllung des Kriteriums beitragen.
- Zugriffskontrolle: Es muss gewährleistet werden, dass die Berechtigten jeweils nur auf die ihrer jeweiligen Berechtigung unterliegenden Daten zugreifen können. U.a. kann ein Berechtigungskonzept zur Erfüllung des Kriteriums beitragen.
- Weitergabekontrolle: Es soll verhindert werden, dass Daten während der Weitergabe unbefugt gelesen, kopiert, verändert oder gelöscht werden können. U.a. können Verschlüsselungsverfahren zur Erfüllung des Kriteriums beitragen.
- Eingabekontrolle: Gewährleistung der nachträglichen Überprüfbarkeit, welche personenbezogenen Daten durch wen zu welcher Zeit in Datenverarbeitungssysteme eingegeben bzw. dort verändert, gelöscht oder entfernt worden sind. U.a. können manuell erzeugte oder automatisierte Erfassungsbelege zur Erfüllung des Kriteriums beitragen.
- Auftragskontrolle: Der Auftragnehmer hat zu gewährleisten, dass die im Auftrag zu verarbeitenden Daten nur entsprechend den Weisungen des Auftraggebers verarbeitet werden. U.a. können eindeutige vertragliche Abreden nebst Kontrollabreden zur Erfüllung des Kriteriums beitragen.
- Verfügbarkeitskontrolle: Es muss der Schutz vor zufälliger Zerstörung (Wasserschäden, Brand, Blitzschlag etc.) sichergestellt werden. U.a. können Brandschutztüren und Backup-Verfahren zur Erfüllung des Kriteriums beitragen.
- Kontrolle der getrennten Verarbeitung: Technische Sicherstellung der zweckbestimmten Verarbeitung. U.a. kann die Trennung über Zugriffsregelungen zur Erfüllung des Kriteriums beitragen.

Ziel der Kontrolle ist festzustellen, dass die vertraglich vereinbarten Maßnahmen[10] umgesetzt wurden und dass das entsprechende Sicherheitskonzept des Auftragnehmers dynamisch an die technischen Entwicklungen angepasst wird.

2.2 Prüfturnus und Kontrolldokumentation

Der Auftraggeber hat sich gem. § 11 Abs. 2 Satz 4 BDSG bereits vor Beginn der Datenverarbeitung von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. „Im Interesse beider Parteien kann dies nach dem Vertragsschluss – also der finalen Auswahl – erfolgen, solange sich der Nutzer vor Beginn der tatsächlichen Datenverarbeitung die Überzeugung verschafft hat. In der praktischen Konsequenz bedeutet das, dass die erforderlichen Maßnahmen selbstverständlich bei Vertragsschluss geklärt worden sein müssen."[11]

Gem. § 11 Abs. 2 Satz 4 BDSG hat sich der Auftragnehmer regelmäßig von der Einhaltung der technischen und organisatorischen Maßnahmen zu überzeugen. Wie oft die Kontrolle stattfinden muss, richtet sich vor allem nach dem Schutzbedarf der personenbezogenen Daten. In der Regel wird jedoch ein jährlicher bis zweijährlicher Prüfturnus angemessen sein.

Der Auftraggeber ist gem. § 11 Abs. 2 Satz 5 BDSG zudem zur Dokumentation der Kontrolle verpflichtet. Festzuhalten ist, die Vornahme und das Ergebnis der Kontrolle.[12]

2.3 Kontrollmöglichkeit

Der Auftraggeber sollte sich von dem Auftragnehmer die Möglichkeit der Kontrolle vertraglich zusichern lassen. Der Auftragnehmer sollte hierbei sowohl auf die Mitwirkung als auch auf wahrheitsgemäße und vollständige Aussagen verpflichtet werden. Zusätzlich sollte sich der Auftragnehmer das Recht einer Vor-Ort-Kontrolle vertraglich zusichern lassen.[13]

knüpfen, sie auf externen Rechnern zu betreiben und Cloud Nutzern flexibel zur Verfügung zu stellen.

7 *Borges et al.*, Datenschutzrechtliche Lösungen für Cloud Computing, S. 8.

8 *Borges et al.*, Datenschutzrechtliche Lösungen für Cloud Computing, S. 8.

9 Vgl. § 9 BDSG, Anlage zu § 9 sowie *Peter Münch*, Technisch-organisatorischer Datenschutz, Auflage 4, Heidelberg 2012, S. 323 ff.

10 Vertraglich ist ein konkretes, den tatsächlichen Gegebenheiten entsprechendes Sicherheitskonzept zu vereinbaren. „Abstrakte oder pauschale Beschreibungen genügen dieser Vorgabe nicht, sondern müssen so konkret sein, dass klar ist, welche Maßnahmen ergriffen sind." Vgl. *Eurocloud Deutschland_eco e.V.*, Leitfaden Cloud Computing, S. 14.

11 *Eurocloud Deutschland_eco e.V.*, Leitfaden Cloud Computing, S. 14.

12 *Eurocloud Deutschland_eco e.V.*, Leitfaden Cloud Computing, S. 15.

13 *Eurocloud Deutschland_eco e.V.*, Leitfaden Cloud Computing, S. 13.

Ist dem Auftragnehmer die Erteilung von Unteraufträgen gestattet, so muss der Auftragnehmer zusätzlich darauf verpflichtet werden, dem Auftraggeber sämtliche Unteraufträge anzuzeigen. Da der Auftraggeber auch bei eventuellen Unteraufträgen für die personenbezogenen Daten verantwortlich bleibt, sollte dem Auftraggeber zudem auch gegenüber sämtlichen Unterauftragnehmern das Recht zur Kontrolle eingeräumt werden.[14]

3 Derzeitige Umsetzung der Kontrolle

Derzeit wird die Kontrollpflicht des Auftragnehmers durch den Auftraggeber z.B. durch persönliche Vor-Ort-Kontrollen oder durch Bescheinigungen Dritter erbracht.[15]

3.1 Vor-Ort-Kontrolle

Bei der persönlichen Vor-Ort-Kontrolle begibt sich der Auftraggeber in das Rechenzentrum des Auftragnehmers, um vor Ort zu überprüfen, ob der Auftragnehmer ausreichende technische und organisatorische Maßnahmen ergriffen hat.

Durch eine persönliche Vor-Ort-Kontrolle kann der Auftraggeber unter anderem kontrollieren, ob die Zutrittskontrolle zum Rechenzentrum und den Serverräumen gewährleistet wird und ob die personenbezogenen Daten – zum Beispiel durch Backup-Verfahren und Brandschutzvorkehrungen – ausreichend vor zufälliger Zerstörung geschützt sind. Auch ein Gespräch mit den Verantwortlichen kann zusätzlich Transparenz und Vertrauen schaffen.

3.2 Vertrauen in die Selbstauskunft des Auftragnehmers

Die Selbstauskunft des Auftraggebers basiert häufig auf einem Fragenkatalog bzw. einer Checkliste, die der Auftraggeber erstellt und mit deren Hilfe er sich eine Übersicht über die vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen verschaffen möchte.[16] Dieser Fragenkatalog wird sodann von dem Auftragnehmer ausgefüllt, evtl. um zusätzliche Dokumente und Informationen ergänzt und im Anschluss von dem Auftraggeber auf Schlüssigkeit überprüft.

Im Rahmen der Prüfung des ausgefüllten Fragebogens kann der Auftraggeber unter anderem in Erfahrung bringen, ob das Gebäude durch Wachpersonal überwacht wird und ob zusätzlich eine Alarmanlage installiert ist, ob ausreichende Verschlüsselungsverfahren zum Einsatz kommen und welche Backup-Verfahren eingesetzt werden. Allerdings basiert das Konzept beinahe ausschließlich auf dem Vertrauen in die Aussage des Auftragnehmers und kommt demnach einer Selbstzertifizierung des Cloud Betreibers gleich. Es ist umstritten, ob eine reine Selbstauskunft des Auftragnehmers ausreicht, um den Kontrollpflichten nach § 11 Abs. 2 Satz 4 BDSG nachzukommen.[17] Daher wird zum Teil empfohlen, die Angaben des Auftraggebers zumindest stichprobenartig persönlich oder durch eine unabhängige Stelle zu überprüfen.[18]

3.3 Bescheinigungen Dritter

Des Weiteren kann sich ein Auftraggeber[19] oder ein Auftragnehmer von Dritten die Eignung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen in Form eines Testats/Zertifikats/Audits nachweisen lassen.[20]

Durch eine solche Bescheinigung können theoretisch Aussagen in der Qualität einer Vor-Ort-Kontrolle getroffen werden. Wie bereits bei der Selbstauskunft des Auftragnehmers ist es jedoch auch bei Bescheinigungen Dritter umstritten, ob das *alleinige* Vorliegen einer solchen Bescheinigung ausreichend im Sinne des § 11 Abs. 2 Satz 4 BDSG ist.[21] Schwierigkeiten bei der Beantwortung dieser Frage resultieren vor allem aus den unterschiedlichen Kriterien, die der Prüfung der technischen und organisatorischen

14 Für die Kontrolle des Unterauftragnehmers gilt: Nicht die tatsächliche Weitergabe personenbezogener Daten an den Unterauftragnehmer indiziert eine Kontrolle – Unterauftragnehmer sind vielmehr bereits dann zu kontrollieren, wenn nicht auszuschließen ist, dass der Unterauftragnehmer Zugriff auf Daten haben könnte. Dies deckt sich mit dem Zweck des § 11 Abs. 2 Satz 4 1. Halbsatz BDSG. Vgl. auch *Eurocloud Deutschland_eco e.V.*, Leitfaden Cloud Computing, S. 15 f.; *Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder,* Orientierungshilfe Cloud Computing, S. 9.

15 http://www.datenschutzbeauftragter-info.de/ auftragsdatenverarbeitung-warum-dienstleisterko ntrollen/, besucht am 16.1.2013.

16 Vgl. auch http://www.datenschutz beauftragter-info.de/auftragsdatenverarbeitung-warum-dienstleisterkontrollen/, besucht am 16.1.2013.

17 *Weichert,* Cloud Computing und Datenschutz; *Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder,* Orientierungshilfe Cloud Computing, S. 9; *Borges et al.,* Datenschutzrechtliche Lösungen für Cloud Computing, S. 12.

18 *Weichert,* Cloud Computing und Datenschutz; *Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder,* Orientierungshilfe Cloud Computing, S. 9.

19 Die Überprüfung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen durch Dritte kann auch direkt vom Auftragnehmer erbeten werden.

20 http://www.datenschutzbeauftragter-info.de/ auftragsdatenverarbeitung-warum-dienstleisterko ntrollen/, besucht am 16.1.2013.

21 *Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder,* Orientierungshilfe Cloud Computing, S. 9; *Weichert,* Cloud Computing und Datenschutz.

Maßnahmen zu Grunde gelegt werden und die als Anforderungen an die prüfende Stelle gestellt werden.

Eine gleichwertig hohe Qualität ist auf dieser Grundlage nicht sichergestellt. Auch hier bedarf es nach aktuellem Stand daher einer eigenen Recherche und/oder Kontrolle des Auftraggebers.[22]

4 Neue Kontrollmodelle

Die AG Rechtsrahmen des Technologieprogramms „Trusted Cloud"[23] hat in einem rechtspolitischen Thesenpapier eine vereinheitlichte Testatlösung als Alternative zur persönlichen Vor-Ort-Kontrolle des Auftraggebers vorgeschlagen. Dieser Vorschlag soll im Folgenden vorgestellt und um weiterführende Überlegungen ergänzt werden.

4.1 Vereinheitlichtes Testat

Laut dem Thesenpapier der AG Rechtsrahmen kann „das wesentliche Problem des Kontrollerfordernisses […] gelöst werden, wenn die Kontrolle durch den Auftraggeber durch das von einem unabhängigen Dritten erstellte Testat ersetzt werden kann, das die Durchführung der Kontrolle im gesetzlich angeordneten Umfang bescheinigt."[24]

Ein Testat wäre dementsprechend ein Prüfbericht eines unabhängigen Dritten.

Die Prüfkriterien für die Erteilung eines Testats sollten laut der AG Rechtsrahmen auf gesetzlicher Grundlage für den europäischen Binnenmarkt einheitlich festgesetzt werden, wobei die Festlegung der Kriterien „durch ein Verfahren erfolgen [sollte], in dem Datenschutzbehörden sowie Vertreter von Anbietern und Nutzern der Auftragsdatenverarbeitung beteiligt werden. [Zudem sollen die Prüfkriterien] an die Veränderungen der Datenverarbeitung angepasst werden können, damit die Schutzziele bei Veränderung technischer oder organisatorischer Gegebenheiten erreicht werden können."[25]

Die Kontrolle könnte sowohl von dem Auftraggeber als auch von dem Auftragnehmer ausgelöst werden und sollte regelmäßig wiederholt werden.[26] Die Ersetzbarkeit der Kontrolle, die von dem Auftraggeber persönlich durchgeführt wird, durch ein Testat sollte laut der AG Rechtsrahmen aus Gründen der Rechtssicherheit gesetzlich festgeschrieben werden. Durch eine ausreichende Dokumentation der testierenden Stelle wäre der Auftraggeber zusätzlich im Stande, die Kontrolle gegenüber den Aufsichtsbehörden nachweisen zu können.

Als Anforderung an die testierende Stelle formuliert die AG Rechtsrahmen eine gesetzlich vorgeschriebene Akkreditierung, welche unter anderem die Unabhängigkeit und fachliche Eignung der testierenden Stelle bestätigen soll. Um die Qualität der Kontrolle zusätzlich zu verbessern, sollte für den Fall, dass die testierende Stelle ein fehlerhaftes Testat ausstellt, eine zivilrechtliche Haftung der testierenden Stelle vorgesehen werden.[27]

Durch die Umsetzung des Vorschlags der AG Rechtsrahmen könnten Testate in Zukunft demnach hinsichtlich der Prüfkriterien und Anforderungen an die testierende Stelle vereinheitlicht und rechtssicher werden. Das vereinheitlichte Testat könnte somit bewirken, dem Auftraggeber eine persönliche Vor-Ort-Kontrolle zu ersparen, ohne auf die Selbstauskunft des Auftragnehmers bzw. Testate unterschiedlicher Qualität zurückgreifen zu müssen, die derzeit für Rechtsunsicherheit sorgen.

4.2 Teilautomatisierte Testat-Lösung

Testate beziehen sich in der Regel auf eine Überprüfung bestimmter Abläufe/Produkte durch einen Dritten, in welcher die testierende Stelle den aktuellen Zustand eines Ablaufs/Produkts überprüft. Für die Überprüfung der Umsetzung technischer und organisatorischer Maßnahmen eines Cloud Betreibers kann es jedoch von großem Interesse und Nutzen sein, nicht nur den Ist-Zustand der Umsetzung, sondern auch die Umsetzung der technischen und organisatorischen Maßnahmen in der Vergangenheit bewerten zu können, um sicherzustellen, dass die technischen und organisatorischen Maßnahmen (zeitlich) lückenlos umgesetzt werden.[28] Hierfür könnte sich die zusätzliche Kontrolle von Log-Daten eignen. Die Log-Daten und sonstigen Dokumentationen zur Auftragsdatenverarbeitung befinden sich beim Cloud Betreiber und dessen eventuellen Unterauftragnehmern. „Während der Cloud [Nutzer] kaum über regelmäßige Reports, Informationen über Schwierigkeiten und wichtige Vorfälle sowie über System- und Nutzungsprotokolle verfügt,"[29] besteht beim Cloud Betreiber die Möglichkeit der Kontrolle dieser Informationen. Eine Selbstkontrolle der Log-Daten durch den Cloud Betreiber wirft jedoch die gleichen Fragen hinsichtlich des Vertrauens in die Aussage des Cloud Betreibers auf, wie die Möglichkeit, die Umsetzung technischer und organisatorischer Maßnahmen durch eine Selbstauskunft des Auftragnehmers zu kontrollieren.

Denkbar wäre daher, im ersten Schritt die Fälschungssicherheit[30] der Log-Daten so weit wie möglich sicherzustellen, die Log-Daten in einer zur Kontrolle der technischen und organisatorischen Maßnahmen geeigneten Form aufzubereiten und den Bericht, der auf fälschungssicheren Log-Daten beruht, durch eine akkreditierte Stelle („Auditor") gegenprüfen zu lassen.

Dieser Anteil des Testats könnte automatisiert erfolgen und der akkreditierten Stelle, welche den Ist-Zustand der Umsetzung der technischen und organisatorischen Maßnahmen händisch kontrolliert, eine Möglichkeit geben, die Umsetzung der technischen und organisatorischen Maßnahmen zusätzlich automatisiert für die Vergangenheit zu bewerten.

4.2.2 Automatisierter Anteil des Testats

Der automatisierte Anteil des Testats basiert auf Log-Daten,[31] die möglichst fälschungssicher sein müssen. Dies sollte durch ein

22 Dies kann sich z.B. auf die Kontrolle des Testat-Prüfberichts auf Vollständigkeit aber auch auf (von der testierenden Stelle unabhängige) stichprobenartige Überprüfung des Auftragnehmers beziehen.

23 Nähere Informationen unter www.trusted-cloud.de, besucht am 15.1.2013.

24 *Borges et al.,* Datenschutzrechtliche Lösungen für Cloud Computing, S. 11.

25 *Borges et al.,* Datenschutzrechtliche Lösungen für Cloud Computing, S. 15.

26 Wie in § 11 Abs. 2 Satz 4 BDSG vorgesehen.

27 *Borges et al.,* Datenschutzrechtliche Lösungen für Cloud Computing, S. 11-21.

28 Ähnlich weisen bereits *Borges et al.* auf diese Möglichkeit hin: „Auch Elemente wie laufende Berichte (Monitoring) ließen sich durch Testierung feststellen und wären Bestandteil des Testats, soweit eine entsprechende gesetzliche Verpflichtung besteht." *Borges et al.,* Datenschutzrechtliche Lösungen für Cloud Computing, S. 12.

29 *Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder,* Orientierungshilfe Cloud Computing, S. 14.

30 Inklusive der Sicherheit vor interner Manipulation durch den Auftragnehmer.

31 Für die Erstkontrolle eines Auftragnehmers können sich die Log-Daten z.B. auf einen Testzugang beziehen, der vom Auditor selbst und kundenunspezifisch überprüft wird.

detailliertes Secure Logging Framework sichergestellt werden, indem beispielsweise eine Verkettung von Hashwerten („Forward Integrity“: Ändern und Löschen von bestehenden Einträgen sind nicht unbemerkt möglich – selbst dann, wenn die Log-Daten an einem unsicheren Ort gespeichert würden), Verschlüsselung und digitale Signaturen zum Einsatz kommen könnten. Die fälschungssicheren Logfiles werden sodann mit Hilfe einer Log-Auswertungskomponente servicespezifisch ausgewertet. Die Auswertung sollte erlauben, eine Aussage zu treffen, ob ein bestimmtes Kriterium erfüllt oder nicht erfüllt ist. Kriterien könnten etwa sein, dass die personenbezogenen Daten nicht den Europäischen Wirtschaftsraum verlassen haben, ein dem Stand der Technik entsprechendes Verschlüsselungsverfahren eingesetzt wurde und dass der Zugriff nur mit Benutzerkennung und Passwort möglich war.[32]

Die automatische Auswertung wird sodann durch einen Auditor auf Schlüssigkeit und Korrektheit überprüft. An den Auditor sind die von der AG Rechtsrahmen genannten Kriterien zu stellen.

Ein Testat sollte immer für einen spezifischen Cloud Computing Service ausgestellt werden. Das Testat könnte sowohl kundenspezifisch als auch kundenunspezifisch ausgestellt werden. Dementsprechend könnte es entweder bestätigen, dass für einen bestimmten Auftraggeber, der einen spezifischen Cloud Computing Service nutzt, rechtliche Anforderungen erfüllt wurden oder aber bestätigen, dass für einen bestimmten Cloud Computing Service – unabhängig zu einer bestimmten Auftragsdatenverarbeitung – datenschutzrechtliche Anforderungen erfüllt wurden.

Das Testat sollte mindestens folgende Elemente enthalten:

- Benennung des Auftraggebers (falls das Testat kundenspezifisch ausgestellt wird)
- Benennung des Auftragnehmers
- Benennung des spezifischen Cloud Computing Services
- Zeitraum der Entstehung und Auswertung der Log-Daten
- Prüfgegenstand
- Prüfergebnis
- Zeitpunkt der Ausstellung des Testats

Prüfgegenstand sollten alle technischen und organisatorischen Maßnahmen sein, die sich – ganz oder teilweise – an Hand von Log-Daten überprüfen lassen. Unter anderem können Log-Daten über Verschlüsselung, Zugriffe Dritter und Weitergabevorgänge der Kontrolle des Auftragnehmers dienen. Zudem können – als Grundvoraussetzung für das Privileg[33] der Auftragsdatenverarbeitung – Log-Daten bezüglich des Speicherorts in die Kontrolle des Auftragnehmers einbezogen werden.

4.2.3 Händischer Anteil des Testats

Nachdem der Auditor die automatische Auswertung auf Schlüssigkeit und Korrektheit überprüft hat, könnte der Auditor optional händisch Einträge vornehmen und somit Erkenntnisse aus seinen eigenen, nicht automatisierten Kontrollen der technischen und organisatorischen Maßnahmen in einen weiteren Prüfbericht zusammenfassen.[34] Im nächsten Schritt kann er auf Grundlage aller Auswertungsergebnisse endgültig festlegen, ob die technischen und organisatorischen Maßnahmen ausreichend umgesetzt sind.

Im Anschluss signiert der Auditor die Auswertung der automatisierten Überprüfung (und seinen eigenen optionalen Prüfbericht) und bestätigt damit im Idealfall die ausreichende Umsetzung der technischen und organisatorischen Maßnahmen durch den Auftragnehmer. Gibt es Unterauftragnehmer, so sollte das Testat auch Aussagen zu den Unterauftragnehmern enthalten.

Das automatisierte Testat kann somit dazu beitragen, nicht nur den Ist-Zustand der Umsetzung technischer und organisatorischer Maßnahmen beim Auftragnehmer zu erfassen, sondern auch festzustellen, ob der Auftragnehmer die Maßnahmen in der Vergangenheit ordnungsgemäß umgesetzt hat und was mit den personenbezogenen Daten tatsächlich passiert ist.

Als Nachteil könnte empfunden werden, dass zur Erstellung eines automatisierten Testats wiederum Daten mit möglichem Personenbezug[35] gespeichert werden müssen – dementsprechend sollten die personenbeziehbaren Daten wann immer möglich pseudonymisiert werden. Zudem ist darauf zu achten, dass die Log-Daten nur so kurz wie möglich gespeichert werden.[36] Es erscheint daher sinnvoll, in regelmäßigen, zeitlich kurzen Abständen automatisierte Testate zu erzeugen, so dass die Log-Daten für die Auswertung nicht über längere Zeiträume gespeichert werden müssen. Dies resultiert zudem in den Vorteil, dass der Auftraggeber relativ kurzfristig davon erfährt, wenn die technischen und organisatorischen Maßnahmen durch den Auftragnehmer nicht ausreichend umgesetzt wurden und er schnell auf diesen Umstand reagieren kann.

5 Zusammenfassung

Im Zeitalter des Cloud Computing passt die persönliche Vor-Ort-Kontrolle eines Auftragsnehmers durch den Auftraggeber nicht mehr mit den technischen Gegebenheiten zusammen und würde einen regelrechten Prüf-Tourismus nach sich ziehen, den ein Cloud Nutzer (Auftraggeber der Auftragsdatenverarbeitung) realistischer Weise nicht erfüllen kann.

Die Testatlösung der AG Rechtsrahmen schafft hier eine logische Abhilfe. Durch Hinzufügen des automatisierten Anteils wird es zudem möglich, nicht nur jede 1-2 Jahre den Ist-Zustand der Umsetzung technischer und organisatorischer Maßnahmen beim Auftragnehmer zu kontrollieren, sondern zusätzlich zu kontrollieren, wie die Maßnahmen im laufenden Betrieb tatsächlich umgesetzt wurden. Durch die Erstellung von automatisierten Testaten kann somit überprüft werden, ob der Auftragnehmer seiner Pflicht zur Umsetzung technischer und organisatorischer Maßnahmen gewissenhaft nachkommt. Fällt ein Testatbericht negativ aus, so kann der Auftraggeber schnell auf diese Situation reagieren, um seiner Letztverantwortung gegenüber den personenbezogenen Daten nachzukommen.

32 Analog zu dem Thesenpapier der AG Rechtsrahmen wäre es auch für den automatisierten Anteils eines Testats ideal, wenn die Prüfkriterien möglichst einheitlich wären.

33 Vgl. Abschnitt 1 „Problemstellung.“

34 Dieser Schritt müsste nicht für jedes automatisch erzeugte Testat durchgeführt werden. Denkbar wäre z.B., dass dieser Schritt – ähnlich wie im Prüfturnus der derzeitigen Kontrollen – alle 1-2 Jahre zusätzlich zu dem automatisierten Anteil hinzugefügt wird.

35 Log-Daten können nach herrschender Meinung Personenbezug besitzen.

36 Für weitere Anforderungen an datenschutzkonformes Logging vgl. Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Orientierungshilfe Protokollierung, über: http://www.bfdi.bund.de/SharedDocs/Publikationen/Orientierungshilfen/OHProtokollierung.pdf?__blob=publicationFile, besucht am 15.1.2013.