Geschäftsplan für ein DIN SPEC-Projekt nach dem PAS-Verfahren zum Thema **„AUDITOR – European Cloud Service Data Protection Certification“**

Status:
Zur Kommentierung durch die Öffentlichkeit (Veröffentlichung)

Anmeldungen zur Mitarbeit sowie Kommentare zum Geschäftsplan sind erbeten und **bis zum 12.02.2019** an samarkhel-khan.yahya@din.de zu übermitteln[1]

Die Empfänger dieses Geschäftsplans werden gebeten, mit ihren Kommentaren **jegliche relevanten Patentrechte**, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Berlin, 15.01.2019

[1] Anmeldungen zur Mitarbeit und Kommentare zum Geschäftsplan, die nach Ablauf der Frist eingehen, müssen nicht berücksichtigt werden. Über die Einarbeitung der fristgerecht eingegangenen Kommentare entscheidet der Workshop (Gremium) nach seiner Konstituierung.

Inhaltsverzeichnis

1. Status des Geschäftsplans

- Zur internen Kommentierung

- **Zur Kommentierung durch die Öffentlichkeit (Veröffentlichung)**

  Dieser Geschäftsplan dient zur Information der Öffentlichkeit über das geplante Projekt. Interessenten haben die Möglichkeit, sich an dem Projekt zu beteiligen und/oder den Geschäftsplan zu kommentieren. Hierfür ist eine entsprechende E-Mail an samarkhel-khan.yahya@din.de zu richten.

  Über die tatsächliche Durchführung des Projekts entscheidet der Vorsitzende des Vorstandes von DIN im Nachgang an die Veröffentlichung dieses Geschäftsplans.

  Kommt das Projekt zustande, werden alle Akteure, die sich fristgerecht zur Mitarbeit angemeldet oder den Geschäftsplan kommentiert haben, zum Kick-Off eingeladen.

- Zur Erarbeitung der DIN SPEC (PAS) nach Annahme am <2019-02-22>

  Änderungsvermerk zur Revision xx:
  - z.B. Abschnitt 2: Tabelle der teilnehmenden Organisationen
  - usw.

2. Initiator[2] und weitere Workshop-Mitglieder

- Initiator:

Person/Organisation	Kurzbeschreibung
Karlsruher Institut für Technologie	Das Karlsruher Institut für Technologie (KIT) ist die Forschungsuniversität in der Helmholtz-Gemeinschaft. Das KIT richtet seine großen Forschungsfelder an den langfristigen Herausforderungen der Gesellschaft aus, um nachhaltige Lösungen für drängende Zukunftsfragen zu entwickeln. Ziel ist es, in Forschung, Lehre und Innovation auf Spitzenniveau maßgeblich zum Gelingen großer Projekte unserer Gesellschaft, wie beispielsweise der

[2] Die in diesem Dokument gewählte männliche Form der geschlechtsbezogenen Begriffe wie z. B. „der Initiator“ gelten selbstverständlich auch für alle weiblichen Personen. Lediglich aufgrund der besseren Verständlichkeit des Textes wurde einheitlich die männliche Form gewählt.

	Energiewende, einer sicheren und nachhaltigen Mobilität oder intelligenter Technologien für die Informationsgesellschaft, beizutragen. Im Fokus stehen die Themen Energie, Mobilität und Information. Weitere thematische Schwerpunkte sind Klima und Umwelt, Materialien, Mensch und Technik sowie Elementarteilchen- und Astroteilchenphysik. Mit rund 9 200 Mitarbeiterinnen und Mitarbeitern, darunter fast 6 000 in Wissenschaft und Lehre, sowie 26 000 Studierenden ist das KIT eine der größten Forschungs- und Lehreinrichtungen Europas.

- Potenzielle zusätzliche Teilnehmer:

Die DIN SPEC wird durch ein Konsortium (temporäres Gremium) erarbeitet, der jedem Interessenten offensteht. Die Mitwirkung von weiteren Experten ist sinnvoll und wünschenswert. Es bietet sich an, dass sich beispielsweise

- Forschungseinrichtungen für Cloud Computing, Datenschutz und Informationssicherheit
- Cloud Dienst Anbieter
- Cloud Dienst Nutzer
- Cloud Dienst Berater
- Zertifizierungsstellen
- Prüfstellen und Auditoren
- Dienstleister im Bereich Datenschutz und Informationssicherheit
- Datenschutz Organisationen
- Aufsichtsbehörden
- Verbände der IT-Anwender
- Juristen mit Schwerpunkt Recht der Technik
- Deutsche Akkreditierungsstelle
- Landesbeauftragte für den Datenschutz
- Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
- usw.

an der Erarbeitung der DIN SPEC beteiligen.

- Organisationen[3], die sich zur Mitwirkung angemeldet haben:

[3] Organisationen sind teilnehmende juristische Personen, die die Experten in das DIN SPEC PAS-Konsortium entsenden und einer Unternehmensstruktur i.S.v. § 15 Aktiengesetz oder § 271 Absatz 2 Handelsgesetzbuch zuzurechnen sind.

Person	Organisation
Prof. Dr. Ali Sunyaev	Karlsruher Institut für Technologie
Sebastian Lins	Karlsruher Institut für Technologie
Heiner Teigeler	Karlsruher Institut für Technologie
Prof. Dr. Alexander Roßnagel	Fachgebiet Öffentliches Recht mit Schwerpunkt Recht der Technik und des Umweltschutzes, Universität Kassel
Dr. Natalie Maier	Fachgebiet Öffentliches Recht mit Schwerpunkt Recht der Technik und des Umweltschutzes, Universität Kassel
Dr. Detlef Hühnlein	ecsec GmbH
Andreas Weiss	EuroCloud Deutschland_eco e.V., eco – Verband der Internetwirtschaft
Thomas Niessen	Kompetenznetzwerk Trusted Cloud e.V.
Sebastian Kliem	VOICE – Bundesverband der IT-Anwender e.V.
Stefan Schumacher	VOICE – Bundesverband der IT-Anwender
Martin Uhlherr	DIN e.V.
Samarkhel-Khan Yahya	DIN e.V.

- Organisationen[3], die diesen Geschäftsplan angenommen haben (Konsortialmitglieder):

Person	Organisation
N.N.	N.N.
N.N.	N.N.
N.N.	N.N.

3. Ziele des Projekts

3.1. Allgemeines

Diese DIN-SPEC wird im Rahmen des Forschungsprojektes European Cloud Service Data Protection Certification (AUDITOR) entwickelt. Das vom Bundesministerium für Wirtschaft und Energie geförderte Projekt hat das Ziel eine Konzeptionierung, exemplarische Umsetzung und Erprobung einer nachhaltig anwendbaren EU-weiten Datenschutzzertifizierung von Cloud-Diensten umzusetzen. Die DIN-SPEC bildet die Anforderungen ab, die zur Zertifizierung von Cloud-Diensten nach EU-Datenschutzgrundverordnung (DSGVO) notwendig sind. Dieses Dokument ist somit ein Prüfstandard für die Datenschutz-Zertifizierung von Cloud-Diensten gemäß den Anforderungen der DSGVO.

Diese DIN-SPEC basiert auf einschlägigen Normen und umfasst Anforderungen an technische und organisatorische Maßnahmen zur Einhaltung der Anforderungen der DSGVO und weiterer einschlägiger Gesetze. Weitere Informationen können der im Anhang referenzierten ersten Entwurfsfassung des AUDITOR- Kriterienkataloges in der Version 0.8 entnommen werden, der die initiale Grundlage der DIN-SPEC bildet.

3.2. Geplanter Anwendungsbereich

Diese DIN-SPEC legt Anforderungen für Verarbeitungsvorgänge von personenbezogenen Daten in Cloud-Diensten zur Einhaltung der DSGVO fest. Diese DIN-SPEC dient als Grundlage zur Zertifizierung von Cloud-Diensten, um die Einhaltung der DSGVO durch eine akkreditierte Zertifizierungsstelle zu zertifizieren.

3.3. Verwandte Aktivitäten

Das Thema der geplanten DIN SPEC (PAS) ist bisher nicht Gegenstand einer Norm. Es existieren jedoch die folgenden, themenverwandten Gremien, Normen und/oder Regelwerke, die im Zuge des Projekts berücksichtigt und ggf. einbezogen werden:

- **Gremien:**
- NA 043-01-27 AA "IT-Sicherheitsverfahren"
- NA 043-01-27-05 AK "Identitätsmanagement und Datenschutz-Technologien"
- NA 043-01-38 AA "Verteilte Anwendungsplattformen und Dienste"
- CEN-CENELEC/TC 8 “Privacy management in products and services”
- ISO/IEC JTC 001/SC 27 "IT Security techniques"
- ISO/IEC JTC 001/SC 27/WG 05 "Identity management and privacy technologies"
- ISO/IEC JTC 001/SC 38 "Cloud Computing and Distributed Platforms"
- ISO/IEC JTC 001/SC 38/WG 03 "Cloud Computing Fundamentals (CCF)"
- ISO/PC 317 “Consumer protection: privacy by design for consumer goods and services”

- **Normen und Standards**:
- DIN 66398 *„Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten“*
- DIN EN ISO 9241-151 *„Ergonomics of human-system interaction - Part 151: Guidance on World Wide Web user interfaces (ISO 9241-151:2008); German version EN ISO 9241-151:2008“*
- DIN ISO/IEC 19086-1 *„Information technology - Cloud computing - Service level agreement (SLA) framework - Part 1: Overview and concepts (ISO/IEC 19086-1:2016); Text in German and English“*
- DIN ISO/IEC 27018 *„Informationstechnik - Sicherheitsverfahren - Leitfaden zum Schutz personenbezogener Daten (PII) in öffentlichen Cloud-Diensten als Auftragsdatenverarbeitung (ISO/IEC 27018:2014)“*
- ISO/IEC 17922 *„Informationstechnik - Sicherheitsverfahren - Rahmenwerk für telebiometrische Authentifizierung unter Nutzung biometrischer Hardware-Sicherheitsmodule“*
- ISO/IEC 19086-1 *„Information technology - Cloud computing - Service level agreement (SLA) framework - Part 1: Overview and concepts“*
- ISO/IEC DIS 19086-2 *„Information technology - Cloud computing - Service level agreement (SLA) framework - Part 2: Metric model“*
- ISO/IEC 19086-3 *„Information technology - Cloud computing - Service level agreement (SLA) framework - Part 3: Core conformance requirements“*

- ISO/IEC 24745 *„Informationstechnik - Sicherheitsverfahren - Schutz biometrischer Informationen “*
- ISO/IEC 24760-1 *„Informationstechnik - Sicherheitsverfahren - Rahmenwerk für Identitätsmanagement - Teil 1: Terminologie und Konzept“*
- ISO/IEC 24760-2 *„Informationstechnik - Sicherheitsverfahren - Ein Rahmenwerk für das Identitätsmanagement - Teil 2: Referenzarchitektur und Anforderungen“*
- ISO/IEC 24760-3 *„Informationstechnik - Sicherheitsverfahren - Rahmenwerk für Identitätsmanagement - Teil 3: Umsetzung“*
- ISO/IEC 24761 *„Informationstechnik - Sicherheitsverfahren - Authentifizierungskontext für Biometrie“*
- ISO/IEC 24761 Technical Corrigendum 1 *„Informationstechnik - Sicherheitsverfahren - Authentifizierungskontext für Biometrie; Korrektur 1“*
- ISO/IEC 27017 *„Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services“*
- ISO/IEC 27018 *„Informationstechnik - Sicherheitsverfahren - Anwendungsregel für den Schutz von Personenbezogenen Daten (PII) in Public Clouds, die als PII Processor auftreten“*
- ISO/IEC 29100 *„Informationstechnik - Sicherheitsverfahren - Rahmenwerk für Datenschutz“*
- ISO/IEC 29100 DAM 1 *„Information technology - Security techniques - Privacy framework - Amendment 1: Clarifications“*
- ISO/IEC 29101 *„Informationstechnik - Sicherheitsverfahren - Rahmenwerk für Datenschutzarchitektur“*
- ISO/IEC 29115 *„Informationstechnik - Sicherheitsverfahren - Rahmenwerk für Vertrauen in die Authentifizierung von Entitäten“*
- ISO/IEC 29115 DAM 1 *„Information technology - Security techniques - Entity authentication assurance framework; Amendment 1“*
- ISO/IEC 29134 *„Informationstechnik - Sicherheitsverfahren - Datenschutz-Folgenabschätzung - Leitfaden“*
- ISO/IEC 29146 *„Informationstechnik - Sicherheitsverfahren - Rahmenwerk für Zugangssteuerung“*
- ISO/IEC 29151 *„Informationstechnik - Sicherheitsverfahren - Leitfaden für den Schutz personenbezogener Daten“*
- ISO/IEC 29190 *„Informationstechnik - Sicherheitsverfahren - Modell zur Bestimmung des Reifegrades im Datenschutz“*
- ISO/IEC 29191 *„Informationstechnik - Sicherheitsverfahren - Anforderungen für teils anonyme, teils nichtverkettbare Authentifizierung“*

4. Arbeitsprogramm

Im Zuge des Projekts soll eine DIN SPEC nach dem PAS-Verfahren (vgl. www.din.de/go/spec) erarbeitet werden. Die DIN SPEC darf nicht in Widerspruch zum Deutschen Normenwerk stehen.

Das Kick-Off wird voraussichtlich am 22.02.2019 in Köln stattfinden. Die Projektlaufzeit beträgt ca. acht Monate.

Das Kick-Off dient der Konstituierung des Konsortiums, der Abstimmung bzw. Klärung weiterer organisatorischer Punkte sowie ggf. der Aufnahme der inhaltlichen Arbeiten.

Die Veröffentlichung eines Entwurfs zur Kommentierung durch die Öffentlichkeit ist vorgesehen.

Es werden zwei Sitzungen (Kick-Off und Arbeitssitzungen) und vier Webkonferenzen durchgeführt, um die jeweils bis dahin erarbeiteten Inhalte vorzustellen, abzustimmen und ggf. zu verabschieden. Die Erarbeitung der Inhalte kann durch einzelne Workshop-Mitglieder oder Arbeitsgruppen erfolgen.

Die Terminierung der weiteren Projektmeetings und/oder Webkonferenzen erfolgt durch den Workshop in Abstimmung mit DIN.

Die DIN SPEC wird in Deutsch erarbeitet (Sitzungssprache, Berichte, usw.). Die DIN SPEC wird in Deutsch und Englisch verfasst.

ANMERKUNG In der Kalkulation wurde nur eine Sprachfassung berücksichtigt. Die Erarbeitung weiterer Sprachfassungen verursacht zusätzliche Kosten und muss deswegen gesondert vereinbart werden. Wenn eine weitere Sprachfassung gewünscht wird, kann die Übersetzung auch durch Beuth/DIN erfolgen. Diese wäre nach Verabschiedung des Manuskripts zur Veröffentlichung der DIN SPEC zusätzlich zu beauftragen.

5. Ressourcenplanung

Jedes Konsortialmitglied trägt seine im Rahmen des Vorhabens anfallenden Aufwendungen selbst.

Genehmigt der Vorsitzende des Vorstandes von DIN die Durchführung des Projekts schließt der Initiator einen Vertrag mit DIN.

Die Mitgliedschaft im Konsortium und die Teilnahme an den Projektmeetings ist kostenfrei, da die Kosten, die DIN aufgrund der Durchführung des Projekts entstehen, durch Mittel aus dem Forschungsprojekt „AUDITOR – European Cloud Service Data Protection Certification“ – gefördert durch das Bundesministerium für Wirtschaft und Energie (kurz BMWi) im Rahmen der Förderbekanntmachung "European Cloud Services Data Protection Certification (AUDITOR)" (Förderkennzeichen: 01MT17003D) – finanziert werden.

6. Regeln der Zusammenarbeit im DIN SPEC (PAS)-Konsortium

Das Projekt unterliegt den PAS-Verfahrensregeln. Alle Interessenten und Konsortialmitglieder sind dazu aufgefordert, sich unter http://www.din.de/go/spec über die Verfahrensregeln in Kenntnis zu setzen.

Die Konstituierung des Konsortiums erfolgt im Zuge des Kick-Offs. Der Kick-Off findet erst statt, nachdem der Geschäftsplan veröffentlicht und die Durchführung des Projekts durch den DIN-Vorstand genehmigt wurde. Das Konsortium muss sich aus mindestens drei Konsortialmitgliedern

unterschiedlicher Organisationen[4] zusammensetzen. Es ist nicht notwendig, dass diese unterschiedliche interessierte Kreise repräsentieren. Durch Zustimmung zum Geschäftsplan erklären die Interessenten ihre Bereitschaft zur Mitarbeit im Konsortium und werden dadurch formell zu Konsortialmitgliedern mit den einhergehenden Rechten und Pflichten. Teilnehmer des Kick-Offs, die den Geschäftsplan nicht annehmen, erhalten nicht den Status eines Konsortialmitglieds und sind von weiteren Entscheidungen des Kick-Offs sowie vom weiteren Projekt ausgeschlossen.

Entsendet eine Organisation (z. B. ein Verband) einen nicht-hauptamtlichen Mitarbeiter in das Konsortium, muss dieser von der Organisation autorisiert und DIN der Nachweis vorgelegt werden.

Jedes Konsortialmitglied erhält ein Stimmrecht und verfügt über jeweils eine Stimme. Entsendet eine Organisation mehrere Experten in das Konsortium, besitzt die Organisation, ungeachtet der Anzahl der entsendeten Teilnehmer, eine Stimme. Eine Übertragung von Stimmen auf andere Konsortialmitglieder ist nicht möglich. Bei Abstimmungen gilt einfache Mehrheit der abgegebenen Stimmen, wobei Stimmenthaltungen grundsätzlich nicht mitgezählt werden.

Das konstituierte Konsortium ist in der Regel geschlossen. Über die Aufnahme zusätzlicher Mitglieder entscheiden die bisherigen Konsortialmitglieder.

Im Zuge des Kick-Offs wählen die Konsortialmitglieder einen Konsortialleiter. Dieser leitet das Konsortium inhaltlich und führt die Entscheidungsfindung (Abstimmungen, Beschlüsse) herbei. Der Konsortialleiter wird hierbei durch den DIN-Projektmanager unterstützt, wobei DIN stets eine inhaltlich neutrale Position einnimmt. Darüber hinaus trägt der DIN-Projektmanager dafür Sorge, dass die Verfahrens- und Gestaltungsregeln von DIN bei der Erstellung der DIN SPEC eingehalten werden. Sollte der Konsortialleiter seine Funktion nicht mehr wahrnehmen können, werden vom DIN-Projektmanager Neuwahlen initiiert.

Die Organisation und Leitung des Kick-Offs erfolgt durch den DIN-Projektmanager in Abstimmung mit dem Initiator. Die übrigen Projektmeetings und/oder Webkonferenzen werden vom DIN-Projektmanager in Abstimmung mit dem Konsortialleiter organisiert.

Wenn Konsortialmitglieder bei der Verabschiedung der DIN SPEC bzw. des Entwurfs nicht anwesend sein können, sind diese über alternative Wege (z. B. schriftlich, elektronisch) in die Abstimmung einzubeziehen.

Alle Konsortialmitglieder, die für die Veröffentlichung der DIN SPEC bzw. des Entwurfs gestimmt haben, werden als Verfasser namentlich und mit der zugehörigen Organisation im Vorwort aufgeführt. Alle Konsortialmitglieder, die

[4] Organisationen sind teilnehmende juristische Personen, die die Experten in das DIN SPEC PAS-Konsortium entsenden und einer Unternehmensstruktur i.S.v. § 15 Aktiengesetz oder § 271 Absatz 2 Handelsgesetzbuch zuzurechnen sind.

gegen die Veröffentlichung der DIN SPEC bzw. des Entwurfs gestimmt oder sich enthalten haben, dürfen nicht im Vorwort genannt werden.

Um die sachgerechte Vervielfältigung und Verbreitung der Ergebnisse der Standardisierungsarbeit zu ermöglichen, räumen die Konsortialmitglieder DIN die Nutzungsrechte an den ihnen erwachsenden Urheberrechten an den Ergebnissen der Standardisierungsarbeit ein. Die Einräumung der Urhebernutzungsrechte hindert die Mitglieder des Konsortiums nicht daran, ihr eingebrachtes Wissen, ihre Erfahrungen und Erkenntnisse weiterhin zu nutzen, zu verwerten und weiterzuentwickeln.

Die Konsortialmitglieder sind angehalten, DIN über relevante Patentrechte, die in Zusammenhang mit diesem DIN SPEC Projekt stehen, zu informieren.

Nachträgliche Änderungen am Anwendungsbereich (Abschnitt 3.2) oder an der Ressourcenplanung (Abschnitt 6) erfordern neben einer 2/3-Mehrheit aller abgegebenen Stimmen zusätzlich die Zustimmung von DIN.

7. Kontaktpersonen

- Konsortialleiter:
  Sebastian Lins

  Karlsruher Institut für Technologie,
  Institut AIFB,
  Forschungsgruppe Critical Information Infrastructures,
  Postfach 6980,
  D-76049 Karlsruhe
  Tel.:+49 721 608- 42819
  Fax: +49 721 608-46581
  Email: sebastian.lins@kit.edu
  Webseite: http://cii.aifb.kit.edu

- Konsortialleiter:
  Heiner Teigeler

  Karlsruher Institut für Technologie,
  Institut AIFB,
  Forschungsgruppe Critical Information Infrastructures,
  Postfach 6980,
  D-76049 Karlsruhe
  Tel.:+49 721 608-47946
  Fax: +49 721 608-46581
  Email: heiner.teigeler@kit.edu
  Webseite: http://cii.aifb.kit.edu

- Projektmanager:
  Martin Uhlherr

DIN Deutsches Institut für Normung e. V.
Am DIN-Platz
Burggrafenstr. 6
10787 Berlin
Tel.: + 49 30 2601- 2591
Fax: + 49 30 2601 - 42591
E-Mail: Martin.Uhlherr@din.de

- Projektmanager:
  Samarkhel-Khan Yahya

  DIN Deutsches Institut für Normung e. V.
  Am DIN-Platz
  Burggrafenstr. 6
  10787 Berlin
  Tel.: + 49 30 2601- 2796
  Fax: + 49 30 2601 - 42796
  E-Mail: Samarkhel-Khan.Yahya@din.de

- Initiator:
  Prof. Dr. Ali Sunyaev

  Karlsruher Institut für Technologie,
  Institut AIFB,
  Forschungsgruppe Critical Information Infrastructures,
  Postfach 6980,
  D-76049 Karlsruhe
  Tel.: +49 721 608 46037
  E-Mail: sunyaev@kit.edu
  Webseite: http://cii.aifb.kit.edu

Anhang: Zeitplan (vorläufig)

DIN SPEC-Projekt	2018									2019																		
	Okt		Nov		Dez		Jan		Feb	Mrz		Apr		Mai		Jun		Jul		Aug		Sep		Okt		Nov	
Initiierung																												
1. Antrag und Prüfung																												
2. Erstellung des Geschäftsplans																												
3. Veröffentlichung des Geschäftsplans																												
Workshop-Phase																												
4. Kick-Off / Workshop-Konstituierung																												
5. Erstellung der DIN SPEC (PAS)																												
6. Erstellung der Übersetzung																												
7. Veröffentlichung des Entwurfs																												
8. Behandlung der Stellungnahmen																												
9. Verabschiedung DIN SPEC im Workshop																												
Veröffentlichung																												
10. Prüfung und Freigabe durch DIN																												
11. Veröffentlichung der DIN SPEC																												
Meilensteine									**K**		**W**			**W**	**W / V**				**W**		**M / V**						

K Kick-Off
M Projektmeeting
W Webkonferenz
V Verabschiedung des/der Entwurfs/DIN SPEC (PAS)

Anhang: „AUDITOR-Kriterienkatalog“ und „Umsetzungshinweise und Nachweise zum AUDITOR-Kriterienkatalog“

European Cloud Service
Data Protection Certification

AUDITOR-Kriterienkatalog

- Entwurfsfassung 0.8 -

Stand 15.10.2018

Beitrag zum Forschungsprojekt „European Cloud Service Data Protection Certification (AUDITOR)“, das aufgrund eines Beschlusses des Deutschen Bundestages vom Bundesministerium für Wirtschaft und Energie gefördert wird (FKZ 01MT17003A).

Gefördert durch:

Bundesministerium
für Wirtschaft
und Energie

aufgrund eines Beschlusses
des Deutschen Bundestages

Autoren

Alexander Roßnagel[a], Ali Sunyaev[b], Sebastian Lins[b], Natalie Maier[a], Heiner Teigeler[b]

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

[b] Forschungsgruppe Critical Information Infrastructures im Institut für Angewandte Informatik und Formale Beschreibungsverfahren (AIFB) des Karlsruher Instituts für Technologie

UNIKASSEL
VERSITÄT

provet

KIT
Karlsruher Institut für Technologie

CRITICAL
INFORMATION
INFRASTRUCTURES

Inhaltsverzeichnis

Abkürzungsverzeichnis

Abs.	Absatz
AGB	Allgemeine Geschäftsbedingungen
Art.	Artikel
BDSG n.F.	Bundesdatenschutzgesetz neue Fassung (Geltung ab 25.5.18)
DSB	Datenschutzbeauftragter
DSGVO	EU-Datenschutz-Grundverordnung (Geltung ab 25.5.18)
EG	Erwägungsgrund
EWR	Europäischer Wirtschaftsraum
i.S.v.	Im Sinne von
i.V.m.	In Verbindung mit
Lit.	Litera
Nr.	Nummer
SDM	Standard-Datenschutzmodell v.1.1 vom 26.4.2018
Sog.	Sogenannt
TCDP	Trusted Cloud Datenschutz-Profil
TOM	technische und organisatorische Maßnahmen
Ziff.	Ziffer

Hinweis zur geschlechtsneutralen Formulierung:

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

A. Gegenstand und Ziele des AUDITOR-Kriterienkatalogs

Der AUDITOR-Kriterienkatalog ist ein Prüfstandard für die Datenschutz-Zertifizierung von Cloud-Diensten gemäß den Anforderungen der EU-Datenschutz-Grundverordnung (DSGVO).

1. Adressaten und Funktionen des AUDITOR-Kriterienkatalogs

Die Datenschutz-Zertifizierung ermöglicht es Anbietern von Cloud-Diensten des privaten Sektors, die Vereinbarkeit ihrer Datenverarbeitungsvorgänge mit datenschutzrechtlichen Anforderungen nachzuweisen. Der AUDITOR-Kriterienkatalog beschreibt die datenschutzrechtlichen Anforderungen an die Verarbeitung von personenbezogenen Daten auf der Seite des Auftragnehmers (Cloud-Anbieter). Jedoch werden die datenschutzrechtlichen Anforderungen an den Auftraggeber (Cloud-Nutzer) nicht adressiert.

Zertifizierungsgegenstand AUDITOR

Den Zertifizierungsgegenstand des AUDITOR-Schemas bilden Datenverarbeitungsvorgänge von personenbezogenen Daten im Kontext von Cloud Computing. Eine Datenverarbeitung ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder Vorgangsreihe. Dazu zählen das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung von Daten.

Den Zertifizierungsgegenstand bilden Datenverarbeitungsvorgänge, die in Produkten oder Diensten oder mit Hilfe von (auch mehreren) Produkten und Diensten erbracht werden. Ein Datenverarbeitungsvorgang kann sowohl technische und automatisierte als auch nicht-technische und somit auch organisatorische (bspw. manuelle, personelle etc.) Vorgangsschritte enthalten, worunter auch Datenschutzkonzepte und -managementsysteme fallen können. Der gesamte Verarbeitungsvorgang muss den Anforderungen der Datenschutz-Grundverordnung entsprechen.

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

Weiterführende Informationen zum Zertifzierungsgegenstand von AUDITOR sind dem Begleitdokument *„Zertifizierungsgegenstand“* zu entnehmen.

Cloud-Anbieter als Adressat

Cloud-Anbieter als Auftragsverarbeiter von Datenverarbeitungsvorgängen stellen die Adressaten und Antragsteller des AUDITOR-Zertifizierungsverfahrens dar. Die Cloud-Anbieter können sowohl B2B- als auch B2C-Anbieter sein. Wichtig ist nur, dass sie als Auftragsverarbeiter tätig sind und die Datenschutzkonformität ihrer Datenverarbeitungsvorgänge durch ein Zertifikat bestätigen lassen möchten. Cloud-Nutzer als Verantwortliche möchten hingegen Kenntnis von der Zertifizierung des Cloud-Anbieters erlangen, um ihren Auswahlpflichten gemäß Art. 28 Abs. 1 DSGVO nachkommen zu können.

Cloud-Anbieter im Sinne dieses Katalogs ist jedes privatwirtschaftliche Unternehmen, das einen Cloud-Dienst am Markt anbietet und sich nach dem AUDITOR-Kriterienkatalog als Auftragsverarbeiter gemäß Art. 4 Nr. 8 DSGVO zertifizieren lassen möchte.

Cloud-Nutzer als Nutznießer

Cloud-Nutzer im Sinne dieses Katalogs ist jede natürliche oder juristische Person, die als Verantwortlicher gemäß Art. 4 Nr. 7 DSGVO Verarbeitungen personenbezogener Daten durchführt und allein oder gemeinsam mit anderen über Zwecke und Mittel dieser Verarbeitungen entscheidet und sich entschließt, diese Verarbeitungen an einen Cloud-Anbieter auszulagern.

Aufgrund der Zertifizierung der Datenverarbeitungsvorgänge eines Cloud-Dienstes kann der Cloud-Nutzer darauf vertrauen, dass der von ihm verwendete Cloud-Dienst datenschutzkonform ist. Der Anwendungsbereich der Datenschutz-Zertifizierung nach AUDITOR ist die Verarbeitung personenbezogener Daten im Auftrag (Auftragsverarbeitung) nach Art. 28 DSGVO durch einen Cloud-Anbieter. Hier muss sich der Cloud-Nutzer des Dienstes als Auftraggeber gemäß Art. 28 Abs. 1 DSGVO davon überzeugen, dass auf Seiten des Cloud-Anbieters hinreichende Garantien bestehen, die bestätigen, dass geeignete technische und organisatorische Maßnahmen (TOM) so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der Datenschutz-Grundverordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet. Der Nachweis hinreichender Garantien wird erleichtert, wenn der Cloud-Anbieter als Auftragnehmer ein Zertifikat vorweist, das die Erfüllung der gesetzlichen Anforderungen bestätigt, da ein Zertifikat gemäß Art. 28 Abs. 5 DSGVO als Faktor herangezogen werden kann, um hinreichende Garantien nachzuweisen. Für die Nutzung von Cloud-Diensten, die im Regelfall als standardisierte Dienste für eine Vielzahl von Nutzern erbracht werden, ist die Datenschutz-Zertifizierung besonders wichtig, da sie eine effiziente Möglichkeit zur Erfüllung der gesetzlichen Überprüfungspflicht darstellt.

Personenbezogene Daten als das zu schützende Gut

Als *personenbezogenen Daten* werden, der gesetzlichen Definition des Art. 4 Abs. 1 DSGVO entsprechend, alle Daten verstanden, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Im Cloud-Kontext können dies beispielsweise Anwendungsdaten des Cloud-Nutzers sein, soweit sie dem jeweiligen Datenverarbeiter die Identifizierung oder Identifizierbarkeit einer natürlichen Person ermöglichen. Die Cloud-Nutzer und Cloud-Anbieter müssen gemäß Art. 28 Abs. 3 Satz 1 DSGVO in einer rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung festlegen, welche Arten personenbezogener Daten im Rahmen der Auftragsverarbeitung weisungsgebunden durch den Auftragsverarbeiter verarbeitet werden sollen.

Verantwortungsverteilung zwischen Cloud-Anbieter und Cloud-Nutzer

Da sich der Anwendungsbereich der Datenschutz-Zertifizierung nach AUDITOR auf die Verarbeitung personenbezogener Daten im Auftrag gemäß Art. 28 DSGVO erstreckt, adressiert der AUDITOR-Kriterienkatalog lediglich datenschutzrechtliche Anforderungen an den Cloud-Anbieter in seiner Funktion als Auftragsverarbeiter. Datenverarbeitungsvorgänge, bei denen der Cloud-Anbieter nicht lediglich weisungsgebunden agiert, sondern als Verantwortlicher über Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet, werden im Rahmen der AUDITOR-Zertifizierung nicht betrachtet.

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

Die Regelungen müssen die tatsächlichen Einflussmöglichkeiten zwischen den Parteien abbilden. Je größer die Einflussmöglichkeiten des Cloud-Anbieters auf die Datenverarbeitung sind, desto eher muss er als Verantwortlicher angesehen werden. Derjenige, der über die Zwecke der Datenverarbeitung entscheidet, ist stets als Verantwortlicher anzusehen. Trifft der Cloud-Anbieter Entscheidungen über die Mittel der Datenverarbeitung, ist er nur dann Verantwortlicher, wenn er über wesentliche Mittel der Verarbeitung entscheidet. Er bleibt jedoch Auftragsverarbeiter, wenn der Cloud-Nutzer den Zweck der Verarbeitung klar definiert, dem Cloud-Anbieter jedoch Entscheidungsbefugnis über die Wahl der technischen und organisatorischen Mittel überlässt, solange diese Mittel angemessen sind, um den Verarbeitungszweck zu erreichen und er den Cloud-Nutzer über diese informiert.

Als Faustformel kann festgehalten werden, dass der Cloud-Nutzer regelmäßig für diejenigen personenbezogenen Daten als Verantwortlicher anzusehen ist, die er oder ihm zurechenbare Personen in die Cloud übertragen oder die bei der Nutzung des Cloud-Dienstes eingegeben oder durch den Cloud-

Dienst abgerufen werden. In diesem Falle spricht man meist von Anwendungsdaten des Cloud-Nutzers.

Der Cloud-Anbieter wird hingegen regelmäßig für die Verarbeitung derjenigen personenbezogenen Daten verantwortlich sein, die für die Erbringung des Cloud-Dienstes erforderlich sind. Dies hat beispielsweise zur Folge, dass der Umgang des Cloud-Anbieters mit Stammdaten und Abrechnungsdaten des Cloud-Nutzers aus dem Anwendungsbereich der AUDITOR-Zertifizierung herausfällt, da in diesem Fall der Cloud-Anbieter als Verantwortlicher angesehen werden muss, da er entscheidet, welche personenbezogenen Daten verarbeitet werden, um den Vertrag mit dem Cloud-Nutzer über die Nutzung des Cloud-Dienstes abzuschließen und auszugestalten und das AUDITOR-Zertifizierungsverfahren lediglich Datenverarbeitungsvorgänge des Cloud-Anbieters in seiner Funktion als Auftragsverarbeiter zertifiziert.

Verantwortungsverteilung zwischen Cloud-Anbieter und Subauftragsverarbeiter

Der Cloud-Anbieter hat die Möglichkeit, den Cloud-Dienstnicht nicht vollständig selbst zu erbringen, sondern sich für die Leistungserbringung weiterer Subauftragsverarbeiter zu bedienen, soweit der Cloud-Nutzer damit einverstanden ist. In diesem Fall können einzelne Abschnitte/Teile des Datenverarbeitungsvorgangs an weitere Auftragsverarbeiter delegiert oder ausgelagert werden, sodass eine Leistungskette entsteht. Die Auslagerung der Datenverarbeitung an weitere Subauftragsverarbeiter, darf jedoch nicht dazu führen, dass die Vorgaben der Datenschutz-Grundverordnung in der Leistungskette missachtet werden. Vielmehr muss der Cloud-Anbieter als Hauptauftragsverarbeiter dafür Sorge tragen, dass auf allen Stufen die einschlägigen Vorschriften der Datenschutz-Grundverordnung von allen Subauftragsverarbeitern eingehalten werden. Für die Auftragsdurchführung gegenüber dem Cloud-Nutzer bleibt der Cloud-Anbieter durchgängig verantwortlich. Setzen die zu zertifizierenden Verarbeitungsvorgänge eines Cloud-Dienstes auf nicht-anbietereigene Plattformen oder Infrastrukturen auf oder setzt der Auftragsverarbeiter sonstige Subauftragsverarbeiter ein, so kann sich das Zertifikat nur auf diejenigen Datenverarbeitungsvorgänge beziehen, die im Verantwortungsbereich des jeweiligen Auftragsverarbeiters stehen. Der Auftragsverarbeiter muss sich jedoch davon überzeugen, dass auch diese fremden von ihm genutzten Plattformen, Infrastrukturen und sonstigen Subauftragsverarbeiter die für sie relevanten datenschutzrechtlichen Vorschriften einhalten und darf nur solche für die Erbringung seines Cloud-Dienstes einsetzen. Ein Cloud-Anbieter darf daher nur solche Subauftragsverarbeiter auswählen, die gemäß Art. 28 Abs. 1 DSGVO ebenfalls *„geeignete Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Personen gewährleistet“.* Subauftragsverarbeiter können die geforderten geeigneten Garantien ihrerseits beispielsweise durch den Nachweis durchlaufener Zertifizierungsverfahren oder durch die Befolgung von anerkannten Verhaltensregeln (Code of Conduct‘) gemäß Art. 40 DSGVO erbringen.

2. Fortentwicklung von TCDP gemäß der Datenschutz-Grundverordnung

Die Zertifizierung nach dem alten Bundesdatenschutzgesetz wurde im Pilotprojekt „Datenschutz-Zertifizierung für Cloud-Dienste“ durch das im September 2016 finalisierte TCDP untersucht. Da bei der Entwicklung der Zertifizierungskriterien nach TCDP noch nicht alle einschlägigen internationalen Normen, neu entwickelten relevanten Kriterienwerke– z. B. Cloud Computing Compliance Controls Catalogue – und insbesondere die Anforderungen der Datenschutz-Grundverordnung berücksichtigt werden konnten, muss mit dem Geltungsbeginn der Datenschutz-Grundverordnung ab dem 25.5.2018 das TCDP-Kriterienwerk an die neuen Regelungen angepasst werden. Dies geschieht mit dem AUDITOR-Kriterienkatalog. Dieser zielt insbesondere auf einheitliche Kriterien für eine unionsweite Zertifizierung.

Der AUDITOR-Kriterienkatalog fokussiert alle relevanten Vorschriften für die Datenschutz-Zertifizierung von Cloud-Diensten in der Datenschutz-Grundverordnung und konkretisiert diese zu prüffähigen Kriterien.

B. Aufbau und Nutzung des AUDITOR-Kriterienkatalogs

1. Kriterienkatalogs

Der AUDITOR-Kriterienkatalog enthält „Kriterien“ und weiterführende „Erläuterungen“. Die *„Kriterien“* bezeichnen die normativen Voraussetzungen, die zu erfüllen sind, um ein Zertifikat auf der Grundlage des AUDITOR-Kriterienkatalogs zu erhalten. Sie stellen somit die Anforderungen dar, die eine akkreditierte Zertifizierungsstelle im Rahmen des Zertifizierungsverfahrens überprüft. Die *„Erläuterungen“* sollen das Verständnis der Kriterien und ihre Herleitung aus dem Gesetz erleichtern.

Darüber hinaus werden in einem Begleitdokument für jedes Kriterium „Umsetzungshinweise“ als exemplarische Leitlinien und Hilfestellungen für das Verständnis und die Umsetzung der Kriterien und „Nachweise“ als exemplarische Hilfestellung für Cloud-Anbieter zur Erbringung von Nachweisen zur Erfüllung des Kriteriums, angegeben. Das AUDITOR-Konformitätsbewertungsprogramm legt fest, wie jedes Kriterium im Rahmen der Zertifizierung zu überprüfen ist.

2. Schutzklassen

Anforderungen an TOM werden nach Schutzklassen differenziert. Dabei orientiert sich der AUDITOR-Kriterienkatalog an dem TCDP-Schutzklassenkonzept, berücksichtigt aber auch die Schutzbedarfsabstufungen nach dem Standard-Datenschutzmodell (SDM) der deutschen Datenschutzaufsichtsbehörden.

2.1 Das Schutzklassenkonzept

Das Schutzklassenklassenkonzept orientiert sich am Risiko der Datenverarbeitung für die Grundrechte und Grundfreiheiten natürlicher Personen. Daneben hat nach Art. 24, 25 und 32 DSGVO die Auswahl von TOM den Stand der Technik und die Implementierungskosten zu berücksichtigen. In Anlehnung an die EG 75, 76, 85, 90, 91, 94, 95 und 96 hat der Verantwortliche jeweils die Risiken einer Verarbeitung personenbezogener Daten für die Rechte und Freiheiten natürlicher Personen vorab zu identifizieren. In einem weiteren Schritt ist abzuschätzen, ob die Verarbeitung zu einem materiellen oder immateriellen Schaden führen könnte, insbesondere wenn sie zu einer Diskriminierung, einem Identitätsdiebstahl oder -betrug, einem finanziellen Verlust, einer Rufschädigung, einem Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten, einer unbefugten Aufhebung der Pseudonymität oder anderen erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen führen kann, wenn die betroffenen Personen um ihre Rechte und Freiheiten gebracht oder daran gehindert werden, die sie betreffenden personenbezogenen Daten zu kontrollieren.

Der Verantwortliche hat gemäß EG 76 Satz 1 die Eintrittswahrscheinlichkeit und Schwere des Schadens für die Rechte und Freiheiten der betroffenen Person in Bezug auf die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung zu bestimmen. Dieses Risiko soll er gemäß dem jeweiligen Verwendungskontext der verarbeiteten personenbezogenen Daten anhand eines objektiven Maßstabs beurteilen. Dabei hat er nach EG 76 Satz 2 festzustellen, ob die Datenverarbeitung ein Risiko oder ein hohes Risiko birgt. Diese Risikoabstufungen werden mit dem AUDITOR-Schutzklassenkonzept umgesetzt.

Der Cloud-Anbieter muss umgekehrt durch seine Dienstbeschreibung zu erkennen geben, für welche Art und Kategorien von Daten und für welche Schutzklassen der angebotene Dienst geeignet ist. Dabei muss jeder geprüfte Datenverarbeitungsvorgang in diesem Cloud-Dienst diese Schutzklasse erfüllen. Schutzklassen werden daher nicht jedem einzelnen Datenverarbeitungsvorgang im jeweiligen Cloud-Dienst zugewiesen, sondern dem Cloud-Dienst als solchem.

Ziel des Schutzklassenkonzepts ist es, den individuellen Maßstab der Datenschutz-Grundverordnung – die Anforderungen an die TOM richten sich nach dem Schutzbedarf der jeweiligen Datenverarbeitung – durch Zuordnung in Schutzklassen zu vereinfachen. Die Schutzklassen haben dabei eine doppelte Funktion: Sie beschreiben zum einen den Schutzbedarf der Datenverarbeitungsvorgänge, zum anderen die Anforderungen an die TOM. Um die unterschiedlichen Funktionen deutlich zu machen, unterscheidet das Schutzklassenkonzept einerseits Schutzbedarfsklassen und andererseits Schutzanforderungsklassen.

Die *Schutzbedarfsklassen* definieren den Schutzbedarf für Datenverarbeitungsvorgänge anhand genereller Merkmale. Dieser ergibt sich aus der Art der Daten, dem Umfang, den Umständen und den Zwecken der konkreten Datenverarbeitung.

Die *Schutzanforderungsklassen* definieren in allgemeiner Form die technischen und organisatorischen Anforderungen, die für Datenverarbeitungsdienste der betreffenden Klasse maßgeblich sind. Dabei wird für jede Schutzbedarfsklasse eine korrespondierende Schutzanforderungsklasse definiert.

Die Unterscheidung von Schutzbedarfs- und Schutzanforderungsklasse korrespondiert mit den Rollen und Verantwortungen von Cloud-Nutzer und Cloud-Anbieter in der Auftragsverarbeitung. Der Cloud-Anbieter beansprucht im Rahmen des Zertifizierungsverfahrens für jeden Dienst auf Grundlage der Prüfung und anhand der konkreten TOM eine bestimmte Schutzanforderungsklasse. Dies wird durch die Zertifizierungsstelle überprüft. Im Zertifikat wird die Eignung des Cloud-Dienstes für eine konkrete Schutzanforderungsklasse zum Ausdruck gebracht. Der Cloud-Nutzer als Verantwortlicher und Auftraggeber hat hingegen die Aufgabe, den Schutzbedarf seiner Datenverarbeitung zu bestimmen, indem er eine Schutzbedarfsklasse auswählt. Lagert er seine Datenverarbeitungsvorgänge an einen Cloud-Dienst aus, muss er einen Cloud-Dienst auszuwählen, der mindestens die entsprechende Schutzanforderungsklasse erfüllt.

2.2 Die Schutzklassen des AUDITOR-Kriterienkatalogs

Der AUDITOR-Kriterienkatalog beruht auf der Unterscheidung von drei Schutzklassen (I, II, III), für die jeweils Schutzbedarf (Schutzbedarfsklassen) und Schutzanforderungen (Schutzanforderungsklassen) beschrieben werden.

Neben den drei Schutzklassen gibt es Datenverarbeitungsvorgänge, die keine Aussagen über persönliche oder sachliche Verhältnisse natürlicher Personen enthalten, erzeugen, unterstützen oder solche ermöglichen und daher keinen datenschutzrechtlichen Schutzbedarf aufweisen. Sie liegen unterhalb von Schutzklasse 1, weshalb sie aus dem Schutzklassenkonzept herausfallen.

Auch Datenverarbeitungsvorgänge mit extrem hohem Schutzbedarf (oberhalb von Schutzbedarfsklasse 3) fallen aus dem Schutzklassenkonzept und der AUDITOR-Zertifizierung heraus. Ein extrem hoher Schutzbedarf liegt vor, wenn die Datenverarbeitungsvorgänge aufgrund der verwendeten Daten oder der konkreten Verarbeitung dieser Daten eine erhebliche Aussagekraft über die Persönlichkeit oder Lebensumstände der betroffenen Person haben, unterstützen oder zu einer solchen führen können oder sonst für die Verhältnisse der betroffenen Person von erheblicher Bedeutung sind und die unbefugte Erhebung, Verarbeitung oder Nutzung dieser Daten zu einer konkreten Gefahr für eine wesentliche Beeinträchtigung von Leben, Gesundheit oder Freiheit der betroffenen Person führen würde.

Nicht abschließende Beispiele für Daten:
- Daten von V-Leuten des Verfassungsschutzes;
- Daten über Personen, die mögliche Opfer von strafbaren Handlungen sein können;
- Adressen von Zeugen in bestimmten Strafverfahren.

Auch Datenverarbeitungsvorgänge mit individuell stark divergierenden Umständen fallen aus dem Schutzklassenkonzept und der AUDITOR-Zertifizierung heraus, weil sie der Generalisierung, die mit dem Schutzklassenkonzept einhergeht, nicht zugänglich sind.

a) Die Ermittlung der Schutzbedarfsklasse

Die Festlegung des Schutzbedarfs obliegt dem Cloud-Nutzer. Der Schutzbedarf wird in einem dreistufigen Verfahren ermittelt:

- Im 1. Schritt wird der abstrakte Schutzbedarf der zu verarbeitenden Daten nach der Datenart bestimmt.
- Im 2. Schritt ist zu prüfen, ob sich der Schutzbedarf aufgrund der konkreten Verwendung der Daten erhöht.
- Im 3. Schritt ist zu prüfen, ob der Schutzbedarf aufgrund konkreter Umstände sinkt.

Im Ergebnis wird der Schutzbedarf der konkreten Datenverarbeitung nach den Schutzbedarfsklassen kategorisiert. Die Schritte zwei und drei werden im AUDITOR-Katalog nicht weiter erläutert, weil sie den Cloud-Nutzer und nicht die Zertifizierung des Cloud-Anbieters als solche betreffen.

Schutzbedarfsklassen nach Datenart (Abstrakter Schutzbedarf – Schritt 1)

Zunächst wird der abstrakte Schutzbedarf der zu verarbeitenden Daten nach der Datenart bestimmt. Diese bildet nur den Ausgangspunkt und dient nur der ersten Einordnung der Daten. Schließlich lässt sich die Schutzbedürftigkeit von Daten nicht abstrakt bestimmen, sondern hängt von ihrem jeweiligen Verwendungszusammenhang ab.

Datenarten mit normalem Schutzbedarf (Schutzbedarfsklasse 1)

Jede Verarbeitung personenbezogener Daten stellt einen Eingriff in die Grundrechte der betroffenen Person dar. Aus diesem Grund wird davon ausgegangen, dass jede Verarbeitung personenbezogener Daten mindestens einen normalen Schutzbedarf aufweist.

In Schutzbedarfsklasse 1 fallen alle Datenverarbeitungsvorgänge, die durch die einbezogenen Daten und die konkrete Verarbeitung dieser Daten Aussagen über die persönlichen oder sachlichen Verhältnisse der betroffenen Person enthalten, erzeugen, unterstützen oder solche ermöglichen. Die unbefugte Verwendung dieser Daten kann von der betroffenen Person leicht durch Aktivitäten verhindert oder abgestellt werden oder lässt keine besonderen Beeinträchtigungen erwarten.

Nicht abschließende Beispiele für Daten (ohne Verarbeitungskontext, soweit nicht Schutzbedarfsklasse 2 oder 3):

- Name;
- Anschrift;
- Beruf;
- Geburtsjahr;
- Titel;
- Adressbuchangaben;
- Telefonverzeichnisse;
- Staatsangehörigkeit;
- Telefonnummer einer natürlichen Person.

Datenarten mit hohem Schutzbedarf (Schutzbedarfsklasse 2)

Datenverarbeitungsvorgänge, die aufgrund der verwendeten Daten oder der konkreten Verarbeitung dieser Daten eine Aussagekraft über die Persönlichkeit und/oder die Lebensumstände der betroffenen Person haben, unterstützen oder zu einer solchen führen können oder sonst für die Verhältnisse der betroffenen Person von Bedeutung sind. Die unbefugte Erhebung, Verarbeitung oder Nutzung solcher Daten kann zu Beeinträchtigungen der betroffenen Person in ihrer gesellschaftlichen Stellung oder ihren wirtschaftlichen Verhältnissen führen („Ansehen“). Weiterhin ist bei Daten, die der Gesetzgeber als besonders schutzwürdig in Art. 9 Abs. 1 DSGVO ausgewiesen hat, von einem hohen Schutzbedarf auszugehen.

Nicht abschließende Beispiele für Daten ohne Verarbeitungskontext, soweit nicht Schutzbedarfsklasse 3 oder 3+):

- Name, Anschrift eines Vertragspartners;
- Geburtsdatum;
- Familienstand;
- verwandtschaftliche Beziehungen und Bekanntenkreis;
- Daten über Geschäfts- und Vertragsbeziehungen;
- Kontext zu einem Vertragspartner (z.B. Gegenstand einer vereinbarten Leistung);
- Verarbeitungen nicht veränderbarer Personendaten, die lebenslang als Anker für Profilbildungen dienen können wie genetische Daten i.S.v. Art. 4 Nr. 13 DSGVO oder biometrische Daten i.S.v. Art. 4 Nr. 14 DSGVO;
- Daten über die rassische und ethnische Herkunft;
- Daten über politische Meinungen;
- Religiöse oder weltanschauliche Überzeugungen;
- Gewerkschaftsangehörigkeit;
- Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person;
- Verarbeitungen eindeutig identifizierender, hoch verknüpfbarer Daten wie Krankenversichertennummern oder Steuernummern;
- Daten, die mögliche Auswirkungen auf das Ansehen/die Reputation der betroffenen Person haben;

- Daten über den geschützten inneren Lebensbereich der betroffenen Person (z.B. Tagebücher)
- Gesundheitsdaten i.S.v. Art. 4 Nr. 15 DSGVO;
- Grad der Behinderung;
- Verarbeitung von Daten mit inhärenter Intransparenz für die betroffene Person (Schätzwerte beim Scoring, Anwendung von Algorithmen);
- Einkommen;
- Sozialleistungen;
- Steuern;
- Ordnungswidrigkeiten;
- Daten über Mietverhältnisse;
- Patientenverwaltungsdaten (mit Ausnahme von besonders sensiblen Diagnosedaten und dergleichen);
- Arbeitszeitzeitdaten;
- Mitgliederverzeichnisse;
- Melderegister;
- Zeugnisse und Prüfungsergebnisse;
- Versicherungsdaten;
- Personalverwaltungsdaten aus Beschäftigungsverhältnissen (mit Ausnahme von dienstlichen Beurteilungen und beruflicher Laufbahn);
- Verkehrsordnungswidrigkeiten;
- einfache Bewertungen eher geringer Bedeutung (z.B. Ja/Nein-Entscheidung bei Einstufung im Mobilfunkvertrag etc.);
- Zugangsdaten zu einem Dienst;
- Kommunikationsinhalte einer Person (z.B. E-Mail-Inhaltsdaten, Brief, Telefonat);
- (genauer) Aufenthaltsort einer Person;
- Finanzdaten einer Person (z.B. Kontostand, Kreditkartennummer, einzelne Zahlung);
- Kreditauskünfte;
- Verkehrsdaten der Telekommunikation.

Hinweis: Kommunikationsinhalte, insbesondere Schrift- oder Sprachaufzeichnungen jeder Art, können sehr unterschiedlichen Schutzbedarf, von niedrig bis sehr hoch aufweisen. Die Festlegung des Schutzbedarfs erfordert eine objektive Bewertung, in der das Ausmaß des Risikos der Datenverarbeitung beurteilt wird. Sofern der Cloud-Nutzer keine Kenntnis vom subjektiven Schutzbedarf der Kommunizierenden hat (Beispiel: allgemeiner Kollaborations-Service mit Datenablage, Videokonferenz und Mailfunktion) oder seine Dienste für besonders schutzbedürftige Kommunikationen anbietet (Beispiel: Konferenzservice für Rechtsanwälte und Mandanten, hier: Schutzklasse 3) darf er von Schutzbedarfsklasse 2 ausgehen.

Datenarten mit sehr hohem Schutzbedarf (Schutzbedarfsklasse 3)

Datenverarbeitungsvorgänge, die aufgrund der verwendeten Daten oder der konkreten Verarbeitung dieser Daten eine erhebliche Aussagekraft über die Persönlichkeit und/oder die Lebensumstände einer betroffenen Person haben, unterstützen oder zu einer solchen führen können oder sonst für die Verhältnisse der betroffenen Person von erheblicher Bedeutung sind. Die unbefugte Erhebung, Verarbeitung oder Nutzung solcher Daten kann zu erheblichen Nachteilen für die betroffene Person hinsichtlich ihrer gesellschaftlichen Stellung und ihren wirtschaftlichen Verhältnissen führen („Existenz“).

Hinweis: Als Datenarten in diesem Sinne werden auch Datenmehrheiten, insbesondere verkettete Daten (z.B. Persönlichkeitsprofile) angesehen, aus denen sich ein neuer Informationsgehalt ergibt.

Nicht abschließende Beispiele für Daten mit sehr hohem Schutzbedarf:

- Daten, die einem Berufs-, Geschäfts-, Fernmelde-, oder Mandantengeheimnis unterliegen (z.B. Patientendaten, Mandantendaten);
- Daten, deren Kenntnis eine erhebliche konkrete Schädigung der betroffenen Person oder Dritter ermöglicht (z.B. Persönliche Identifikationsnummer, Transaktionsnummer im Online-Banking);
- Schulden;
- Patientendaten (besonders sensible Diagnosedaten wie Aids, Krebs, psychischer Erkrankungen und dergleichen, soweit nicht Schutzbedarfsklasse 2);
- besonders sensible Sozialdaten;

- Pfändungen;
- Personalverwaltungsdaten wie dienstliche Beurteilungen, berufliche Laufbahn und dergleichen soweit nicht Schutzbedarfsklasse 2;
- Daten über Vorstrafen und strafprozessuale Verhältnisse (z.B. Ermittlungsverfahren) einer Person und entsprechende Verdachtsmomente; Straffälligkeit;
- Besonders sensitive Gesundheitsdaten i.S.v. Art. 4 Nr. 15 DSGVO wie z.B. zu Krankheiten, deren Bekanntwerden der betroffenen Person in besonderem Maße unangenehm sind oder zu einer gesellschaftlichen Stigmatisierung der betroffenen Person führen können;
- Persönlichkeitsprofile, z.B. Bewegungsprofil, Kaufverhaltensprofil, mit erheblicher Aussagekraft über die Persönlichkeit der betroffenen Person.

b) Schutzanforderungsklassen

Die Schutzanforderungsklassen dienen dazu, die TOM festzulegen, die dazu geeignet sind, die Rechte und Freiheiten der betroffenen Personen in Bezug auf die jeweiligen Risiken des Dienstes angemessen zu schützen.

Schutzanforderungsklasse 1

Der Cloud-Anbieter hat risikoangemessene TOM zu ergreifen, um die Datenminimierung, Verfügbarkeit, Integrität, Vertraulichkeit, Nichtverkettung, Transparenz und Intervenierbarkeit von personenbezogenen Daten sicherzustellen (siehe auch Gewährleistungsziele aus dem SDM). Für den Bereich der Informationssicherheit bedeutet dies, dass die Daten, insbesondere gegen Vernichtung, Verlust, Veränderung, unbefugten Zugang und unbefugte Offenlegung, zu schützen sind sowie die Belastbarkeit des Cloud-Dienstes zu gewährleisten ist.

Die TOM müssen geeignet sein, um im Regelfall solche Vorgänge aufgrund technischer oder organisatorischer Fehler, einschließlich Bedienfehler, des Cloud-Anbieters oder seiner Mitarbeiter oder fahrlässiger Handlungen Dritter auszuschließen. Gegen vorsätzliche Eingriffe ist ein Mindestschutz vorzusehen, der diese erschwert. Jeder Eingriff muss nachträglich festgestellt werden können.

Schutzanforderungsklasse 2

Ein hoher Schutzbedarf führt dazu, dass zusätzliche oder wirksamere risikoangemessene TOM ergriffen werden müssen, um die Datenminimierung, Verfügbarkeit, Integrität, Vertraulichkeit, Nichtverkettung, Transparenz und Intervenierbarkeit von personenbezogenen Daten sicherzustellen (siehe auch Gewährleistungsziele aus dem SDM). Für die Informationssicherheit bedeutet dies, dass die Daten, insbesondere gegen Vernichtung, Verlust, Veränderung, unbefugten Zugang und unbefugte Offenlegung, zu schützen sind sowie die Belastbarkeit des Cloud-Dienstes zu gewährleisten ist. Gleichzeitig müssen die für Schutzanforderungsklasse 1 geeigneten Maßnahmen erfüllt und ihre Ausführung an den Schutzbedarf angepasst werden.

Dies kann erreicht werden, indem die Wirkung einer Maßnahme erhöht wird, soweit diese einen Ansatzpunkt für eine solche Skalierung bietet. Ein Beispiel hierfür ist die Erhöhung der Länge eingesetzter kryptografischer Schlüssel oder der Einsatz einer Zwei-Faktor-Authentifizierung oder von Hardware-Token. Weiterhin kann eine Anpassung dadurch erfolgen, dass mit größerer Zuverlässigkeit eine spezifikationsgerechte Ausführung der Maßnahme sichergestellt wird. Dazu müssen mögliche Störeinflüsse bestimmt und die Robustheit der Maßnahmen durch zusätzliche Vorkehrungen – oft organisatorischer Natur – erhöht werden.

Die ergriffenen Maßnahmen müssen geeignet sein, um im Regelfall solche Vorgänge aufgrund technischer oder organisatorischer Fehler, einschließlich Bedienfehler, des Cloud-Anbieters oder seiner Mitarbeiter oder fahrlässiger Handlungen Dritter auszuschließen. Die Maßnahmen müssen auch geeignet sein, Schädigungen durch fahrlässige Handlungen Befugter im Regelfall auszuschließen. Gegen vorsätzliche Eingriffe ist ein Schutz vorzusehen, der zu erwartende Eingriffe hinreichend sicher ausschließt. Dazu gehört insbesondere ein hinreichender Schutz gegen bekannte Angriffsszenarien sowie Maßnahmen, durch die Eingriffe im Regelfall (nachträglich) festgestellt werden können.

Schutzanforderungsklasse 3

Der Cloud-Anbieter muss über die TOM der Schutzanforderungsklassen 1 und 2 hinaus risikoangemessene TOM ergreifen, um die Daten, insbesondere gegen Vernichtung, Verlust, Veränderung, unbefugten Zugang und unbefugte Offenlegung, zu schützen.

Die Maßnahmen müssen geeignet sein, um solche Vorgänge aufgrund technischer oder organisatorischer Fehler, einschließlich Bedienfehler, oder fahrlässiger oder vorsätzlicher Handlungen hinreichend sicher auszuschließen. Dazu gehört insbesondere ein hinreichender Schutz gegen bekannte Angriffsszenarien sowie Verfahren zur Erkennung von Missbräuchen. Jeder Eingriff muss nachträglich festgestellt werden können.

C. Kriterien und Umsetzungsempfehlungen

Kapitel I: rechtsverbindliche Vereinbarung zur Auftragsverarbeitung

Erläuterung

Der Cloud-Anbieter muss sicherstellen, dass die Leistungen gegenüber dem Cloud-Nutzer aufgrund einer rechtsverbindlichen Vereinbarung[1] erbracht werden, die die gesetzlichen Anforderungen der Datenschutz-Grundverordnung an die Auftragsverarbeitung erfüllt. Die gesetzlichen Anforderungen an diese Vereinbarung werden durch die nachfolgenden Kriterien der Nummern 1.1 bis 1.8, die unabhängig vom jeweiligen Service-Modell des Cloud-Dienstes Anwendung finden, konkretisiert.

Nr. 1 – Wirksame und eindeutige Vereinbarung zwischen Cloud-Anbieter und Cloud-Nutzer (Art. 28 Abs. 3 DSGVO)

Nr. 1.1 – Dienstleistung aufgrund einer rechtsverbindlichen Vereinbarung und Form der Vereinbarung (Art. 28 Abs. 3 Satz 1 und Abs. 9 DSGVO)

Kriterium

(1) Der Cloud-Anbieter stellt durch geeignete technische oder organisatorische Vorkehrungen sicher, dass der Cloud-Dienst erst nach dem Abschluss einer rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung mit dem Cloud-Nutzer erbracht wird.

(2) Diese Vereinbarung muss die Kriterien dieses Kapitels (Nr. 1.1 bis 1.8) erfüllen.

(3) Die rechtsverbindliche Vereinbarung ist schriftlich oder in einem elektronischen Format[2] abzufassen.

Erläuterung

Die rechtsverbindliche Vereinbarung zur Datenverarbeitung im Auftrag ist wesentlich, da mit dieser die Rolle des Cloud-Anbieters als Auftragsverarbeiter i.S.v. Art. 4 Nr. 8 DSGVO gegenüber der Rolle des Cloud-Nutzers als Verantwortlichem ausdrücklich klargestellt wird. Oft liegt dieser Vereinbarung eine weitere Vereinbarung über die Leistungserbringung zugrunde; beide Vereinbarungen sind zu unterscheiden.

Nr. 1.2 – Gegenstand und Dauer der Verarbeitung (Art. 28 Abs. 3 Satz 1 DSGVO)

Kriterium

(1) Der Gegenstand und die Dauer des Auftrags sind in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung so konkret wie möglich festzulegen.

(2) Der Gegenstand des Auftrags gemäß der in Anspruch genommen Datenverarbeitung ist in der rechtsverbindlichen Vereinbarung zu spezifizieren.

(3) Die Vereinbarung muss die Dauer des Auftrages durch einen Start- und Endpunkt oder den Verweis auf eine unbestimmte Nutzungszeit festlegen.

---

[1] Art. 28 Abs. 3 Satz 1 DSGVO schreibt die Auftragsverarbeitung auf Grundlage eines Auftragsverarbeitungsvertrags vor. Alternativ zum Vertrag kann auch ein anderes Rechtsinstrument nach dem Unionsrecht oder dem Recht der Mitgliedstaaten im Sinne des Art. 28 Abs. 3 Satz 1 DSGVO als Rechtsgrundlage für die Auftragsverarbeitung dienen.

[2] Für das elektronische Format reicht die Textform i.S.v. § 126b BGB aus.

(4) Die Voraussetzungen einer Kündigung sind in die Vereinbarung aufzunehmen.

Nr. 1.3 – Art und Zwecke der Datenverarbeitung (Art. 28 Abs. 3 Satz 1 DSGVO)

Kriterium

(1) In der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung werden der Umfang, die Art und der Zweck der vorgesehenen Verarbeitung von Daten im Auftrag, die Art der gemäß dem Schutzklassenkonzept verarbeiteten Daten sowie die Kategorien betroffener Personen festgelegt.

Nr. 1.4 – Weisungsbefugnisse des Cloud-Nutzers (Art. 28 Abs. 3 Satz 2 lit. a DSGVO)

Kriterium

(1) Die rechtsverbindliche Vereinbarung über die Auftragsverarbeitung sieht vor, dass 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 werden.

(2) Wird im Rahmen standardisierter Massengeschäfte keine individuelle rechtsverbindliche Vereinbarung geschlossen, hat der Cloud-Anbieter in seiner Dienstbeschreibung die durch ihn technisch ausführbaren Dienstleistungen auf eine aus der Cloud-Nutzer-Perspektive nachvollziehbare Weise so präzise wie möglich zu benennen, um diesem eine Auswahl nach Art. 28 Abs. 1 DSGVO zu ermöglichen.

Erläuterung

Die Weisungsgebundenheit wird in der Datenschutz-Grundverordnung an mehreren Stellen genannt (Art. 28 Abs. 3 Satz 2 lit. a; Art. 28 Abs. 3 Satz 3 DSGVO; indirekt in Art. 28 Abs. 10 und Art. 29, Art. 32 Abs. 4 DSGVO).

Überschreitet der Cloud-Anbieter die Maßgaben des Cloud-Nutzers nach dessen Weisungen, so liegt ein Verstoß gegen Art. 28 Abs. 10 und Art. 29 DSGVO vor, und der Cloud-Anbieter hat mit haftungsrechtlichen Konsequenzen zu rechnen.

Nr. 1.5 – Ort der Datenverarbeitung (indirekt Art. 28 Abs. 3 Satz 2 lit. a DSGVO)

Kriterium

(1) In der rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung wird festgelegt, ob der Cloud-Anbieter die Daten des Cloud-Nutzers innerhalb der EU/des EWR verarbeitet oder in einem Drittland.

(2) Wird die Datenverarbeitung in einem Drittland durchgeführt, ist dieses konkret in der rechtsverbindlichen Vereinbarung zu benennen.

(3) In der rechtsverbindlichen Vereinbarung muss festgelegt werden, dass in den Fällen, in denen sich während des Vereinbarungszeitraums der Ort der Verarbeitung aus Gründen ändert, die im Verantwortungsbereich des Cloud-Anbieters liegen oder für beide Parteien unvorhersehbar sind, der Cloud-Anbieter diese Änderung dem Cloud-Nutzer unverzüglich mitteilt.

(4) Bei jeder wesentlichen Abweichung von der Festlegung des Ortes der Datenverarbeitung wird dem Cloud-Nutzer in der rechtsverbindlichen Vereinbarung ein sofortiges Kündigungsrecht eingeräumt.

Nr. 1.6 – Verpflichtung zur Vertraulichkeit (Art. 28 Abs. 3 Satz 2 lit. b DSGVO)

Kriterium

(1) Der Cloud-Anbieter verpflichtet sich in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung, dass die zur Verarbeitung von personenbezogenen Daten befugten Personen vor Aufnahme der datenverarbeitenden Tätigkeit zur Vertraulichkeit verpflichtet werden, sofern sie nicht bereits einer angemessenen vergleichbaren gesetzlichen Verschwiegenheitspflicht unterliegen.

Erläuterung

Die Verpflichtung zur Vertraulichkeit und die Belehrung zur Verschwiegenheit fördern das Gewährleistungsziel der Vertraulichkeit (SDM 6.2.3)

Nr. 1.7 – Technisch-organisatorische Maßnahmen, Unterbeauftragung und Unterstützung (Art. 28 Abs. 3 Satz 2 lit. c bis f i.V.m. Kap. III und Art. 32 – 36 DSGVO)

Kriterium

(1) Die Schutzklasse und die für sie zu treffenden TOM werden in einer rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung festgelegt.

(2) Die rechtsverbindliche Vereinbarung über die Auftragsverarbeitung enthält die Angabe, ob der Cloud-Anbieter oder der Cloud-Nutzer eine Pseudonymisierung, Anonymisierung oder Verschlüsselung (Nr. 2.7, Nr. 2.8 und Nr. 2.9) der zu verarbeitenden personenbezogenen Daten vornimmt und ob diese auch gegenüber den Mitarbeitern des Cloud-Anbieters wirksam sind. Die maximale Anzahl an Personen aus den Mitarbeitern des Cloud Anbieters und seiner Subauftragsverarbeiter sind anzugeben, für die die Pseudonymisierung, Anonymisierung oder Verschlüsselung nicht wirksam sind.

(3) Der Cloud-Anbieter legt in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung fest, auf welchem Niveau und in welchem Zeitraum er nach einem physischen oder technischen Zwischenfall die Daten des Cloud-Nutzers wiederherstellen und dem Cloud-Nutzer Zugang zu ihnen gewährleistet kann (Nr. 2.11).

(4) In der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung wird bestimmt, wie der Cloud-Anbieter die Bedingungen gemäß Art. 28 Abs. 2 und 4 DSGVO für die Inanspruchnahme der Dienste weiterer Auftragsverarbeiter einhält.

(5) Die Verfahren zur Unterstützung des Cloud-Nutzers bei der Erfüllung der Betroffenenrechte gemäß 6, bei der Durchführung einer Datenschutz-Folgenabschätzung gemäß 7 und zur Erfüllung der Meldepflicht bei Datenschutzverletzungen nach Nr. 8.2 werden in der rechtgültigen Vereinbarung über die Auftragsverarbeitung festgelegt.

Nr. 1.8 – Rückgabe von Datenträgern und Löschung von Daten (Art. 28 Abs. 3 Satz 2 lit. g DSGVO)

Kriterium

(1) Die Pflichten des Cloud-Anbieters zur Rückgabe von Datenträgern, Rückführung von Daten und Löschung von Daten nach Ende der Auftragsverarbeitung sind in einer rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung festzulegen.

Kapitel II: Rechte und Pflichten des Cloud-Anbieters

Nr. 2 – Gewährleistung der Datensicherheit durch geeignete TOM nach dem Stand der Technik

Nr. 2.1 – Risiko- und Schutzkonzept (Art. 24, 25, 28, 32, 35 i.V.m. Art. 5 Abs. 1 lit. f DSGVO)

Kriterium

(1) Der Cloud-Anbieter führt eine Risikoanalyse in Bezug auf die Datensicherheit durch und verfügt über ein Risiko- und Schutzkonzept entsprechend seiner Schutzklasse, das den spezifischen Risiken seiner Datenverarbeitungsvorgänge angemessen ist.

(2) Im Risiko- und Schutzkonzept stellt der Cloud-Anbieter die von ihm ergriffenen Datensicherheitsmaßnahmen dar und schildert auch die Abwägungen, die er vorgenommen hat, um zu diesen Maßnahmen zu gelangen.

(3) Das Risiko- und Schutzkonzept ist schriftlich zu dokumentieren.

(4) Das Risiko- und Schutzkonzept ist in regelmäßigen Abständen auf Aktualität und Angemessenheit zu überprüfen und bei Bedarf zu aktualisieren.

(5) Das Risiko- und Schutzkonzept grenzt die Verantwortung des Cloud-Anbieters von der Verantwortlichkeit der Cloud-Nutzer ab.

(6) Das Risiko- und Schutzkonzept grenzt die Verantwortung des Cloud-Anbieters von der Verantwortlichkeit eingebundener Subauftragsverarbeiter ab.

(7) Soweit das Risiko- und Schutzkonzept Sicherheitsmaßnahmen des Cloud-Nutzers verlangt, sind diese dem Cloud-Nutzer in Schriftform oder in einem elektronischen Format mitzuteilen.

Erläuterung

Der Cloud-Anbieter hat risikoangemessene TOM festzulegen, um Risiken einer Verletzung der Rechte und Freiheiten von natürlichen Personen zu verhindern. Insbesondere hat er Risiken gegen unbeabsichtigte und unrechtmäßige Vernichtung, Verlust, Veränderung, unbefugte Offenlegung oder unbefugten Zugang zu personenbezogenen Daten auszuschließen oder zu minimieren. Bei der Festlegung der konkreten Maßnahmen berücksichtigt er nicht nur die Modalitäten der Verarbeitung und die Eintrittswahrscheinlichkeit und Schwere des Schadens, sondern auch den Stand der Technik sowie die Implementierungskosten der Maßnahmen. Die dabei getroffenen Abwägungen müssen aus dem Risiko- und Schutzkonzept ersichtlich sein. Der Cloud-Nutzer ermittelt den Schutzbedarf für seine Datenverarbeitung und legt dafür eine Schutzbedarfsklasse fest. Der Cloud-Anbieter legt für seinen angebotenen Dienst die Schutzanforderungsklasse fest. Der Cloud-Nutzer wählt einen Cloud-Dienst aus, der eine zu seiner Schutzbedarfsklasse passende Schutzanforderungsklasse bietet.

Nr. 2.2 – Sicherheitsbereich und Zutrittskontrolle (Art. 32 Abs. 1 lit. b und Abs. 2 i.V.m. Art. 5 Abs. 1 lit. f DSGVO)

Kriterium

(1) Insofern der Cloud-Anbieter für den Sicherheitsbereich und die Zutrittskontrolle zu Räumen und Datenverarbeitungsanlagen verantwortlich ist, muss er folgende Kriterien gemäß seiner Schutzklasse erfüllen.

Schutzklasse 1

(3) Der Cloud-Anbieter stellt durch risikoangemessene TOM sicher, dass Räume und Anlagen gegen Schädigung durch Naturereignisse[3] gesichert werden und Unbefugte keinen Zuritt zu Räumen und Datenverarbeitungsanlagen erhalten, um unbefugte Kenntnisnahmen personenbezogener Daten und Einwirkungsmöglichkeiten auf die Datenverarbeitungsanlagen auszuschließen.

(4) Die Maßnahmen müssen geeignet sein, um im Regelfall den Zutritt Unbefugter aufgrund technischer oder organisatorischer Fehler, einschließlich Bedienfehler, des Cloud-Anbieters oder fahrlässiger Handlungen Dritter auszuschließen. Gegen vorsätzliche Eingriffe ist ein Mindestschutz vorzusehen, der diese erschwert.

Schutzklasse 2

(5) Es müssen die Kriterien von Schutzklasse 1 erfüllt werden.

(6) Die Maßnahmen müssen auch geeignet sein, Schädigungen durch fahrlässige Handlungen Befugter im Regelfall auszuschließen. Weiterhin muss sichergestellt sein, dass unbefugter Zutritt durch fahrlässige und vorsätzliche Handlungen hinreichend sicher ausgeschlossen ist. Dies schließt Schutz gegen Zutrittsversuche durch Täuschung oder Gewalt ein. Es ist ein hinreichender Schutz gegen bekannte Angriffsszenarien sowie Maßnahmen, durch die ein unbefugter Zutritt im Regelfall (nachträglich) festgestellt werden kann, vorzusehen.

Schutzklasse 3

(7) Es müssen die Kriterien von Schutzklasse 1 und Schutzklasse 2 erfüllt werden.

(8) Jeder Zutritt und jeder Zutrittsversuch müssen festgestellt werden können.

Erläuterung

Dieses Kriterium konkretisiert in Teilen die in Art. 32 Abs. 1 lit. b und Art. 5 Abs. 1 lit. f DSGVO enthaltene, in hohem Maße konkretisierungsbedürftige Pflicht, die Gewährleistungsziele Integrität, Vertraulichkeit und Verfügbarkeit (SDM 6.2.1 – 6.2.3) von personenbezogenen Daten und Diensten auf Dauer zu gewährleisten. Dies setzt ein Berechtigungskonzept für den Zutritt zu Datenverarbeitungsanlagen voraus. Die Zutrittskontrolle gewährleistet den Zutrittsschutz nicht nur im Normalbetrieb, sondern auch im Zusammenhang mit Naturereignissen.

Nr. 2.3 – Zugangskontrolle (Art. 32 Abs. 1 lit. b und Abs. 2 i.V.m. Art. 5 Abs. 1 lit. f DSGVO)

Kriterium

(1) Insofern der Cloud-Anbieter für den Zugang zu Datenverarbeitungsvorgängen verantwortlich ist, muss er folgende Kriterien gemäß seiner Schutzklasse erfüllen.

Schutzklasse 1

(2) Der Cloud-Anbieter hat sicherzustellen, dass Unbefugte keinen Zugang zu Datenverarbeitungsvorgängen erhalten und auf diese einwirken können. Dies gilt auch für Sicherungskopien, soweit diese personenbezogene Daten enthalten.

(3) Die Erforderlichkeit der Berechtigungen für den Zugang zu Datenverarbeitungsanlagen ist in regelmäßigen Abständen auf Aktualität und Angemessenheit zu überprüfen und bei Bedarf zu aktualisieren.

(4) Für Zugänge von Befugten über das Internet ist eine starke Authentifizierung erforderlich, die mindestens zwei Elemente der Kategorie Wissen, Besitz oder Inhärenz verwendet. Die Elemente müssen voneinander unabhängig sein, sodass die Überwindung eines Elements die Zuverlässigkeit des anderen nicht beeinflusst. Sie müssen so konzipiert sein, dass die Ver-

[3] Naturereignisse stellen ungewöhnliche, in der Natur ablaufende Vorgänge dar, die vom Menschen nicht beeinflusst werden können und zeitlich begrenzt sind. Beispiele sind Blitze, Hochwasser, Trockenheit.

traulichkeit der Authentifizierungsdaten gewährleistet ist. Der Zugang über das Internet hat über einen verschlüsselten Kommunikationskanal zu erfolgen.

(5) Die Maßnahmen zur Zugangskontrolle müssen geeignet sein, um im Regelfall den Zugang zu Datenverarbeitungsvorgängen und Daten durch Unbefugte aufgrund technischer oder organisatorischer Fehler, einschließlich Bedienfehler, des Cloud-Anbieters oder fahrlässiger Handlungen des Cloud-Nutzers oder Dritter auszuschließen. Gegen vorsätzliche Eingriffe ist ein Mindestschutz vorzusehen, der diese erschwert.

Schutzklasse 2

(6) Es müssen die Kriterien von Schutzklasse 1 erfüllt werden.

(7) Gegen zu erwartenden vorsätzlichen unbefugten Zugang ist ein Schutz vorzusehen, der zu erwartende Zugangsversuche hinreichend sicher ausschließt. Dazu gehören insbesondere ein hinreichender Schutz gegen bekannte Angriffsszenarien sowie Maßnahmen, durch die ein unbefugter Zugang im Regelfall nachträglich festgestellt werden kann.

Schutzklasse 3

(8) Es müssen die Kriterien von Schutzklasse 1 und Schutzklasse 2 erfüllt werden.

(9) Es muss sichergestellt sein, dass unbefugter Zugang zu Datenverarbeitungssystemen hinreichend sicher ausgeschlossen ist. Dies schließt regelmäßig Maßnahmen zur aktiven Erkennung von Angriffen ein. Jeder unbefugte Zugang und entsprechende Versuche müssen nachträglich festgestellt werden können.

Erläuterungen

Das Kriterium der Zugangskontrolle konkretisiert in Teilen die in Art. 32 Abs. 1 lit. b und Abs. 2 DSGVO enthaltene, in hohem Maße konkretisierungsbedürftige Pflicht, die Gewährleistungsziele der Integrität, Vertraulichkeit und Verfügbarkeit (SDM 6.2.1 – 6.2.3) von personenbezogenen Daten und Diensten auf Dauer sicherzustellen. Dies setzt ein Berechtigungskonzept für den Zugang zu Datenverarbeitungsvorgängen voraus.

Nr. 2.4 – Zugriffskontrolle (Art. 32 Abs. 1 lit. b und Abs. 2 i.V.m. Art. 5 Abs. 1 lit. f DSGVO)

Kriterium

Schutzklasse 1

(1) Der Cloud-Anbieter stellt durch TOM sicher, dass Berechtigte nur im Rahmen ihrer Berechtigungen Zugriff auf Datenverarbeitungsvorgänge nehmen können und unbefugte Einwirkungen auf Datenverarbeitungsvorgänge ausgeschlossen werden. Dies gilt auch für Sicherungskopien, soweit sie personenbezogene Daten enthalten.

(2) Zugriffe auf Datenverarbeitungsvorgänge sind abzusichern und zu kontrollieren.

(3) Die Maßnahmen müssen geeignet sein, um im Regelfall den Zugriff auf Daten durch Unbefugte aufgrund technischer oder organisatorischer Fehler, einschließlich Bedienfehler, des Cloud-Anbieters oder fahrlässiger Handlungen des Cloud-Nutzers oder Dritter auszuschließen. Gegen vorsätzliche Eingriffe ist ein Mindestschutz vorzusehen, der diese erschwert.

(4) Für Zugriffe von Befugten über das Internet ist eine starke Authentifizierung erforderlich, die mindestens zwei Elemente der Kategorie Wissen, Besitz oder Inhärenz verwendet, die insofern voneinander unabhängig sind, als die Überwindung eines Elements die Zuverlässigkeit des anderen nicht in Frage stellt, und die so konzipiert ist, dass die Vertraulichkeit der Authentifizierungsdaten gewährleistet ist.

(5) Administrative Zugriffe und Tätigkeiten auf kritischen Systemen sind durch einen starken Authentisierungsmechanismus zu schützen und zu protokollieren. Die Fernadministration des Cloud-Dienstes durch Mitarbeiter des Cloud-Anbieters hat über einen verschlüsselten Kommunikationskanal zu erfolgen.

(6) Ist ein privilegierter Zugriff der Mitarbeiter des Cloud-Anbieters auf personenbezogene Daten auf Weisung im Cloud-Dienst vorgesehen, muss dieser eindeutig geregelt und dokumentiert sein. Die privilegierten Zugriffe müssen eine andere Nutzeridentität aufweisen als die Zugriffe für die tägliche Arbeit.

Schutzklasse 2

(7) Es müssen die Kriterien von Schutzklasse 1 erfüllt werden.

(8) Gegen zu erwartenden vorsätzlichen unbefugten Zugriff ist ein Schutz vorzusehen, der zu erwartende Zugriffsversuche hinreichend sicher ausschließt. Dazu gehören insbesondere ein hinreichender Schutz gegen bekannte Angriffsszenarien sowie Maßnahmen, durch die ein unberechtigter Zugriff im Regelfall nachträglich festgestellt werden kann.

(9) Es ist sicherzustellen, dass verschiedene zweckbezogene Nutzerrollen für Mitarbeiter des Cloud-Nutzers festgelegt werden, damit nicht zweckgemäße Zugriffe auf personenbezogene Daten logisch ausgeschlossen werden.

(10) Ist ein privilegierter Zugriff der Mitarbeiter des Cloud-Anbieters auf personenbezogene Daten auf Weisung vorgesehen, muss dieser eindeutig geregelt und dokumentiert sein. Der privilegierte Zugriff darf nur in Rollen erfolgen, die von der Administration und vom Rechenzentrumsbetrieb unabhängig sind. Der Zugriff ist mit Zwei-Faktor-Authentifizierung abzusichern und die Anzahl der Mitarbeiter mit privilegiertem Zugriff ist so gering wie möglich zu halten.

Schutzklasse 3

(11) Es müssen die Kriterien von Schutzklasse 1 und Schutzklasse 2 erfüllt werden.

(12) Es muss sichergestellt sein, dass unbefugte Zugriffe auf Daten hinreichend sicher ausgeschlossen sind. Dies schließt regelmäßig Maßnahmen zur aktiven Erkennung von Angriffen ein. Jeder unbefugte Zugriff und entsprechende Versuche müssen nachträglich festgestellt werden können.

Erläuterungen

Das Kriterium der Zugriffskontrolle konkretisiert in Teilen die in Art. 32 Abs. 1 lit. b und Abs. 2 DSGVO enthaltene, in hohem Maße konkretisierungsbedürftige Pflicht, die Gewährleistungsziele Integrität, Vertraulichkeit und Verfügbarkeit (SDM 6.2.1 – 6.2.3) von personenbezogenen Daten und Diensten auf Dauer sicherzustellen. Dies setzt ein Berechtigungskonzept für den Zugriff auf personenbezogenen Daten voraus.

Nr. 2.5 – Übertragung von Daten und Transportverschlüsselung (Art. 32 Abs. 1 lit. b und Abs. 2 i.V.m. Art. 5 Abs. 1 lit. f DSGVO)

Kriterium

Schutzklasse 1

(1) Der Cloud-Anbieter setzt bei Datenübertragungen eine Transportverschlüsselung nach dem Stand der Technik oder gleichermaßen angemessene Maßnahmen ein oder fordert dies durch entsprechende Konfiguration von Schnittstellen. Die eingesetzte Transportverschlüsselung muss gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

(2) Die Maßnahmen müssen geeignet sein, um im Regelfall solche Handlungen Unbefugter aufgrund technischer oder organisatorischer Fehler, einschließlich Bedienfehler, des Cloud-Anbieters oder seiner Mitarbeiter oder fahrlässiger Handlungen des Cloud-Nutzers oder Dritter auszuschließen. Die Maßnahmen müssen ferner geeignet sein, die fahrlässige Weitergabe von Daten an Unbefugte durch den Cloud-Anbieter und seine Mitarbeiter im Regelfall auszuschließen. Gegen vorsätzliche Eingriffe ist ein Mindestschutz vorzusehen, der diese erschwert.

(3) Datenübertragungen, auch solche vom und an den Cloud-Nutzer oder an Subauftragsverarbeiter, müssen automatisiert protokolliert werden.

(4) Es muss dokumentiert sein, an welche Empfänger eine Weitergabe personenbezogener Daten durchgeführt wurde.

(5) Die Kriterien gelten auch für die Übertragung von Daten im eigenen Netzwerk des Cloud-Anbieters und seiner Subauftragsverarbeiter und zwischen diesen.

(6) Der Transport von Datenträgern ist mit TOM zu schützen, sodass personenbezogene Daten beim Transport der Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Der Cloud-Anbieter dokumentiert die Transporte.

Schutzklasse 2

(7) Es müssen die Kriterien von Schutzklasse 1 erfüllt werden.

(8) Gegen vorsätzliches unbefugtes Lesen, Kopieren, Verändern oder Entfernen ist ein Schutz vorzusehen, der zu erwartende Versuche hinreichend sicher ausschließt. Dazu gehören insbesondere ein hinreichender Schutz gegen bekannte Angriffsszenarien sowie Maßnahmen, durch die ein unbefugtes Lesen, Kopieren, Verändern oder Entfernen im Regelfall (nachträglich) festgestellt werden kann. Bei verschlüsselter Übertragung sind die Schlüssel sicher aufzubewahren.

Schutzklasse 3

(9) Es müssen die Kriterien von Schutzklasse 1 und Schutzklasse 2 erfüllt werden.

(10) Es muss sichergestellt sein, dass unbefugtes Lesen, Kopieren, Verändern oder Entfernen von Daten durch den Cloud-Anbieter, seine Mitarbeiter oder Dritte hinreichend sicher ausgeschlossen ist. Dies schließt regelmäßig Maßnahmen zur aktiven Erkennung und Abwehr von Angriffen ein. Jedes unbefugte Lesen, Kopieren, Verändern oder Entfernen von Daten und auch jeder entsprechende Versuch müssen nachträglich festgestellt werden können. Bei verschlüsselter Übertragung ist durch TOM sicherzustellen, dass der Cloud-Anbieter und seine Mitarbeiter keinen Zugriff auf die Schlüssel haben.

Erläuterungen

Das Kriterium der Übertragungs- und Transportkontrolle konkretisiert die in Art. 32 Abs. 1 lit. b und Abs. 2 DSGVO enthaltene, in hohem Maße konkretisierungsbedürftige Pflicht, die Gewährleistungsziele Integrität, Vertraulichkeit und Verfügbarkeit (SDM 6.2.1 – 6.2.3) von personenbezogenen Daten und Diensten auf Dauer sicherzustellen und personenbezogene Daten gegen unbeabsichtigte oder unrechtmäßige Vernichtung, Verlust, Veränderung, unbefugten Zugang oder unbefugte Offenlegung während der elektronischen Übertragung, des Transports oder der Speicherung auf Datenträgern zu schützen.

Nr. 2.6 – Nachvollziehbarkeit der Datenverarbeitung (Art. 32 Abs. 1 lit. b und Abs. 2 i.V.m. Art. 5 Abs. 1 lit. c, e und f DSGVO)

Kriterium

Schutzklasse 1

(1) Der Cloud-Anbieter hat durch Maßnahmen, die der Schutzbedürftigkeit der verarbeiteten Daten nach dem Schutzklassenkonzept angemessen sind, sicherzustellen, dass Eingaben, Veränderungen und Löschungen personenbezogener Daten protokolliert werden, um eine nachträgliche Prüfbarkeit und Nachvollziehbarkeit der Datenverarbeitung sicherzustellen. Bei Protokollierungen sind die Grundsätze der Erforderlichkeit, Zweckbindung und Datenminimierung zu beachten.

(2) Die Maßnahmen müssen geeignet sein, um Dateneingaben, -veränderungen oder -löschungen, die bei der bestimmungsgemäßen Nutzung des Cloud-Dienstes durch den Cloud-Nutzer wie bei administrativen Maßnahmen des Cloud-Anbieters erfolgen, jederzeit nachvollziehen können.

(3) Die dafür eingesetzten Maßnahmen, etwa Protokollierung der administrativen Aktivitäten und der Nutzer-Aktivitäten, müssen so gestaltet sein, dass die Nachvollziehbarkeit von Eingaben, Veränderungen und Löschungen im Regelfall auch bei technischen oder organisatorischen

Fehlern, einschließlich Bedienfehlern des Cloud-Anbieters oder seiner Mitarbeiter oder fahrlässige Handlungen des Cloud-Nutzers oder Dritter gewahrt bleibt. Gegen vorsätzliche Manipulationen an den Maßnahmen zur Nachvollziehbarkeit ist ein Mindestschutz vorzusehen, der diese Manipulationen erschwert.

Schutzklasse 2

(4) Es müssen die Kriterien von Schutzklasse 1 erfüllt werden.

(5) Gegen zu erwartende vorsätzliche Manipulationen der Protokollierungsinstanzen und gegen vorsätzlichen Zugriff auf oder Manipulationen von Protokollierungsdateien (Logs) durch Unbefugte ist ein Schutz vorzusehen, der zu erwartende Manipulationsversuche hinreichend und sicher ausschließt. Dazu gehören insbesondere ein hinreichender Schutz gegen bekannte Angriffsszenarien sowie Maßnahmen, durch die eine Manipulation im Regelfall (nachträglich) festgestellt werden kann.

Schutzklasse 3

(6) Es müssen die Kriterien von Schutzklasse 1 und Schutzklasse 2 erfüllt werden.

(7) Es muss sichergestellt sein, dass Manipulationen von Protokollierungsinstanzen und -dateien (Logs) hinreichend sicher ausgeschlossen sind. Dies schließt regelmäßig Maßnahmen zur aktiven Erkennung von Manipulationen ein. Jede Manipulation und möglichst auch jeder entsprechende Versuch müssen nachträglich festgestellt werden können.

Erläuterung

Das Kriterium der Nachvollziehbarkeit konkretisiert in Teilen die in Art. 32 Abs. 1 lit. b und Abs. 2 DSGVO enthaltene, in hohem Maße konkretisierungsbedürftige Pflicht, die Gewährleistungsziele Integrität, Vertraulichkeit und Verfügbarkeit (SDM 6.2.1 – 6.2.3) von personenbezogenen Daten und Diensten auf Dauer sicherzustellen und personenbezogene Daten gegen unbeabsichtigte oder unrechtmäßige Vernichtung, Verlust, Veränderung, unbefugten Zugang oder unbefugte Offenlegung zu schützen. Hierzu muss nachträglich überprüft und festgestellt werden können, ob, wann und von wem und mit welchen inhaltlichen Auswirkungen personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, um gegebenenfalls Zugriffsrechte für die Zukunft anders zu gestalten. Die Protokolldaten müssen sicher aufbewahrt werden, damit sie als Nachweis zur Verfügung stehen. Zusätzlich ist zu beachten, dass die Auswertbarkeit der Protokolldaten sichergestellt ist.

Da im Rahmen von Protokollierungen regelmäßig personenbezogene Daten anfallen, unterliegt der Umgang mit Protokollierungsdaten ebenfalls datenschutzrechtlichen Anforderungen. Auf die Datenschutzgrundsätze aus Art. 5 DSGVO wird Bezug genommen. Auf das Gewährleistungsziel der Datenminimierung und der Zweckbindung aus Art. 5 Abs. 1 lit. c und b DSGVO ist besonderes Augenmerk zu legen.

Nr. 2.7 – Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO)

Kriterium

Schutzklasse 1

(1) Der Cloud-Anbieter bietet selbst keinen Pseudonymisierungsdienst an, ermöglicht es dem Cloud-Nutzer jedoch, die von pseudonymisierten Daten zu verarbeiten.

Schutzklasse 2

(2) Der Cloud-Anbieter hat sicherzustellen, dass die Daten pseudonymisiert verarbeitet werden. Entsprechend der rechtsverbindlichen Vereinbarung (Nr. 1.7) pseudonymisiert der Cloud-Nutzer die personenbezogenen Daten selbst oder der Cloud-Anbieter führt die Pseudonymisierung auf Weisung des Cloud-Nutzers durch.

(3) Wird die Pseudonymisierung vom Cloud-Anbieter durchgeführt, so stellt dieser sicher, dass die zusätzlichen Informationen zur Identifizierung der betroffenen Person gesondert aufbe-

wahrt werden und TOM unterliegen, sodass nur der Cloud-Nutzer Zugang zum Datensatz mit den Identifizierungsdaten hat.

(4) Der Datensatz mit der Zuordnung des Kennzeichens zu einer Person muss so geschützt werden, dass zu erwartende Manipulationsversuche hinreichend und sicher ausgeschlossen werden.

(5) Der Cloud-Anbieter gewährleistet darüber hinaus, dass er die technische Entwicklung im Bereich der Pseudonymisierungsverfahren laufend verfolgt und seine Verfahren den aktuellen technischen Empfehlungen (best practice) entsprechen.

Schutzklasse 3

(6) Der Cloud-Anbieter verfügt über einen Cloud-Dienst, der die Verarbeitung durch den Cloud-Nutzer pseudonymisierter Daten ermöglicht.

(7) Der Cloud-Anbieter hat keinen Zugang zu den Identifizierungsdaten.

Erläuterung

Die Pseudonymisierung wird neben der Verschlüsselung in Art. 32 Abs. 1 lit. a DSGVO explizit als einzusetzende Sicherheitsmaßnahme benannt. Sie trägt dazu bei, das Gewährleistungsziel der Nichtverkettung (SDM 6.2.4) zu fördern. Da durch Pseudonymisierung Dritte selbst bei einem unbefugten Zugriff auf den Cloud-Dienst keine Kenntnis von den personenbezogenen Daten erlangen können oder der Personenbezug zumindest erheblich erschwert wird, mindert die Pseudonymisierung die Risiken für die Grundrechte und Grundfreiheiten der betroffenen Personen.

Nr. 2.8– Anonymisierung (Art. 5 Abs. 1 lit. c DSGVO)

Kriterium

Schutzklasse 1

(1) Der Cloud-Anbieter bietet selbst keine Anonymisierung an, ermöglicht es dem Cloud-Nutzer jedoch, die von ihm anonymisierten Daten zu verarbeiten.

Schutzklasse 2 und 3

(2) Soweit mit dem Cloud-Nutzer vereinbart (Nr. 1.7), stellt der Cloud-Anbieter sicher, dass die Daten anonymisiert verarbeitet werden. Entsprechend der rechtsverbindlichen Vereinbarung anonymisiert der Cloud-Nutzer die personenbezogenen Daten selbst oder der Cloud-Anbieter auf Weisung.

(3) Wird die Anonymisierung vom Cloud-Anbieter durchgeführt, so gewährleistet der Cloud-Anbieter, dass er die technische Entwicklung im Bereich der Anonymisierungsverfahren laufend verfolgt und seine Verfahren den aktuellen technischen Empfehlungen (best practice) entsprechen. Die Anonymisierung muss nach dem Stand der Technik eine Re-Identifizierung der betroffenen Person ausschließen.

Erläuterung

Die Anonymisierung ist neben dem Verzicht der Datenerhebung die wirksamste Maßnahme zur Datenvermeidung und Datenminimierung. Sie trägt dazu bei, das Gewährleistungsziel der Datenminimierung (SDM 7.1) zu fördern.

Nr. 2.9 – Verschlüsselung gespeicherter Daten (Art. 32 Abs. 1 lit. a DSGVO)

Kriterium

Schutzklasse 1

(1) Der Cloud-Anbieter ist nicht verpflichtet, selbst Verschlüsselungsverfahren für die verschlüsselte Speicherung von Daten anzubieten, jedoch muss er dem Cloud-Nutzer die verschlüssel-

te Speicherung von Daten ermöglichen und die technische Entwicklung im Bereich der Verschlüsselung verfolgen.

Schutzklasse 2

(2) Der Cloud-Anbieter bietet Verschlüsselungsverfahren an, um dem Cloud-Nutzer die verschlüsselte Speicherung von Daten zu ermöglichen oder auf dessen Weisung hin, die Daten selbst zu verschlüsseln.

(3) Der Cloud-Anbieter verfolgt laufend die technische Entwicklung im Bereich der Verschlüsselung. Die von ihm getroffenen Maßnahmen entsprechen den aktuellen technischen Empfehlungen (best practice).

(4) Die Geeignetheit der Maßnahmen muss fortdauernd geprüft und die Maßnahmen müssen gegebenenfalls aktualisiert werden.

(5) Die angemessene Implementierung der Maßnahmen überprüft der Cloud-Anbieter durch geeignete Tests und dokumentiert diese.

Schutzklasse 3

(6) Personenbezogene Daten der Schutzklasse 3 werden vom Cloud-Nutzer verschlüsselt. Die Schlüssel werden bei diesem sicher aufbewahrt. Der Cloud-Anbieter unterstützt den Cloud-Nutzer bei der Verschlüsslung und Entschlüsselung der Daten, ohne den Schlüssel kennen zu können.

(7) Der Cloud-Anbieter verfolgt die technische Entwicklung im Bereich der Verschlüsselung und hält seine unterstützenden Maßnahmen auf dem Stand der aktuellen technischen Empfehlungen (best practice).

Erläuterung

Die Verschlüsselung wird neben der Pseudonymisierung in Art. 32 Abs. 1 lit. a DSGVO explizit als eine einzusetzende Sicherheitsmaßnahme benannt. Zweck der Verschlüsselung ist es, die Gewährleistungsziele der Vertraulichkeit und Integrität (SDM 6.2.2 und 6.2.2) sicherzustellen. Die Schwelle, ab der zu verschlüsseln ist, ist niedrig, sodass personenbezogene Daten bereits bei niedrigem Risiko verschlüsselt werden sollten, soweit dies möglich ist.

Nr. 2.10 – Getrennte Verarbeitung (Art. 5 Abs. 1 lit. b i.V.m. Art. 24, 25, 32 Abs. 1 lit. b und Abs. 2)

Kriterium

Schutzklasse 1

(1) Der Cloud-Anbieter stellt durch risikoangemessene TOM sicher, dass die Daten des Cloud-Nutzers von den Datenbeständen anderer Cloud-Nutzer und von anderen Datenbeständen des Cloud-Anbieters logisch oder physisch getrennt verarbeitet werden und dass der Cloud-Nutzer die Datenverarbeitung nach verschiedenen Verarbeitungszwecken trennen kann, um die Daten vor unbefugtem Zugang, Veränderungen und Vernichtung zu schützen und eine Verkettung der Daten zu verhindern (sichere Mandantentrennung).

(2) Die Maßnahmen müssen so gestaltet sein, dass die Datentrennung im Regelfall auch bei technischen oder organisatorischen Fehlern, einschließlich Bedienfehlern, des Cloud-Anbieters oder seiner Mitarbeiter oder fahrlässiger Handlungen des Cloud-Nutzers oder Dritter gewahrt bleibt. Es ist ein Mindestschutz vorzusehen, der vorsätzliche Verstöße gegen das Trennungsgebot verhindert.

Schutzklasse 2

(3) Es müssen die Kriterien von Schutzklasse 1 erfüllt werden.

(4) Der Cloud-Anbieter gewährleistet, dass gegen zu erwartende vorsätzliche Verstöße ein Schutz besteht, der diese hinreichend sicher ausschließt. Dazu gehören im Rahmen der Datenspeicherung die Verschlüsselung mit individuellen Schlüsseln und die Verwendung ge-

trennter Betriebsumgebungen für verschiedene Verarbeitungen oder der Einsatz gleichwertiger Verfahren. Weiterhin sind Maßnahmen zu ergreifen, durch die vorsätzliche Verstöße gegen das Trennungsgebot im Regelfall (nachträglich) festgestellt werden können, z.B. durch Protokollierung der Zugriffe.

Schutzklasse 3

(5) Es müssen die Kriterien von Schutzklasse 1 und Schutzklasse 2 erfüllt werden.

(6) Der Cloud-Anbieter stellt sicher, dass eine Verletzung der Datentrennung hinreichend sicher ausgeschlossen ist. Dazu gehören im Rahmen der Datenspeicherung die Verschlüsselung mit getrennten Schlüsseln und die Verwendung getrennter Betriebsumgebungen für verschiedene Verarbeitungen. Es ist zudem ein Verfahren zur Erkennung von vorsätzlichen Verstößen gegen die getrennte Verarbeitung vorzusehen.

Erläuterung

Das Kriterium fördert das Gewährleistungsziel der Verfügbarkeit, Integrität, Vertraulichkeit und Nichtverkettung (SDM 6.2.1 – 6.2.4) und zielt damit auch auf die Sicherstellung des Zweckbindungsgrundsatzes aus Art. 5 Abs. 1 lit. b DSGVO.

Hinsichtlich der Trennung der Datenverarbeitung nach verschiedenen Verarbeitungszwecken ist zu beachten, dass der Cloud-Anbieter lediglich die technische Möglichkeit der getrennten Verarbeitung bieten muss, während die Umsetzung der getrennten Datenverarbeitung nach Verarbeitungszwecken dem Cloud-Nutzer obliegt.

Nr. 2.11 – Wiederherstellbarkeit nach physischem oder technischem Zwischenfall (Art. 32 Abs. 1 lit. c DSGVO)

Kriterium

(1) Der Cloud-Anbieter gewährleistet durch risikoangemessene TOM, dass die Daten innerhalb der in der rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung angegebenen Zeiten wiederhergestellt werden können. Hierbei wird zwischen einer normalen, hohen und sehr hohen Wiederherstellbarkeit unterschieden:

Normale Wiederherstellbarkeit

Es ist ein Schutz zu gewährleisten, der gegen zu erwartende, naheliegende Ereignisse so zuverlässig absichert, dass diese Risiken bei normalem Verlauf nicht zu endgültigem Datenverlust führen. „Zu erwartend, naheliegend“ sind Ereignisse, die nicht vorkommen sollen, nach der Lebenserfahrung aber trotz hinreichender Vorsicht nicht ausgeschlossen werden können und „immer wieder einmal“ vorkommen, wie etwa Unfälle im Straßenverkehr oder der technische Defekt von Hardware.

Hohe Wiederherstellbarkeit

Es ist ein Schutz zu gewährleisten, der gegen seltene Ereignisse so zuverlässig absichert, dass diese Risiken bei normalem Verlauf der Datenverarbeitung nicht zu endgültigem Datenverlust führen. „Selten“ sind Ereignisse, die nicht vorkommen sollen und nach der Lebenserfahrung bei hinreichender Vorsicht „praktisch nie“ vorkommen, aber gleichwohl in einigen Fällen zu beobachten sind, wie etwa „Jahrhunderthochwasser“ oder gezielte, umfangreiche Angriffe auf den Cloud-Dienst oder ein plötzlich erhöhtes Zugriffsvolumen.

Sehr hohe Widerherstellbarkeit

Es ist ein hoher Schutz zu gewährleisten, der außergewöhnliche, aber nicht als theoretisch auszuschließende Ereignisse so zuverlässig absichert, dass diese Risiken bei normalem Verlauf der Datenverarbeitung nicht zu endgültigem Datenverlust führen. „Außergewöhnlich, aber nicht als theoretisch auszuschließen“ sind Ereignisse, die nicht vorkommen sollen und nach der Lebenserfahrung nicht auftreten, aber gleichwohl in extrem seltenen Einzelfällen zu beobachten sind, wie etwa „Black Swan“-Ereignisse oder ein unkontrollierbarer Blitzeinschlag ins Rechenzentrum.

(2) Der Cloud-Anbieter stellt dem Cloud-Nutzer sein Konzept der geeigneten TOM auf Anfrage zur Verfügung.

Erläuterung

Das Kriterium fördert das Gewährleistungsziel der Verfügbarkeit (SDM 6.2.1). Gemäß Art. 32 Abs. 1 lit. c DSGVO muss die Wiederherstellung „rasch“ erfolgen. Was als „rasch“ gilt, hängt auch von der Schwere des Zwischenfalls und der Bedeutung der Systeme und Daten ab. Der Cloud-Nutzer muss wählen können, welcher Wiederherstellungszeitraum ihm ausreicht. Z.B. sind an die Wiederherstellbarkeit der Daten im Krankenhaus strengere Anforderungen zu stellen als an die im Datenarchiv.

Da die Verfügbarkeit von personenbezogenen Daten nicht notwendigerweise mit ihrer Schutzbedürftigkeit nach dem Schutzklassenkonzept zusammenfallen muss, sondern auf der Seite des Cloud-Nutzers auch das Erfordernis bestehen kann, dass personenbezogene Daten der Schutzklasse 1 nach einem physischen oder technischen Zwischenfall sehr schnell wiederhergestellt sein müssen, wird bei diesem Kriterium nicht nach Schutzklassen unterschieden. Stattdessen wird die Möglichkeit der Wiederherstellung in den Wiederherstellbarkeitsniveaus „normale Widerherstellbarkeit“, „hohe Wiederherstellbarkeit“ und „sehr hohe Wiederherstellbarkeit“ ausgedrückt. Für eine Differenzierung spricht auch, dass es bei der Wiederherstellung nach einem physischen oder technischen Zwischenfall nicht wie bei den anderen Kriterien der Nummer 2 um den Normalbetrieb geht, sondern um physische oder technische Störfälle.

Als Ereignisse gelten Naturereignisse, Störungen der Infrastruktur sowie Betriebsstörungen, Bedienungsfehler oder vorsätzliche Eingriffe.

Nr. 3 – Weisungsbefolgungspflicht des Cloud-Anbieters

Nr. 3.1 – Sicherstellung der Weisungsbefolgung (Art. 28 Abs. 3 Satz 2 lit. a; 29 DSGVO)

Kriterium

Schutzklasse 1

(1) Der Cloud-Anbieter führt die Datenverarbeitung im Auftrag ausschließlich auf dokumentierte Weisung des Cloud-Nutzers aus.

(2) Der Cloud-Anbieter gewährleistet durch risikoangemessene Maßnahmen, dass die Verarbeitung der Daten des Cloud-Nutzers nur nach Maßgabe der Weisungen des Cloud-Nutzers erfolgt. Die Maßnahmen müssen geeignet sein, um im Regelfall Abweichungen von den Weisungen aufgrund technischer oder organisatorischer Fehler, einschließlich Bedienfehler, des Cloud-Anbieters oder seiner Mitarbeiter oder fahrlässiger Handlungen des Cloud-Nutzers oder Dritter auszuschließen. Gegen vorsätzliche Manipulationen von Weisungen ist ein Mindestschutz vorzusehen, der diese erschwert.

(3) Sollte der Cloud-Anbieter einen Subauftragsverarbeiter heranziehen, hat er sicherzustellen, dass auch der Subauftragsverarbeiter und seine Mitarbeiter die Datenverarbeitung ausschließlich gemäß der Weisung des Cloud-Nutzers ausführen.

(4) Im Rahmen von standardisierten Massengeschäften gewährleistet der Cloud-Anbieter die Einhaltung einer konkreten und nachvollziehbaren Dienstbeschreibung zu den von ihm technisch ausführbaren Dienstleistungen, sodass der Cloud-Nutzer den Cloud-Anbieter durch seine Auswahl für eine Auftragsverarbeitung anweisen kann. Zudem ermöglicht er dem Cloud-Nutzer, Weisungen mittels Softwarebefehlen zu erteilen, die automatisiert ausgeführt und dokumentiert werden.

Schutzklasse 2

(5) Es müssen die Kriterien von Schutzklasse 1 erfüllt werden.

(6) Die Maßnahmen müssen ein Abweichen von den Weisungen durch zu erwartende vorsätzliche Eingriffe hinreichend sicher ausschließen und sicherstellen, dass Eingriffe im Regelfall (nachträglich) festgestellt werden können.

Schutzklasse 3

(7) Es müssen die Kriterien von Schutzklasse 1 und Schutzklasse 2 erfüllt werden.

(8) Es muss sichergestellt sein, dass Abweichungen von den Weisungen des Cloud-Nutzers hinreichend sicher ausgeschlossen sind. Dies schließt regelmäßig eine umfassende Protokollierung von Administratorenzugriffen ein sowie Maßnahmen, die Eingriffe in die zu verarbeitenden Daten und Datenverarbeitungsvorgänge, abweichend von den Weisungen des Nutzers, auch durch Administratoren erheblich erschweren.

Nr. 4 – Hinweispflicht des Cloud-Anbieters

Nr. 4.1 – Weisungen entgegen datenschutzrechtlicher Vorschriften (Art. 28 Abs. 3 Satz 3 i.V.m Art. 29)

Kriterium

(1) Der Cloud-Anbieter informiert den Cloud-Nutzer unverzüglich, wenn er der Ansicht ist, dass eine Weisung des Cloud-Nutzers gegen datenschutzrechtliche Vorschriften verstößt.

Erläuterung

Die Verantwortung für die Konformität einer Weisung mit dem geltenden Datenschutzrecht liegt beim Cloud-Nutzer. Dennoch darf der Cloud-Anbieter eine Weisung, deren Rechtmäßigkeit er bezweifelt, nicht unbesehen ausführen. Vielmehr muss er den Cloud-Nutzer warnen, wenn er Zweifel an der Vereinbarkeit einer Weisung mit dem geltenden Datenschutzrecht hat, und die Entscheidung des Cloud-Nutzers abwarten.

Nr. 4.2 – Änderungen des Datenverarbeitungsortes (indirekt Art. 28 Abs. 3 Satz 2 lit. a DSGVO)

Kriterium

(1) Der Cloud-Anbieter richtet Maßnahmen ein, um sicherzustellen, dass er den Cloud-Nutzer unverzüglich in jenen Fällen informiert, in denen sich während des Vereinbarungszeitraums der Ort der Datenerarbeitung gegenüber dem in der Vereinbarung festgelegten (Nr. 1.5) aus Gründen ändert, die im Verantwortungsbereich des Cloud-Anbieters liegen oder für beide Parteien unvorhersehbar sind.

Erläuterung

-

Nr. 5 – Vertraulichkeitspflicht des Cloud-Anbieters

Nr. 5.1 – Sicherstellung der Vertraulichkeit beim Personal (Art. 28 Abs. 3 Satz 2 lit. b DSGVO)

Kriterium

(1) Der Cloud-Anbieter richtet ein organisatorisches Verfahren ein, um sicherzustellen, dass die zur Verarbeitung von personenbezogenen Daten befugten Personen vor Aufnahme der datenverarbeitenden Tätigkeit zur Vertraulichkeit gemäß der Vereinbarung zur Auftragsverarbeitung (Nr. 1.6) verpflichtet werden, sofern sie nicht bereits einer angemessenen vergleichbaren gesetzlichen Verschwiegenheitspflicht unterliegen.

(2) Das organisatorische Verfahren umfasst auch die Dokumentation der Verpflichtungserklärungen sowie ihre Anpassungen, wenn sich Zugriffs- und Verarbeitungsbefugnisse ändern.

Erläuterung

Die Verpflichtung zur Vertraulichkeit und die Belehrung zur Verschwiegenheit fördern das Gewährleistungsziel der Vertraulichkeit (SDM 6.2.3)

Nr. 6 – Unterstützung des Cloud-Nutzers bei der Wahrung der Betroffenenrechte

Erläuterung

Für die Erfüllung der Rechte der betroffenen Personen ist der Cloud-Nutzer als Verantwortlicher zuständig. Soweit ihm dies aber nicht selbst möglich ist, muss ihn der Cloud-Anbieter als Auftragsverarbeiter unterstützen. Für diesen Fall muss er eine Kontaktstelle für den Cloud-Nutzer vorhalten, die durch angemessene Erreichbarkeit und Befugnisse eine unverzügliche Umsetzung von Betroffenenrechten veranlassen kann.

Nr. 6.1 – Auskunftserteilung (Art. 28 Abs. 3 lit. e i.V.m. Art. 15)

Kriterium

(1) Der Cloud-Anbieter stellt sicher, dass der Cloud-Nutzer die Möglichkeit hat, betroffenen Personen Auskunft über die Datenverarbeitung zu erteilen und ihnen eine Kopie der personenbezogenen Daten zur Verfügung zu stellen oder dies durch den Cloud-Anbieter vornehmen zu lassen.

(2) Der Cloud-Anbieter hat Weisungen zur Umsetzung der Betroffenenrechte zu dokumentieren.

(3) Der Cloud-Anbieter ist von der Auskunftserteilung in jenen Fällen entbunden, in denen der Verantwortungsbereich beim Cloud-Nutzer liegt und dieser über Anwendungen und Dateien bestimmt.

Erläuterung

Der Cloud-Nutzer ist nach Art. 15 DSGVO verpflichtet, der betroffenen Person auf Antrag Auskunft über eine Datenverarbeitung und ihre Umstände zu erteilen. Der Cloud-Anbieter hat den Cloud-Nutzer durch geeignete TOM bei der Erfüllung der Rechte betroffener Personen zu unterstützen. Dieses Kriterium fördert die Gewährleistungsziele der Transparenz und der Intervenierbarkeit (SDM 6.2.5 und 6.2.6).

Nr. 6.2 – Berichtigung und Vervollständigung (Art. 28 Abs. 3 lit. e i.V.m. Art. 16)

Kriterium

(1) Der Cloud-Anbieter stellt durch geeignete Maßnahmen sicher, dass der Cloud-Nutzer die Möglichkeit hat, die Berichtigung und Vervollständigung personenbezogener Daten selbst vorzunehmen oder durch den Cloud-Anbieter vornehmen zu lassen.

(2) Der Cloud-Anbieter hat Weisungen zur Umsetzung der Betroffenenrechte zu dokumentieren.

(3) Der Cloud-Anbieter ist von der Berichtigung und Vervollständigung in jenen Fällen entbunden, in denen der Verantwortungsbereich beim Cloud-Nutzer liegt und dieser über Anwendungen und Dateien bestimmt.

Erläuterung

Der Cloud-Nutzer ist nach Art. 16 DSGVO verpflichtet, auf Antrag unrichtige personenbezogene Daten zu berichtigen und unvollständige personenbezogene Daten zu vervollständigen. Der Cloud-Anbieter ist verpflichtet, den Cloud-Nutzer durch geeignete TOM bei der Erfüllung der Rechte betroffener Personen zu unterstützen. Die Berichtigung gemäß Art. 16 DSGVO fördert das Gewährleistungsziel der Intervenierbarkeit (SDM 6.2.6).

Nr. 6.3 – Löschung

(Art. 28 Abs. 3 lit. e i.V.m. Art. 17 Abs. 1)

Kriterium

(1) Der Cloud-Anbieter stellt sicher, dass der Cloud-Nutzer die Möglichkeit hat, die Löschung personenbezogener Daten selbst vorzunehmen oder durch den Cloud-Anbieter vornehmen zu lassen.

(2) Der Cloud-Anbieter hat Weisungen zur Umsetzung der Betroffenenrechte zu dokumentieren.

(3) Der Cloud-Anbieter ist von der Löschung in jenen Fällen entbunden, in denen der Verantwortungsbereich beim Cloud-Nutzer liegt und dieser über Anwendungen und Dateien bestimmt.

Erläuterung

Der Cloud-Nutzer ist nach Art. 17 Abs. 1 DSGVO verpflichtet, personenbezogene Daten zu löschen. Der Cloud-Anbieter ist verpflichtet, den Cloud-Nutzer durch geeignete TOM bei der Erfüllung der Rechte betroffener Personen zu unterstützen. Das Kriterium fördert die Gewährleistungsziele der Intervenierbarkeit und Nichtverkettung (SDM 6.2.4 und 6.2.6).

Nr. 6.4 – Einschränkung der Verarbeitung
(Art. 28 Abs. 3 lit. e i.V.m. Art. 18 Abs. 1)

Kriterium

(1) Der Cloud-Anbieter stellt sicher, dass der Cloud-Nutzer die Möglichkeit hat, die Verarbeitung personenbezogener Daten selbst einzuschränken oder die Einschränkung durch den Cloud-Anbieter vornehmen zu lassen.

(2) Der Cloud-Anbieter hat Weisungen zur Umsetzung der Betroffenenrechte zu dokumentieren.

(3) Der Cloud-Anbieter ist von der Einschränkung der Verarbeitung in jenen Fällen entbunden, in denen der Verantwortungsbereich beim Cloud-Nutzer liegt und dieser über Anwendungen und Dateien bestimmt.

Erläuterung

Der Cloud-Nutzer ist nach Art. 18 Abs. 1 DSGVO verpflichtet, die Verarbeitung personenbezogener Daten unter bestimmten Voraussetzungen einzuschränken. Der Cloud-Anbieter ist verpflichtet, den Cloud-Nutzer durch geeignete TOM bei der Erfüllung der Rechte betroffener Personen zu unterstützen. Das Kriterium fördert das Gewährleistungsziel der Intervenierbarkeit (SDM 6.2.6).

Nr. 6.5 – Mitteilungspflicht bei Berichtung, Löschung oder Einschränkung der Verarbeitung
(Art. 28 Abs. 3 lit. e i.V.m. Art. 19)

Kriterium

(1) Der Cloud-Anbieter stellt sicher, dass der Cloud-Nutzer die Möglichkeit hat, Empfängern, denen er personenbezogene Daten offengelegt hat, jede Berichtigung, Löschung oder Einschränkung der Verarbeitung mitzuteilen oder die Mitteilung durch den Cloud-Anbieter vornehmen zu lassen, sowie die betroffene Person auf Verlangen über die Empfänger zu unterrichten.

(2) Der Cloud-Anbieter hat Weisungen zur Umsetzung der Betroffenenrechte zu dokumentieren.

(3) Der Cloud-Anbieter ist von der Mitteilungspflicht in jenen Fällen entbunden, in denen der Verantwortungsbereich beim Cloud-Nutzer liegt und dieser über Anwendungen und Dateien bestimmt.

Erläuterung

Der Cloud-Nutzer ist nach Art. 19 DSGVO verpflichtet, Empfängern, denen er personenbezogene Daten offengelegt hat, jede Berichtigung, Löschung oder Einschränkung der Verarbeitung mitzuteilen

und die betroffene Person auf Verlangen über die Empfänger zu unterrichten. Soweit der Cloud-Anbieter an der Offenlegung beteiligt war, ist er verpflichtet, den Cloud-Nutzer durch geeignete TOM bei der Erfüllung der Rechte betroffener Personen zu unterstützen. Das Kriterium fördert die Gewährleistungsziele der Transparenz und der Intervenierbarkeit (SDM 6.2.5 und 6.2.6).

Nr. 6.6 – Datenübertragung (Art. 28 Abs. 3 lit. e i.V.m. Art. 20 Abs. 1 und 2)

Kriterium

(1) Der Cloud-Anbieter stellt sicher, dass der Cloud-Nutzer die Möglichkeit hat, die von einer betroffenen Person bereitgestellten personenbezogenen Daten dieser Person oder einem anderen Verantwortlichen in einem strukturierten, gängigen und maschinenlesbaren Format zu übermitteln oder durch den Cloud-Anbieter übermitteln zu lassen.

(2) Der Cloud-Anbieter kann die ihm möglichen gängigen Formate in der rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung festhalten.

(3) Der Cloud-Anbieter hat Weisungen zur Umsetzung der Betroffenenrechte zu dokumentieren.

(4) Der Cloud-Anbieter ist von der Datenübertragung in jenen Fällen entbunden, in denen der Verantwortungsbereich beim Cloud-Nutzer liegt und dieser über Anwendungen und Dateien bestimmt.

Erläuterung

Der Cloud-Nutzer ist nach Art. 20 Abs. 1 und 2 DSGVO verpflichtet, auf Wunsch der betroffenen Person ihr oder einem anderen Verantwortlichen ihre bereitgestellten personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu übermitteln. Der Cloud-Anbieter ist verpflichtet, den Cloud-Nutzer durch geeignete TOM bei der Erfüllung der Rechte betroffener Personen zu unterstützen. Das Kriterium fördert das Gewährleistungsziel der Intervenierbarkeit (SDM 6.2.6).

Nr. 6.7 – Widerspruch (Art. 28 Abs. 3 lit. e i.V.m. Art. 21 Abs. 1 und Art. 32 Abs. 1 lit. b)

Kriterium

(1) Der Cloud-Anbieter stellt sicher, dass er dem Cloud-Nutzer alle Daten zur Verfügung stellt, die erforderlich sind, damit dieser beurteilen kann, ob das Widerspruchsrecht der betroffenen Person wirksam ausgeübt worden ist.

(2) Ist der Widerspruch gegen die Datenverarbeitung wirksam, stellt der Cloud-Anbieter im Rahmen seiner Möglichkeiten sicher, dass die Daten nicht mehr verarbeitet werden können.

(3) Der Cloud-Anbieter hat Weisungen zur Umsetzung der Betroffenenrechte zu dokumentieren.

(4) Ausgenommen sind die Fälle, in denen der Verantwortungsbereich beim Cloud-Nutzer liegt und dieser über Anwendungen und Dateien bestimmt.

Erläuterung

Der betroffenen Person steht entsprechend Art. 21 DSGVO das Recht zu, Widerspruch gegen eine Verarbeitung ihrer Daten einzulegen. Hat die betroffene Person das Widerspruchsrecht wirksam ausgeübt, ist der Cloud-Nutzer verpflichtet, die Verarbeitung der betroffenen personenbezogenen Daten für die Zukunft zu unterlassen. Der Cloud-Anbieter ist verpflichtet, den Cloud-Nutzer durch geeignete TOM bei der Erfüllung der Rechte betroffener Personen zu unterstützen. Das Kriterium fördert das Gewährleistungsziel der Intervenierbarkeit (SDM 6.2.6).

Nr. 7 – Unterstützung des Cloud-Nutzers bei der Datenschutz-Folgenabschätzung

Nr. 7.1 – Datenschutz-Folgenabschätzung (Art. 28 Abs. 3 lit. f i.V.m. Art. 35 und 36 DSGVO)

Kriterium

(1) Der Cloud-Anbieter unterstützt den Cloud-Nutzer bei der Durchführung seiner Datenschutzfolgenabschätzung.

(2) Ist dem Cloud-Anbieter durch eine vorher beim Cloud-Nutzer durchgeführte Datenschutzfolgenabschätzung das hohe Risiko der Verarbeitung bekannt, hat der Cloud-Anbieter risikoangemessene Vorkehrungen bereitzuhalten.

(3) Der Cloud-Anbieter stellt dem Cloud-Nutzer alle Informationen zur Verfügung, die in seinen Verantwortungsbereich fallen und die der Cloud-Nutzer für seine Datenschutz-Folgenabschätzung benötigt.

(4) Der Cloud-Anbieter unterstützt den Cloud-Nutzer bei der Bewältigung der Risiken der durch den Cloud-Nutzer geplanten Abhilfemaßnahmen, die z.B. Sicherheitsvorkehrungen und sonstige Verfahren enthalten und der Sicherstellung des Schutzes von personenbezogenen Daten dienen.

Erläuterung

Soweit der Cloud-Nutzer zu einer Datenschutz-Folgenabschätzung verpflichtet ist, hat ihn der Cloud-Anbieter durch Informationen, Analysen und Schutzmaßnahmen zu unterstützen.

Kapitel III: Datenschutz-Managementsystem des Cloud-Anbieters

Erläuterung

Der Cloud-Anbieter muss seine Datenschutzmaßnahmen in einem Datenschutz-Managementsystem organisieren. Die Einrichtung eines Datenschutz-Managementsystems indizieren die Art. 24 und 25, 32, 33, 34 sowie 37 bis 39 DSGVO. Die Sicherstellung eines Datenschutz-Managementsystems sollte der fortwährenden Sicherstellung des Datenschutzniveaus des zertifizierten Cloud-Dienstes dienen.

Nr. 8 – Datenschutz-Managementsystem

Nr. 8.1 – Benennung, Stellung und Aufgaben eines Datenschutzbeauftragten (Art. 37-39 DSGVO, § 38 BDSG)

Kriterium

(1) Der Cloud-Anbieter benennt einen Datenschutzbeauftragten (DSB) auf Grund seiner beruflichen Qualifikation und insbesondere seines Fachwissens, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie auf Grundlage seiner Fähigkeit zur Erfüllung der in Art. 39 DSGVO genannten Aufgaben.

(2) Der Cloud-Anbieter stellt sicher, dass der DSB unmittelbar der höchsten Managementebene berichtet.

(3) Der Cloud-Anbieter stellt sicher, dass der DSB bei der Erfüllung seiner Aufgaben keine Anweisungen bezüglich der Ausübung dieser Aufgaben erhält.

(4) Der Cloud-Anbieter stellt sicher, dass der DSB ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden wird.

(5) Der Cloud-Anbieter stellt die Anerkennung der Person und Funktion des DSB im Organisationsgefüge sicher und unterstützt ihn bei seinen Aufgaben, insbesondere mit angemessenen Ressourcen.

(6) Der Cloud-Anbieter stellt sicher, dass der DSB seinen Aufgaben nach Art. 39 Abs. 1 DSGVO im angemessenen Umfang nachkommt.

(7) Für den Fall, dass ein Beauftragter für Informationssicherheit benannt wird, muss dieser die Einhaltung der datenschutzrechtlich gebotenen TOM sicherstellen. Im Fall einer Personalunion des DSB mit dem Beauftragten für Informationssicherheit müssen beide Positionen klar definiert und dokumentiert werden. Werden beide Positionen nicht in Personalunion benannt, stellt der Cloud-Anbieter sicher, dass der DSB und der Beauftragte für Informationssicherheit in angemessener Weise kooperieren (gegenseitige Information und Unterstützung).

Erläuterung

Sofern Cloud-Anbieter die Pflicht haben, einen DSB zu benennen, müssen sie ihn sorgfältig auswählen, ausstatten, schützen und ihm in der Betriebsorganisation einen gebührenden Platz zuweisen.

Die Benennung eines Beauftragten für Informationssicherheit wird durch die Datenschutz-Grundverordnung nicht verlangt. Der Cloud-Anbieter kann jedoch aufgrund anderweitiger Verpflichtungen zur Benennung verpflichtet sein oder die Benennung freiwillig vornehmen.

Nr. 8.2 – Meldung von Datenschutzverletzungen (Art. 33 Abs. 2 und Art. 28 Abs. 3 lit. f)

Kriterium

(1) Der Cloud-Anbieter stellt durch geeignete Maßnahmen sicher, dass er dem Cloud-Nutzer Datenschutzverletzungen und deren Ausmaß unverzüglich meldet.

(2) Um eine unverzügliche Mitteilung zu ermöglichen, muss festgelegt werden, wer zuständig ist, über die Mitteilung an den Cloud-Nutzer zu entscheiden und diese vorzunehmen. Die zuständigen Stellen müssen für Mitarbeiter und Subauftragsverarbeiter in einer Weise erreichbar sein, dass Mitteilungen über etwaige Verstöße zeitnah entgegengenommen und bearbeitet werden können.

(3) Die zuständigen Stellen müssen über ausreichend Ressourcen verfügen, um eine rasche Bearbeitung von Meldungen sicher zu stellen. Die Mitarbeiter in den zuständigen Stellen müssen ausreichend geschult sein, um Verstöße beurteilen und eine Folgeabschätzung durchführen zu können.

Erläuterung

Der Cloud-Anbieter ist zur unverzüglichen Meldung von Datenschutzverstößen an den Cloud-Nutzer verpflichtet, damit dieser seiner Meldepflicht an die Aufsichtsbehörde und seiner Unterrichtungspflicht gegenüber den betroffenen Personen aus Art. 34 Abs. 1 DSGVO nachkommen kann. Diese Pflicht bezieht sich auch auf Verstöße von Subauftragnehmern in der gesamten Subauftragsverarbeiterkette. Das Kriterium fördert das Gewährleistungsziel der Integrität und Transparenz (SDM 6.2.2 und 6.2.5).

Nr. 8.3 – Führen eines Verarbeitungsverzeichnisses (Art. 30 Abs. 2 DSGVO)

Kriterium

(1) Cloud-Anbieter, die mehr als 250 Mitarbeiter beschäftigen, führen ein Verarbeitungsverzeichnis. Der Cloud-Anbieter hat unabhängig von der Beschäftigtenzahl ein Verarbeitungsverzeichnis zu führen, wenn die Verarbeitung für die betroffenen Personen mit Risiken für ihre Rechte und Freiheiten verbunden ist.

(2) Im Verzeichnis hat der Cloud-Anbieter alle Kategorien von im Auftrag eines Verantwortlichen durchzuführende Verarbeitungsvorgänge aufzuführen. Das Verzeichnis enthält außerdem die in Art. 30 Abs. 2 DSGVO aufgelisteten Inhalte.

(3) Für jeden einzelnen Cloud-Nutzer ist jeweils ein eigenes Verarbeitungsverzeichnis zu führen.

(4) Das Verarbeitungsverzeichnis ist schriftlich oder in einem elektronischen Format zu führen. Es ist der Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen.

Erläuterung

Das Kriterium fördert das Gewährleistungsziel der Transparenz (SDM 6.2.5).

Risikobehaftet ist ein Verarbeitungsvorgang i.S.d. Art. 30 Abs. 2 DSGVO, wenn er Risiken für die Rechte und Freiheiten von betroffenen Personen birgt oder besondere Kategorien von personenbezogenen Daten gemäß Art. 9 DSGVO oder Art. 10 DSGVO zum Gegenstand hat. Auch Cloud-Anbieter mit weniger als 250 Mitarbeitern werden in der Regel ein Verarbeitungsverzeichnis führen müssen, da sich bereits aus der Menge der verarbeiteten Daten Risiken ergeben und die Datenverarbeitung nicht nur gelegentlich erfolgt, sodass die Ausnahme aus Art. 30 Abs. 5 DSGVO im Regelfall nicht anwendbar ist.

Nr. 8.4 – Rückgabe von Datenträgern und Löschung von Daten (Art. 28 Abs. 3 lit. h DSGVO)

Kriterium

(1) Der Cloud-Anbieter stellt durch geeignete Maßnahmen sicher, dass die Rückgabe überlassener Datenträger, die Rückführung von Daten und die Löschung der beim Cloud-Anbieter gespeicherten Daten nach Abschluss der Auftragsverarbeitung oder nach Weisung des Cloud-Nutzers erfolgen.

Nr. 8.5 – Einrichtung eines internen Kontrollsystems (Art. 24 DSGVO)

Kriterium

(1) Der Cloud-Anbieter stellt sicher, dass die Umsetzung aller in diesem Katalog geprüften Kriterien regelmäßig in einem internen Revisionsverfahren überprüft wird. Hierfür legt der Cloud-Anbieter Kontrollverfahren und Zuständigkeiten fest.

(2) Der Cloud-Anbieter stellt durch geeignete TOM sicher, dass bei der (Weiter-)Entwicklung oder Änderung des Cloud-Dienstes die in diesem Katalog geprüften Kriterien weiterhin eingehalten werden.

Erläuterungen

Der Cloud-Anbieter hat sicherzustellen, dass die Maßnahmen zur Erfüllung der datenschutzrechtlichen Pflichten nach diesem Katalog nicht nur einmalig implementiert werden, sondern während der Gültigkeit eines Zertifikats aufrechterhalten werden.

Nr. 8.6 – Auswahl und Einsatz geeigneter Personen (Art. 28 Abs. 3 Satz 2 lit. e und f DSGVO)

Kriterium

(1) Der Cloud-Anbieter stellt sicher, dass er nur Mitarbeiter für die Durchführung von Verarbeitungsvorgängen betraut, die fachlich für die Erfüllung ihrer jeweiligen Aufgaben befähigt sind, die nötige Zuverlässigkeit aufweisen und sowohl im Datenschutz als auch in der Datensicherheit sensibilisiert und geschult sind.

(2) Der Cloud-Anbieter stellt sicher, dass bei den Mitarbeitern keine Interessenkonflikte hinsichtlich der Ausübung ihrer jeweiligen Aufgaben bestehen.

Erläuterungen

Der Einsatz geeigneter Mitarbeiter ist die Voraussetzungen dafür, dass der Cloud-Anbieter seinen zahlreichen Pflichten überhaupt nachkommen kann. Das Kriterium steht zudem in enger Verbindung mit dem Kriterium Nr. 8.1, da der DSB für die Sensibilisierung und Schulung von an Verarbeitungsvorgängen beteiligten Mitarbeitern zuständig ist und die diesbezüglichen Überprüfungen vornimmt.

Kapitel IV: Datenschutz durch Systemgestaltung

Nr. 9 – Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

Nr. 9.1 – Datenschutz durch Systemgestaltung (Art. 25 Abs. 1 DSGVO i.V.m. Art. 5 Abs. 1 lit. f DSGVO)

Kriterium

(1) Der Cloud-Anbieter stellt im Rahmen des angebotenen Dienstes sicher, dass er bei der Auftragsverarbeitung die Grundsätze des Art. 5 DSGVO (Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz, Zweckfestlegung und Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Systemdatenschutz und Verantwortlichkeit) möglichst praktikabel und zielführend umsetzt.

(2) Der Cloud-Anbieter verfügt über Prozesse zur Transparenz und zur aktiven Verfolgung des Stands der Technik, sowohl auf den Ebenen der konzeptionellen Zielsetzung, der Architektur, der Systemgestaltung als auch der der Implementierung.

(3) Der Cloud-Anbieter stellt sicher, dass zu jedem Zeitpunkt durch seine Systemgestaltung in den angebotenen Anwendungen und durch die Konzeption der Dienstleistung die Nachvollziehbarkeit und Transparenz der Datenverarbeitungen, auch in den verlängerten Leistungsketten durch etwaige Subauftragsverhältnisse, gewährleistet ist.

Erläuterung

Der Cloud-Nutzer muss als Verantwortlicher die Gestaltungspflicht aus Art. 25 Abs. 1 DSGVO erfüllen. Sobald er einen Cloud-Dienst nutzt, muss er einen Cloud-Anbieter auswählen, der diese Pflicht erfüllt. Technik und Organisation des Cloud-Dienstes sind daher so zu gestalten, dass sie die Datenschutzgrundsätze des Art. 5 DSGVO bestmöglich unterstützen.

Nr. 9.2 – Datenschutz durch Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Kriterium

(1) Der Cloud-Anbieter stellt durch seine Entwicklung und Voreinstellungen im jeweiligen Dienst sicher, dass der Zugang zu den personenbezogenen Daten auf das Maß beschränkt wird, das erforderlich ist, um den Verarbeitungszweck des Cloud-Nutzers zu erfüllen.

(2) Der Cloud-Anbieter muss durch Entwicklung und Voreinstellungen sicherstellen, dass personenbezogene Daten nicht ohne Eingreifen der betroffenen Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden und hierbei keine Risiken für die betroffenen Personen durch eine zu umfassende Zugänglichmachung von personenbezogenen Daten entstehen.

Erläuterung

Der Verantwortliche muss die Pflichten aus Art. 25 Abs. 2 DSGVO erfüllen. Sobald er eine Datenverarbeitung im Auftrag ausführen lässt, muss der Cloud-Nutzer einen Cloud-Anbieter auswählen, der diese Pflichten erfüllt. Die Voreinstellungen des Cloud-Dienstes sind daher so zu wählen, dass sie die Pflicht des Art. 25 Abs. 2 Satz 1 DSGVO erfüllen.

Kapitel V: Subauftragsverarbeitung

Erläuterung

Für die Auftragsverarbeitung gilt grundsätzlich das Prinzip der höchstpersönlichen Leistungserbringung. Unter bestimmten Voraussetzungen kann der Cloud-Anbieter weitere Subauftragsverarbeiter in Anspruch nehmen. Soweit auch Subauftragsverarbeiter ihrerseits auf Subauftragsverarbeiter zugreifen, ergeben sich mehrstufige Unterauftragsverhältnisse.

Der Cloud-Anbieter als Hauptauftragsverarbeiter hat allerdings dafür Sorge zu tragen, dass auf allen Stufen die Kriterien der Auftragsverarbeitung von allen Subauftragsverarbeitern eingehalten werden, da nur er gegenüber dem Cloud-Nutzer durchgängig für die Auftragsausführung verantwortlich bleibt.

Nr. 10 – Subauftragsverhältnisse

Nr. 10.1 – Weitere Auftragsverarbeiter des Cloud-Anbieters (Subauftragsverarbeitung) (Art. 28 Abs. 2 DSGVO)

Kriterium

(1) Der Cloud-Anbieter stellt sicher, dass ein Cloud-Dienst unter Einbeziehung von Subauftragsverarbeitern nur dann erbracht wird, wenn und soweit der Cloud-Nutzer vorher in diese Subauftragsverarbeitung in Schrift- oder Textform eingewilligt hat. Zustimmungsbedürftig sind nur solche Subaufträge, bei denen der weitere Auftragsverarbeiter eine Möglichkeit hat, die zu verarbeitenden personenbezogenen Daten zur Kenntnis zu nehmen.

(2) Der Cloud-Anbieter stellt sicher, dass auch der Subauftragsverarbeiter alle TOM im Rahmen seiner Auftragsverarbeitung gewährleistet und alle Pflichten erfüllt, die auch der Cloud-Anbieter als Hauptauftragsverarbeiter erfüllen muss, soweit er hiervon nicht gesetzlich befreit ist. Der Subauftragsverarbeiter muss dieselben Garantien nachweisen können wie der Hauptauftragsverarbeiter.

Erläuterung

Die Qualitätssicherung und die Einhaltung des Datenschutzes in der Leistungskette sind durch den Cloud-Anbieter zu gewährleisten. Insbesondere darf der Subauftrag nicht dazu führen, dass die Wahrung der Betroffenenrechte erschwert wird.

Nr. 10.2 – Rechtsverbindliche Vereinbarung als Grundlage der Subauftragsverarbeitung (Art. 28 Abs. 4 DSGVO)

Kriterium

(1) Der Cloud-Anbieter stellt sicher, dass seine Subauftragsverarbeiter nur auf Grundlage einer rechtsverbindlichen Vereinbarung zur Subauftragsverarbeitung tätig werden, die mit der rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung zwischen dem Cloud-Anbieter und Cloud-Nutzer in Einklang steht.

(2) Der Cloud-Anbieter verpflichtet seine Subauftragsverarbeiter sicherzustellen, dass ihre Subauftragsverarbeiter ebenfalls auf Grundlage einer rechtsverbindlichen Vereinbarung zur Subauftragsverarbeitung tätig werden und auf ihre Sub-Subauftragsverarbeiter dieselbe Verpflichtung übertragen.

Nr. 10.3 – Information des Cloud-Nutzers (Art. 28 Abs. 2 Satz 2 DSGVO)

Kriterium

(1) Der Cloud-Anbieter informiert den Cloud-Nutzer über die Identität aller von ihm eingeschalteten Subauftragsverarbeiter auf allen Stufen (einschließlich ladungsfähiger Anschrift).

(2) Der Cloud-Anbieter informiert den Cloud-Nutzer immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Subauftragsverarbeiter und gewährleistet, dass der Cloud-Nutzer auf jeder Stufe der Auftragsverarbeitung Gebrauch von seinem Einspruchsrecht machen kann.

Erläuterung

Dem Cloud-Nutzer muss zu jedem Zeitpunkt der Auftragsverarbeitung möglich sein zu erfahren, welcher Subauftragsverarbeiter sich in welchem Verarbeitungsschritt befindet und welche Anwendungen und Dienste in Bezug auf personenbezogene Daten durch welchen Subauftragsverarbeiter auf welcher Stufe der Auftragsverarbeitung ausgeführt werden.

Nr. 10.4 – Auswahl und Kontrolle der Subauftragsverarbeiter (Art. 28 Abs. 4 Satz 1 DSGVO)

Kriterium

(1) Der Cloud-Anbieter stellt sicher, dass auf allen Stufen nur solche Subauftragsverarbeiter in die Auftragsverarbeitung einbezogen werden, die die Gewähr für die Einhaltung der datenschutzrechtlichen Anforderungen an die von ihnen zu erbringende Leistung bieten.

(2) Der Cloud-Anbieter überzeugt sich davon, dass seine Subauftragsverarbeiter die datenschutzrechtlichen Anforderungen an die von ihnen zu erbringende Leistung erfüllen.

Nr. 10.5 – Gewährleistung der Unterstützungsfunktionen (Art. 28 Abs. 4 Satz 1 i.V.m. Art. 28 Abs. 3 Satz 2 DSGVO)

Kriterium

(1) Der Cloud-Anbieter stellt zu jedem Stadium der Auftragsverarbeitung sicher, dass durch die Einschaltung von (mehreren) Subauftragsverarbeitern seine Unterstützungsfunktionen im vereinbarten Umfang sowie seine Pflichten als Hauptauftragsverarbeiter erfüllt werden.

(2) Der Cloud-Anbieter stellt durch geeignete Verfahren und Vorkehrungen sicher, dass die Verlängerung der Leistungskette in der Auftragsverarbeitung nicht zur Minderung der Achtung von datenschutzrechtlichen Standards und Verpflichtungen führt.

Kapitel VI: Auftragsverarbeitung außerhalb der EU und des EWR

Nr. 11 – Datenübermittlung

Nr. 11.1 – Geeignete Garantien für die Datenübermittlung (Art. 46 Abs. 2 lit. f i.V.m. Art. 42 Abs. 1 und 2 DSGVO)

Kriterium

(1) Der Cloud-Anbieter übermittelt personenbezogene Daten in Drittstaaten oder an internationale Organisationen nur, sofern für den Empfängerstaat oder die internationale Organisation ein Beschluss der Europäischen Kommission nach Art. 45 Abs. 3 DSGVO vorliegt, dass dort ein angemessenes Datenschutzniveau gilt.

(2) Alternativ kann die Übermittlung stattfinden, wenn der Empfänger geeignete Garantien im Sinne des Art. 46 Abs. 2 DSGVO vorweist und den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe in dem Drittstaat oder gegenüber der Internationalen Organisation zur Verfügung stehen. Geeignete Garantien sind auch bei einem Zertifikat nach Art. 42 Abs. 2 DSGVO gegeben, wenn außerdem rechtsverbindliche und durchsetzbare Verpflichtungen des Cloud-Anbieters in dem Drittstaat bestehen, geeignete Garantien, einschließlich in Bezug auf die Rechte der betroffenen Personen, anzuwenden.

Erläuterung

Auftragsverarbeitungen sind außerhalb der EU und des EWR nur unter den in Art. 44 ff. DSGVO genannten Voraussetzungen zulässig. Das Gleiche gilt für die Übermittlung von personenbezogenen Daten in ein EU-Drittland oder an eine Internationale Organisation, für die kein angemessenes Datenschutzniveau anerkannt ist.

Nr. 11.2 – Vertreterbenennung (Art. 27 i.V.m. Art. 3 Abs. 2 DSGVO)

Kriterium

(1) Der Cloud-Anbieter, der nicht in der EU niedergelassen ist, für den die Datenschutz-Grundverordnung aber dennoch nach Art. 3 Abs. 2 DSGVO gilt, hat einen Vertreter in der EU schriftlich zu benennen.

(2) Der Cloud-Anbieter beauftragt den Vertreter, zusätzlich zum ihm oder an seiner Stelle insbesondere für Aufsichtsbehörden und betroffene Personen bei sämtlichen Fragen im Zusammenhang mit der Verarbeitung zur Gewährleistung der Einhaltung der DSGVO als Anlaufstelle zu dienen.

Erläuterung

Der Vertreter muss in einem der Mitgliedstaaten niedergelassen sein, in denen sich die betroffenen Personen befinden, deren personenbezogene Daten im Zusammenhang mit den ihnen angebotenen Waren oder Dienstleistungen verarbeitet werden oder deren Verhalten beobachtet wird (Art. 27 Abs. 3 DSGVO).

European Cloud Service
Data Protection Certification

Umsetzungshinweise und Nachweise zum AUDITOR-Kriterienkatalog

- Entwurfsfassung 0.8 -

Stand 15.10.2018

Beitrag zum Forschungsprojekt „European Cloud Service Data Protection Certification (AUDITOR)“, das aufgrund eines Beschlusses des Deutschen Bundestages vom Bundesministerium für Wirtschaft und Energie gefördert wird (FKZ 01MT17003A).

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

Autoren

Alexander Roßnagel[a], Ali Sunyaev[b], Sebastian Lins[b], Natalie Maier[a], Heiner Teigeler[b]

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

[b] Forschungsgruppe Critical Information Infrastructures im Institut für Angewandte Informatik und Formale Beschreibungsverfahren (AIFB) des Karlsruher Instituts für Technologie

Inhaltsverzeichnis

Abkürzungsverzeichnis

Abs.	Absatz
AGB	Allgemeine Geschäftsbedingungen
Art.	Artikel
BDSG n.F.	Bundesdatenschutzgesetz neue Fassung (Geltung ab 25.5.18)
DSB	Datenschutzbeauftragter
DSGVO	EU-Datenschutz-Grundverordnung (Geltung ab 25.5.18)
EG	Erwägungsgrund
EWR	Europäischer Wirtschaftsraum
i.S.v.	Im Sinne von
i.V.m.	In Verbindung mit
Lit.	Litera
Nr.	Nummer
SDM	Standard-Datenschutzmodell v.1.1 vom 26.4.2018
TCDP	Trusted Cloud Datenschutz-Profil
TOM	technische und organisatorische Maßnahmen
Ziff.	Ziffer

Hinweis zur geschlechtsneutralen Formulierung:

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

A. Leitfaden zum AUDITOR Kriterienkatalog

1. Einleitung

Der AUDITOR-Kriterienkatalog ist ein Prüfstandard für die Datenschutz-Zertifizierung von Cloud-Diensten gemäß den Anforderungen der EU-Datenschutz-Grundverordnung (DSGVO). Der Kriterienkatalog legt *„Kriterien“* fest, welche die normativen Anforderungen bezeichnen, die zu erfüllen sind, um ein Zertifikat auf der Grundlage des AUDITOR-Kriterienkatalogs zu erhalten.

Dieses Dokument umfasst die Umsetzungshinweise zum AUDITOR-Kriterienkatalog und ist gemäß der Gliederung der einzelnen Kriterien strukturiert. Die *„Umsetzungshinweise“* sollen exemplarische Leitlinien und Hilfestellungen für das Verständnis und die Umsetzung der Kriterien geben; sie selbst haben jedoch keinen verpflichtenden Charakter. Die *„Nachweise“* liefern die Antwort auf die Frage, wie das Vorliegen der Kriterien im konkreten Zertifizierungsverfahren erwiesen werden kann. Nachweise stellen analog zu den Umsetzungshinweisen exemplarische Leitlinien und informative Hilfestellungen dar, die Cloud-Anbieter, Zertifizierungsstellen, Prüfer und weitere Interessierte bei der Beurteilung der Einhaltung von Kriterien unterstützen sollen. Es besteht keine Verpflichtung, die Nachweise gemäß diesem Dokument zu erbringen.

B. Umsetzungshinweise und Nachweise

Kapitel I: rechtsverbindliche Vereinbarung zur Auftragsverarbeitung

Nr. 1 – Wirksame und eindeutige Grundlage zwischen Cloud-Anbieter und Cloud-Nutzer (Art. 28 Abs. 3 DSGVO)

Nr. 1.1 – Dienstleistung aufgrund einer rechtsverbindlichen Vereinbarung und Form der Vereinbarung (Art. 28 Abs. 3 Satz 1 und Abs. 9 DSGVO)

Umsetzungshinweis

Der Cloud-Anbieter trifft technische oder organisatorische Vorkehrungen, die einen automatischen Vereinbarungsschluss vor der eigentlichen Dienstnutzung sicherstellen. Hierzu kann dem potentiellen Cloud-Nutzer während der Registrierung eine entsprechende Vereinbarung angezeigt werden, die dieser vor der Dienstnutzung bestätigen muss.

Bei standardisierten Massengeschäften werden in der Regel, auch unter Unternehmern, vorformulierte Vertragsklauseln (Allgemeine Geschäftsbedingungen - AGB) eingesetzt, die wirksam im Sinne des jeweiligen AGB-Rechts zu sein haben.

Nachweis

Der Cloud-Anbieter kann im Rahmen der Zertifizierung alle oder eine repräsentative Stichprobe von rechtsverbindlichen Vereinbarungen vorlegen, die er mit den Cloud-Nutzern geschlossen hat. Außerdem kann er anhand einer geeigneten Dokumentation nachweisen, dass technische oder organisatorische Vorkehrungen getroffen wurden, welche eine Dienstnutzung erst nach Abschluss der Vereinbarung sicherstellen.

Nr. 1.2 – Gegenstand und Dauer der Verarbeitung (Art. 28 Abs. 3 Satz 1 DSGVO)

Umsetzungshinweis

Für beide Parteien sollte anhand dieser Eingrenzung des Auftragsgegenstandes klar hervorgehen, welche Verarbeitungsvorgänge oder Verarbeitungskategorien nach welcher Schutzklasse durch den Cloud-Anbieter für den Cloud-Nutzer durchgeführt werden. Insbesondere sollte in transparenter Form dargelegt werden, welche Einflussmöglichkeiten dem Cloud-Anbieter bei der Wahl der Verarbeitungsmittel zur Ausführung von Verarbeitungsvorgängen, in denen personenbezogene Daten verarbeitet werden, zukommen. Regelungen zum Gegenstand des Auftrags sollten auch die abgegrenzten Verantwortungsbereiche zwischen Cloud-Nutzer und Cloud-Anbieter abbilden.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er einen Entwurf einer rechtsverbindlichen Vereinbarung mit diesen Angaben vorhält und ein Verfahren implementiert hat, wonach die Vereinbarung mit diesen Festlegungen geschlossen wird.

Nr. 1.3 – Art und Zwecke der Datenverarbeitung (Art. 28 Abs. 3 Satz 1 DSGVO)

Umsetzungshinweis

Diese Einzelangaben müssen zwar nicht jeden konkreten Einzelfall abdecken, sollten jedoch so präzise sein, dass die im Rahmen der Auftragsverarbeitung zulässigen Datenverarbeitungsvorgänge im Einzelnen aus Sicht des Cloud-Nutzers nachvollzogen werden können.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er einen Entwurf einer rechtsverbindlichen Vereinbarung mit diesen Angaben vorhält und ein Verfahren implementiert hat, wonach die Vereinbarung mit diesen Festlegungen geschlossen wird.

Nr. 1.4 – Weisungsbefugnisse des Cloud-Nutzers (Art. 28 Abs. 3 Satz 2 lit. a DSGVO)

Umsetzungshinweis

Es sollte aus der rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung hervorgehen, wer zur Erteilung von Weisungen befugt ist und wer auf Seiten des Cloud-Anbieters mit der Entgegennahme der Weisungen betraut ist. Die zu Weisungen befugten Abteilungs- und Funktionsebenen können in der rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung benannt und deren Authentifizierungsmittel festgelegt werden.

Im der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung oder in vorformulierten Klauseln des Cloud-Anbieters sind die technisch ausführbaren Dienstleistungen und Weisungsbefugnisse des Cloud-Nutzers aufzuführen. Die rechtsverbindliche Vereinbarung sollte die Möglichkeiten darstellen, die dem Cloud-Nutzer zur Ausübung seiner Weisungsbefugnis eingeräumt werden. Diese können insbesondere auch in automatisierten Verfahren bestehen. Anhand einer (im Massengeschäft einseitig vorgegebenen) Dienstbeschreibung des Cloud-Anbieters sollen die potentiellen Cloud-Nutzer eine Auskunft für ihre Auswahl nach Art. 28 Abs. 1 DSGVO erhalten. In diesem Fall weist der Cloud-Nutzer durch die Auswahl des Cloud-Dienstes den Cloud-Anbieter an, die beschriebene, standardisierte Dienstleistung auszuführen.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er entsprechende Regelungen zur Weisungserteilung in rechtsverbindlichen Vereinbarungen offenlegt und vorhandene Dokumentationen von Einzelanweisungen vorzeigt.

Nr. 1.5 – Ort der Datenverarbeitung (indirekt Art. 28 Abs. 3 Satz 2 lit. a DSGVO)

Umsetzungshinweis

-

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er einen Entwurf einer rechtsverbindlichen Vereinbarung vorhält, in der er sich verpflichtet, den Cloud-Nutzer unverzüglich über Änderungen des Ortes der Datenverarbeitung zu informieren.

Nr. 1.6 – Verpflichtung zur Vertraulichkeit (Art. 28 Abs. 3 Satz 2 lit. b DSGVO)

Umsetzungshinweis

-

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er einen Entwurf einer rechtsverbindlichen Vereinbarung vorhält, in der er sich verpflichtet, Mitarbeiter, die zur Verarbeitung von personenbezogenen Daten befugten sind, vor Aufnahme der datenverarbeitenden Tätigkeit zur Vertraulichkeit zu verpflichten, sofern sie nicht bereits einer angemessenen vergleichbaren gesetzlichen Verschwiegenheitspflicht unterliegen.

Nr. 1.7 – Technisch-organisatorische Maßnahmen, Unterbeauftragung und Unterstützung (Art. 28 Abs. 3 Satz 2 lit. c bis f i.V.m. Kap. III und Art. 32 – 36 DSGVO)

Umsetzungshinweis

Angaben zur Umsetzung der Kriterien unter Nr. 2 können an Gewährleistungszielen ausgerichtet werden, während die konkreten Maßnahmen der Zielerreichung dem Cloud-Anbieter überlassen werden können. Für den Cloud-Nutzer ist es wichtig zu wissen, welcher Schutzanforderungsklasse der Cloud-Dienst entspricht.

Die Vorgaben des Art. 28 Abs. 3 Satz 2 lit. d DSGVO sollten in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung präzisiert werden, so dass ihre Einhaltung für den Cloud-Nutzer leicht überprüfbar ist.

Da dem Cloud-Nutzer bei Änderungen in der Unterbeauftragung ein Einspruchsrecht zusteht (Nr. 10.3), sollten in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung die Voraussetzungen und Folgen eines Einspruchs geregelt werden, bspw. ob der Cloud-Nutzer bei Einspruch die Vereinbarung aufkündigen darf.

Bei der Festlegung der Unterstützungspflichten des Cloud-Anbieters in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung sollen diese unter Berücksichtigung der Ausgestaltung des konkreten Cloud-Dienstes und der dem Cloud-Anbieter zumutbaren und geeigneten TOM konkretisiert werden. Damit sollen Unsicherheiten hinsichtlich der sich aus der Vereinbarung ergebenden Rechte und Pflichten vermieden werden.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er einen Entwurf einer rechtsverbindlichen Vereinbarung mit diesen Angaben vorhält und ein Verfahren implementiert hat, wonach die Vereinbarung mit diesen Festlegungen geschlossen wird.

Nr. 1.8 – Rückgabe von Datenträgern und Löschung von Daten (Art. 28 Abs. 3 Satz 2 lit. g DSGVO)

Umsetzungshinweis

Der Nachweis der Rückgabe von Datenträgern und der Löschung von Daten kann auch durch Verweis auf entsprechende Grundsätze des Cloud-Anbieters erfolgen. Der Cloud-Nutzer kann zwischen den Abwicklungsmodalitäten wählen. Die Pflichten des Cloud-Anbieters entfallen, wenn er eine Pflicht zur Speicherung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten hat. Die Umsetzungshinweise aus ISO/IEC 27040:2017-03 Ziff. 6.8.1 zur Datenlöschung sind anwendbar.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er einen Entwurf einer rechtsverbindlichen Vereinbarung mit diesen Festlegungen vorhält und ein Verfahren implementiert hat, wonach die Vereinbarung mit diesen Festlegungen geschlossen wird.

Kapitel II: Rechte und Pflichten des Cloud-Anbieters

Nr. 2 – Gewährleistung der Datensicherheit durch geeignete TOM nach dem Stand der Technik

Nr. 2.1 – Risiko- und Schutzkonzept (Art. 24, 25, 28, 32, 35 i.V.m. Art. 5 Abs. 1 lit. f DSGVO)

Umsetzungshinweis

Das Risiko- und Schutzkonzept soll die sich aus den spezifischen Umständen des Cloud-Dienstes, seiner Datenverarbeitungsvorgänge und Räumlichkeiten ergebenden Risiken abdecken und zu jedem Risiko eine oder gegebenenfalls mehrere Schutzmaßnahmen beinhalten sowie Ressourcen, Verantwortlichkeiten und Priorisierungen für den Umgang mit Informationssicherheitsrisiken spezifizieren. Alle identifizierten Restrisiken des Cloud-Dienstes, die nicht vollständig behandelt werden können, sollten von der Geschäftsleitung des Cloud-Anbieters zur Kenntnis genommen werden. Der Risikobewertungsansatz und die Risikobewertungsmethodik des Cloud-Anbieters sollten dokumentiert werden.

Bei der Analyse von Risiken können folgende Merkmale analysiert und evaluiert werden:

1) Evaluierung der Auswirkungen auf die Organisation, Technik oder Dienstbereitstellung aufgrund eines Sicherheitsausfalls und Berücksichtigung der Konsequenzen des Verlusts von Vertraulichkeit, Integrität oder Verfügbarkeit;

2) Evaluierung der realistischen Wahrscheinlichkeit eines solchen Sicherheitsausfalls unter Berücksichtigung aller denkbaren Bedrohungen und Sicherheitslücken;

3) Abschätzung des möglichen Schadensausmaßes für die Grundrechte und Freiheiten der betroffenen Personen;

4) Prüfung, ob alle möglichen Optionen für die Behandlung der Risiken identifiziert und evaluiert sind;

5) Bewertung, ob das verbleibende Risiko akzeptierbar oder eine Gegenmaßnahme erforderlich ist.

Das Risiko- und Schutzkonzept sollte unter Berücksichtigung neu auftretender Sicherheitsherausforderungen kontinuierlich aktualisiert und verbessert werden. Dabei sollten Risikobewertungen, das mögliche Schadensausmaß und die identifizierten akzeptablen Risiken regelmäßig unter Berücksichtigung des Wandels der Organisation, Technologie, Geschäftsziele und -prozesse, erkannten Bedrohungen, der Auswirkung der implementierten Kontrollen und externen Ereignisse überprüft werden.

Nachweis

Das Risiko- und Schutzkonzept und seine Angemessenheit kann der Cloud-Anbieter dadurch nachweisen, dass er dieses vorlegt.

Nr. 2.2 – Sicherheitsbereich und Zutrittskontrolle (Art. 32 Abs. 1 lit. b und Abs. 2 i.V.m. Art. 5 Abs. 1 lit. f DSGVO)

Umsetzungshinweis

Die Umsetzungshinweise aus ISO/IEC 27001 Ziff. A11 und ISO/IEC 27018 Ziff. 11 sind anwendbar.

Um sicherzustellen, dass Unbefugte keinen Zuritt zu Räumen und Datenverarbeitungsanlagen erhalten, sollte der Zutritt ins Rechenzentrum über Videoüberwachungssysteme, Bewegungssensoren, Alarmsysteme und von geschultem Sicherheitspersonal permanent überwacht werden.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er im Risiko- und Schutzkonzept die TOM zur Zutrittskontrolle darlegt.

Nr. 2.3 – Zugangskontrolle (Art. 32 Abs. 1 lit. b und Abs. 2 i.V.m. Art. 5 Abs. 1 lit. f DSGVO)

Umsetzungshinweis

Die Umsetzungshinweise aus ISO/IEC 27001 Ziff. A12.1.4, A12.4.2 und ISO/IEC 27018 Ziff. 9 sind anwendbar.

Die Aufgaben und Rollen zur Wahrung der Informationssicherheit für Datenverarbeitungsvorgänge des Cloud-Anbieters sollten klar definiert und verständlich dokumentiert sein. Alle Anlagen des Cloud-Anbieters sollten korrekt gewartet werden, damit ihre fortgesetzte Verfügbarkeit und Integrität gewährleistet werden können.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er im Risiko- und Schutzkonzept die TOM zur Zugangskontrolle darlegt.

Nr. 2.4 – Zugriffskontrolle (Art. 32 Abs. 1 lit. b und Abs. 2 i.V.m. Art. 5 Abs. 1 lit. f DSGVO)

Umsetzungshinweis

Die Umsetzungshinweise aus ISO/IEC 27002 Ziff. 13.2 und ISO/IEC 27018 Ziff. 9.2, 9.2.1, 9.4.2 sind anwendbar.

Berechtigungskonzepte müssen sowohl für die Nutzer des Dienstes als auch für die Mitarbeiter des Cloud-Anbieters bestehen. Ein geeigneter Managementprozess für die Zugriffskontrolle sollte etabliert werden, welcher die Erforderlichkeit der Berechtigungen in regelmäßigen Abständen auf Angemessenheit überprüft, die Vergabe, Aktualisierung, Kontrolle und den Entzug von Berechtigungen regelt, Zugriffspolitiken überwacht und aktualisiert sowie Passwortrichtlinien überprüft und die Einhaltung sicherstellt**.**

Es sollten angemessene Sicherheitsmaßnamen gegen sowohl interne auch gegen externe Angriffe implementiert werden, um einen unbefugten Zugriff zu verhindern. Hierzu zählen bspw. sämtliche Standardmaßnahmen für den Schutz des Cloud-Hosts, d. h. Host Firewalls, Network-Intrusion-Prevention-Systeme, Applikationsschutz, Antivirus, regelmäßige Integritätsüberprüfungen wichtiger Systemdateien und Host-based Intrusion-Detection-Systeme. Der Cloud-Dienst sollte 24/7 auf Angriffe und Sicherheitsvorfälle überwacht werden, um verdächtige Aktivitäten (bspw. Extraktion großer Datenmengen mehrerer Mandanten), Angriffe und Sicherheitsvorfälle rechtzeitig erkennen und angemessene und zeitnahe Reaktionen einleiten zu können.

Sämtliche relevanten Sicherheitsereignisse einschließlich aller Sicherheitslücken oder -vorfälle sollten erfasst, protokolliert, revisionssicher archiviert und ausgewertet werden. Ein handlungsfähiges Team für Security-Incident-Handling und Trouble-Shooting sollte 24/7 erreichbar sein, damit Sicherheitsvorfälle gemeldet und zeitnah bearbeitet werden können.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er im Risiko- und Schutzkonzept die TOM zur Zugriffskontrolle darlegt.

Nr. 2.5 – Übertragung von Daten und Transportverschlüsselung (Art. 32 Abs. 1 lit. b und Abs. 2 i.V.m. Art. 5 Abs. 1 lit. f DSGVO)

Umsetzungshinweis

Die Umsetzungshinweise aus ISO/IEC 27018 Ziff. 10.1.1, A.10.6, A.10.9, ISO/IEC 27002 Ziff. 12.4, ISO/IEC 27040:2017-03 Ziff. 6.7.1 und ISO/IEC 27040:2017-03 Ziff. 7.7.1 sind anwendbar.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er im Risiko- und Schutzkonzept die TOM zur Übertragungskontrolle darlegt.

Nr. 2.6– Nachvollziehbarkeit der Datenverarbeitung (Art. 32 Abs. 1 lit. b und Abs. 2 i.V.m. Art. 5 Abs. 1 lit. c, e und f DSGVO)

Umsetzungshinweis

Die Umsetzungshinweise aus ISO/IEC 27018 Ziff. 12.4.1, 12.4.2 und ISO/IEC 27002 Ziff. 12.4 sind anwendbar.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er im Risiko- und Schutzkonzept dokumentiert, wie er durch Festlegung von Gegenstand und Umfang der Protokollierung, Aufbewahrung und Verwendung der Protokolldaten, Integritätsschutz und Löschung von Protokollen, die Datenschutzziele sicherstellt.

Nr. 2.7 – Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO)

Umsetzungshinweis

Der Cloud-Nutzer hat zu prüfen, ob es bereichsspezifische oder generische technische Standards für die Pseudonymisierung gibt, die als verpflichtend vorgeschrieben sind oder empfohlen werden. Der Cloud-Anbieter sollte öffentlich bekannt geben, welche dieser technischen Standards sein Pseudonymisierungsverfahren erfüllt. Beispielsweise kann zur Pseudonymisierung in der medizinischen Informatik DIN EN ISO 25237 herangezogen werden.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er im Risiko- und Schutzkonzept dokumentiert, wie er selbst Pseudonymisierungen durchführt, Identifizierungsdaten sicher aufbewahrt und pseudonymisierte Daten verarbeitet.

Nr. 2.8 – Anonymisierung (Art. 5 Abs. 1 lit. c DSGVO)

Umsetzungshinweis

Der Cloud-Nutzer sollte prüfen, ob es bereichsspezifische technische Standards für die Anonymisierung gibt, die als verpflichtend vorgeschrieben sind oder empfohlen werden. Der Cloud-Anbieter sollte öffentlich bekannt geben, welche dieser technischen Standards sein Anonymisierungsverfahren erfüllt.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er im Risiko- und Schutzkonzept dokumentiert, wie er selbst Anonymisierungen durchführt und anonymisierte Daten verarbeitet.

Nr. 2.9 – Verschlüsselung gespeicherter Daten (Art. 32 Abs. 1 lit. a DSGVO)

Umsetzungshinweis

Der Stand der Technik ergibt sich aus aktuellen technischen Normen für kryptographische Verfahren und deren Anwendung. Die Umsetzungshinweise aus ISO/IEC 27018 Ziff. 10 und ISO/IEC 27002, Z. 10 sind anwendbar.

Soweit der Cloud-Anbieter Daten verschlüsselt, sollte die Schlüsselerzeugung in einer sicheren Umgebung und unter Einsatz geeigneter Schlüsselgeneratoren erfolgen. Kryptografische Schlüssel sollten möglichst nur für einen Einsatzzweck dienen und generell nie in klarer Form, sondern grundsätzlich verschlüsselt im System gespeichert werden. Die Speicherung muss stets redundant gesichert und wiederherstellbar sein, um einen Verlust eines Schlüssels auszuschließen. Schlüsselwechsel müssen regelmäßig durchgeführt werden. Der Zugang zum Schlüsselverwaltungssystem sollte eine separate Authentisierung erfordern. Cloud-Administratoren dürfen keinen Zugriff auf Kundenschlüssel haben.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er im Risiko- und Schutzkonzept dokumentiert, dass die angebotenen und angewandten Verschlüsselungsverfahren den aktuellen technischen Anforderungen entsprechen. Er legt Prozessdokumentationen vor, wie er die technische Entwicklung im Bereich der Verschlüsselung verfolgt und die Geeignetheit des Verfahrens fortdauernd prüft und es gegebenenfalls aktualisiert. Er weist in seinem Risiko- und Schutzkonzept nach, dass er bei Diensten der Schutzklasse 2 die Verschlüsselungstechniken durch geeignete technische Tests geprüft hat.

Nr. 2.10 – Getrennte Verarbeitung (Art. 5 Abs. 1 lit. b i.V.m. Art. 24, 25, 32 Abs. 1 lit. b und Abs. 2)

Umsetzungshinweis

Die Umsetzungshinweise aus ISO/IEC 27002 Ziff. 12.1.4, 13.1.3 sind anwendbar.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er im Risiko- und Schutzkonzept dokumentiert, welche TOM er ergriffen hat, um die Daten unterschiedlicher Nutzer voneinander zu trennen und die Daten eines Nutzers nach den Verarbeitungszwecken trennen zu können.

Nr. 2.11 – Wiederherstellbarkeit nach physischem oder technischem Zwischenfall (Art. 32 Abs. 1 lit. c DSGVO)

Umsetzungshinweis

Zur Wiederherstellung von Daten und Systemen sollte ein Cloud-Anbieter ein wirksames Datensicherungskonzept erstellen, in dem er Systeme zu Datensicherungen, ein Notfallmanagement, Pläne zur Wiederherstellung und zur Schadensbegrenzung sowie einen Plan zur regelmäßigen Überprüfung und Aktualisierung der vorgesehenen Maßnahmen vorsieht.

Es sollten regelmäßig Sicherheitskopien von Daten, Prozesszuständen, Konfigurationen, Datenstrukturen, Transaktionshistorien u. ä. gemäß einem Datensicherungskonzept angefertigt werden. Hierin sollten auch Aufbewahrungs- und Schutzanforderungen festgelegt werden. Für die Aufstellung eines Datensicherungskonzepts sind die Umsetzungshinweise aus ISO/IEC 27018 Ziff. 12.3.1, A.10.3 anwendbar.

Die Datensicherungsstrategien und -maßnahmen des Datensicherungskonzepts sollten für Cloud-Nutzer transparent definiert werden, sodass alle Informationen nachvollziehbar sind, einschließlich Umfang, Speicherintervallen, Speicherzeitpunkten und Speicherdauern.

Neben der Erstellung von Sicherheitskopien sollte der Cloud-Anbieter ein Notfallmanagement mit entsprechenden Notfallplänen etablieren. Dabei gilt es unter anderem, mögliche Unterbrechungen zu identifizieren und zu bewerten, sodass Pläne zur Wiederherstellung und Schadensbegrenzung entwickelt und im Notfall eingesetzt werden können. Die entwickelten Notfallpläne sind fortlaufend zu aktualisieren und auf ihre Wirksamkeit zu testen, um bei einem Eintritt einer Unterbrechung eine möglichst schnelle Reaktion sicherzustellen.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er im Risiko- und Schutzkonzept dokumentiert, mit welchen Ereignissen er sich auseinandergesetzt hat, die zu einem physischen, organisatorischen oder technischen Zwischenfall führen können, ob sein Cloud-Dienst normale, hohe oder sehr hohe Wiederherstellbarkeit gewährleistet und welche konkreten Maßnahmen zur Wiederherstellbarkeit der Daten nach einem Zwischenfall er ergriffen hat.

Nr. 3 – Weisungsbefolgungspflicht des Cloud-Anbieters

Nr. 3.1 – Sicherstellung der Weisungsbefolgung (Art. 28 Abs. 3 Satz 2 lit. a; 29 DSGVO)

Umsetzungshinweis

Des Cloud-Anbieter unterweist alle Mitarbeiter, deren Tätigkeiten im Zusammenhang mit der Verarbeitung von personenbezogenen Daten stehen, in die vertraglich dokumentierten Weisungen (Art. 29 DSGVO) und stellt auch in einer etwaigen Datenverarbeitungskette die Weisungsbefolgung sicher. Der Cloud-Anbieter hat regelmäßig zu kontrollieren, ob die Weisungen des Cloud-Nutzers eingehalten werden.

In der Praxis werden Weisungen des Cloud-Nutzers insbesondere mittels Softwarebefehlen automatisiert ausgeführt (z.B. durch Interaktion mit einer graphischen Benutzeroberfläche oder über Kommandozeileneingabe), weshalb diese Nutzerinteraktionen auch automatisiert protokolliert oder dokumentiert werden sollten.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er im Risiko- und Schutzkonzept dokumentiert, wie er Weisungen des Cloud-Nutzers empfängt, umsetzt und dokumentiert. Bei Massengeschäften erbringt der Cloud-Anbieter den Nachweis über seine konkrete Dienstbeschreibung zu seinen technisch ausführbaren Dienstleistungen und den Nachweis zur Ausführbarkeit von Weisungen durch Softwarebefehle in Form einer technischen Dokumentation oder durch Dienstnutzung.

Nr. 4 – Hinweispflicht des Cloud-Anbieters

Nr. 4.1 – Weisungen entgegen datenschutzrechtlicher Vorschriften (Art. 28 Abs. 3 Satz 3 i.V.m Art. 29)

Umsetzungshinweis

Bei der Aufnahme von Weisungen in die rechtsverbindliche Vereinbarung zur Auftragsverarbeitung und bei jeder nach deren Abschluss ergangenen Weisung sollte der Cloud-Anbieter seinen Datenschutzbeauftragten (DSB) konsultieren, wenn sich die Datenschutzwidrigkeit der Weisung einem datenschutzrechtlich geschulten Mitarbeiter des Cloud-Dienstes aufdrängt. Der Cloud-Anbieter hat keine Pflicht, eine Weisung ohne Anlass zu überprüfen.

Bei Massengeschäften, in denen der Cloud-Nutzer durch die Auswahl des Cloud-Dienstes aufgrund einer Dienstbeschreibung des Cloud-Anbieters die Weisung erteilt, hat der Cloud-Anbieter TOM zu treffen, durch die er den Cloud-Nutzer darauf hinweist, wenn dieser seinen Dienst datenschutzwidrig entgegen der Dienstbeschreibung nutzt (z.B. die vom Cloud-Anbieter zur Verfügung gestellten Datensicherungsmaßnahmen wie Verschlüsselung und Pseudonymisierung nicht nutzt).

Die Umsetzungshinweise aus ISO/IEC 27018 Ziff. 16.1.1 sind anwendbar.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, indem er dokumentiert, wie er Weisungen prüft, Zweifel an deren datenschutzrechtlicher Zulässigkeit erkennt und den Cloud-Nutzer vor Ausführung der Weisung darauf hinweist.

Nr. 4.2 – Änderungen des Datenverarbeitungsortes (indirekt Art. 28 Abs. 3 Satz 2 lit. a DSGVO)

Umsetzungshinweis

Bei Massengeschäften sollte ein Kommunikationsprozess, möglichst unterstützt durch ein automatisiertes Informationssystem innerhalb des Cloud-Dienstes, beispielsweise auf der Website des Cloud-Anbieters, eingerichtet werden, wodurch der Cloud-Nutzer bei Ortsänderungen die Möglichkeit der Kenntnisnahme vom Ort der Datenverarbeitung erhält.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er Maßnahmen und Zuständigkeiten dokumentiert, die er implementiert hat, um den Cloud-Nutzer bei Änderungen des Datenverarbeitungsortes zu informieren.

Nr. 5 – Vertraulichkeitspflicht des Cloud-Anbieters

Nr. 5.1 – Sicherstellung der Vertraulichkeit beim Personal (Art. 28 Abs. 3 Satz 2 lit. b DSGVO)

Umsetzungshinweis

Den Mitarbeitern des Cloud-Anbieters sollte der Cloud-Anbieter eine Ausfertigung des Verpflichtungstextes mitsamt den Hinweisen auf mögliche Folgen von Verschwiegenheitspflichtverletzungen aushändigen. Er sollte die Belehrung in angemessenen Abständen wiederholen, etwa im Zusammenhang mit Schulungen oder insbesondere bei Änderung der Zugriffs- und Verarbeitungskompetenz des jeweiligen Mitarbeiters. Außerdem sollte der Cloud-Anbieter die betroffenen Personen zu Fragen des Datenschutzes und der Datensicherheit in Bezug auf ihre Tätigkeit regelmäßig sensibilisieren.

In der Dokumentation des Verfahrens sollte er Festlegungen treffen, wer für die Vornahme der Belehrung und Verpflichtung verantwortlich ist, wer sie wann und in welcher Weise durchführt, welche Personen zu welchem Zeitpunkt verpflichtet und belehrt werden müssen und welcher Nachweis über die Verpflichtung und Belehrung wo und wie lange aufbewahrt wird.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er Belehrungen und Verpflichtungen sowie die zugehörigen Verfahren und Zuständigkeiten dokumentiert.

Nr. 6 – Unterstützung des Cloud-Nutzers bei der Wahrung der Betroffenenrechte

Nr. 6.1 – Auskunftserteilung (Art. 28 Abs. 3 lit. e i.V.m. Art. 15)

Umsetzungshinweis

Soweit dem Cloud-Nutzer eine Umsetzung der Betroffenenrechte nicht selbst möglich ist, sollte eine organisatorische Kontaktstelle für den Cloud-Nutzer vorgehalten werden, die durch angemessene Erreichbarkeit und Befugnisse eine unverzügliche Umsetzung von Betroffenenrechten veranlassen kann.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, indem er dokumentiert, welche Maßnahmen er ergriffen hat, um dem Cloud-Nutzer die Auskunftserteilung gegenüber einer betroffenen Person zu ermöglichen oder die Auskunft durch den Cloud-Anbieter erteilen zu lassen. Auch können anhand einer Prozessdokumentation die tatsächlich durchgeführten Auskunftserteilungen nachgewiesen werden.

Nr. 6.2 – Berichtigung und Vervollständigung (Art. 28 Abs. 3 lit. e i.V.m. Art. 16)

Umsetzungshinweis

Soweit dem Cloud-Nutzer eine Umsetzung der Betroffenenrechte nicht selbst möglich ist, sollte eine organisatorische Kontaktstelle für den Cloud-Nutzer vorgehalten werden, die durch angemessene Erreichbarkeit und Befugnisse eine unverzügliche Umsetzung von Betroffenenrechten veranlassen kann.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er dokumentiert, welche Maßnahmen er ergriffen hat, um dem Cloud-Nutzer die Berichtigung und Vervollständigung von Daten zu ermöglichen oder diese durch den Cloud-Anbieter vornehmen zu lassen. Auch können anhand einer

Prozessdokumentation die tatsächlich durchgeführten Berichtigungen und Vervollständigungen nachgewiesen werden.

Nr. 6.3 – Löschung (Art. 28 Abs. 3 lit. e i.V.m. Art. 17 Abs. 1)

Umsetzungshinweis

Die Erstellung eines Löschkonzepts, z.B. nach DIN 66398-2016, wird empfohlen. Dieses kann die Festlegung von Löschverfahren beinhalten, mit denen es dem Cloud-Nutzer ermöglicht wird, seinen Löschungspflichten nachzukommen. Dies sollte auch Backup- und Ausfallsicherungssysteme, einschließlich aller Vorgängerversionen der Daten, temporäre Dateien, Metadaten und Dateifragmente umfassen. Die Maßnahmen aus DIN 66398 zur Erstellung eines Löschkonzepts sowie DIN 66993 zur Vernichtung von Datenträgern können hinzugezogen werden.

Alle Datenträger des Cloud-Anbieters sollten durch den Einsatz eines formalen Managementverfahrens sicher und geschützt entsorgt werden, wenn sie nicht mehr benötigt werden.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er dokumentiert, welche Maßnahmen er ergriffen hat, um dem Cloud-Nutzer die Löschung von Daten zu ermöglichen oder diese durch den Cloud-Anbieter vornehmen zu lassen. Auch können anhand einer Prozessdokumentation die tatsächlich durchgeführten Löschungen nachgewiesen werden.

Nr. 6.4 – Einschränkung der Verarbeitung (Art. 28 Abs. 3 lit. e i.V.m. Art. 18 Abs. 1)

Umsetzungshinweis

Soweit dem Cloud-Nutzer eine Umsetzung der Betroffenenrechte nicht selbst möglich ist, sollte eine organisatorische Kontaktstelle für den Cloud-Nutzer vorgehalten werden, die durch angemessene Erreichbarkeit und Befugnisse eine unverzügliche Umsetzung von Betroffenenrechten veranlassen kann

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er dokumentiert, welche Maßnahmen er ergriffen hat, um dem Cloud-Nutzer die Einschränkung der Verarbeitung von Daten zu ermöglichen oder dies durch den Cloud-Anbieter vornehmen zu lassen.

Nr. 6.5 – Mitteilungspflicht bei Berichtung, Löschung oder Einschränkung der Verarbeitung (Art. 28 Abs. 3 lit. e i.V.m. Art. 19)

Umsetzungshinweis

Soweit dem Cloud-Nutzer eine Umsetzung der Betroffenenrechte nicht selbst möglich ist, sollte eine organisatorische Kontaktstelle für den Cloud-Nutzer vorgehalten werden, die durch angemessene Erreichbarkeit und Befugnisse eine unverzügliche Umsetzung von Betroffenenrechten veranlassen kann.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er dokumentiert, welche Maßnahmen er ergriffen hat, um es dem Cloud-Nutzer zu ermöglichen, Empfängern, denen er personenbezogene Daten offengelegt hat, jede Berichtigung, Löschung oder Einschränkung der Verarbeitung mitzuteilen und die betroffene Person auf Verlangen über die Empfänger zu unterrichten oder dies durch den Cloud-Anbieter vornehmen zu lassen.

Nr. 6.6 – Datenübertragung (Art. 28 Abs. 3 lit. e i.V.m. Art. 20 Abs. 1 und 2)

Umsetzungshinweis

Der Cloud-Anbieter sollte geeignete technische Funktionen innerhalb seines angebotenen Dienstes bereitstellen, die es ermöglichen, Daten in ein strukturiertes, gängiges und maschinenlesbares Format zu übertragen. Hierzu gehören z.B. Exportfunktionen in XML- oder JSON-Formate.

Soweit dem Cloud-Nutzer eine Umsetzung der Betroffenenrechte nicht selbst möglich ist, sollte eine organisatorische Kontaktstelle für den Cloud-Nutzer vorgehalten werden, die durch angemessene Erreichbarkeit und Befugnisse eine unverzügliche Umsetzung von Betroffenenrechten veranlassen kann.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er dokumentiert, welche Maßnahmen er ergriffen hat, um es dem Cloud-Nutzer zu ermöglichen, der betroffenen Person oder einem anderen Verantwortlichen die von dieser betroffenen Person bereitgestellten Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu übermitteln oder durch den Cloud-Anbieter übermitteln zu lassen.

Nr. 6.7 – Widerspruch (Art. 28 Abs. 3 lit. e i.V.m. Art. 21 Abs. 1 und Art. 32 Abs. 1 lit. b)

Umsetzungshinweis

Der Cloud-Anbieter sollte über ein Konzept verfügen, aus dem hervorgeht, durch welche Maßnahmen er sicherstellt, dass er dem Cloud-Nutzer alle erforderlichen Daten zur Verfügung stellen und die künftige Verarbeitung der Daten unterbinden kann.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er dokumentiert, welche Maßnahmen er implementiert hat, um dem Cloud-Nutzer die erforderlichen Daten zur Verfügung zu stellen.

Nr. 7 – Unterstützung des Cloud-Nutzers bei der Datenschutz-Folgenabschätzung

Nr. 7.1 – Datenschutz-Folgenabschätzung (Art. 28 Abs. 3 lit. f i.V.m. Art. 35 und 36 DSGVO)

Umsetzungshinweis

Die Unterstützungspflichten bei der Datenschutz-Folgenabschätzung sollten am Einflussbereich des Cloud-Anbieters ausgerichtet werden, etwa im Bereich der TOM zur Gewährleistung der Datensicherheit. Zur Einschätzung, ob ein oder welches Risiko bei den jeweiligen Datenverarbeitungsvorgängen des Cloud-Dienstes gegeben ist, können Datenflussmodelle und -analysen erstellt werden, wenn diese nicht bereits aus der Dienstbeschreibung des Cloud-Anbieters hervorgehen.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er dokumentiert, wie er den Cloud-Nutzer durch einschlägige Informationen unterstützen kann. Er sollte darlegen, dass diese Informationen vorliegen oder von ihm in kurzer Zeit generiert werden können.

Kapitel III: Datenschutz-Managementsystem des Cloud-Anbieters

Nr. 8 – Datenschutz-Managementsystem

Nr. 8.1 – Benennung, Stellung und Aufgaben eines Datenschutzbeauftragten (Art. 37-39 DSGVO, § 38 BDSG)

Umsetzungshinweis

Der Cloud-Anbieter sollte eine schriftliche Dokumentation der für den jeweiligen Cloud-Dienst eingesetzten Systeme, Verfahren und Prozesse (Software, Hardware, beteiligte Organisationseinheiten, Rollen und Dienstleister) und eine möglichst exakte Beschreibung der Gesamtheit der getroffenen TOM führen (z.B. in einem Risiko- und Datenschutzkonzept) und dem DSB sowie (auf Anfrage) der Aufsichtsbehörde zugänglich machen.

Ist der DSB bei einem anderen Unternehmen beschäftigt (externer DSB des Cloud-Anbieters) oder gleichzeitig DSB anderer Unternehmen, gilt seine Weisungsfreiheit auch gegenüber seinem Arbeitgeber und seinen anderen Auftraggebern. Die Anforderung der Abwesenheit von Interessenskonflikten ist primär eine Benennungsvoraussetzung und in sekundärer Hinsicht eine Organisationspflicht des Cloud-Anbieters. Der Cloud-Anbieter weist dem DSB keine zusätzlichen Aufgaben zu, die ihn in einen Interessenskonflikt bringen könnten. Interessenskonflikte sind im Rahmen folgender Tätigkeiten anzunehmen: Tätigkeiten, im Rahmen derer der DSB sich selbst kontrollieren müsste, z.B. Stellung als Geschäftsführer, IT- oder Personalabteilungsleiter, Informationssicherheitsbeauftragter, wirtschaftliche Interessen des DSB am Unternehmenserfolg, zu große Nähe zur benennenden Stelle.

Die Verschwiegenheitspflicht des DSB umfasst insbesondere die Identität des Beschwerdeführers oder der betroffenen Person(en), alle datenschutzrechtlich relevanten Informationen sowie alles, was zur Identifizierung eines Hinweisgebers führen könnte. Auch gegenüber der ihn benennenden Stelle ist der DSB zur umfassenden Verschwiegenheit verpflichtet. Das Kriterium fördert das Gewährleistungsziel der Vertraulichkeit (SDM 6.2.3).

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, indem er einen DSB benannt hat und durch Einträge auf seiner Webseite seine direkte Ansprechbarkeit der Öffentlichkeit vorstellt. Zur Beurteilung der fachlichen und persönlichen Eignung kann er einschlägige Zeugnisse und Beurteilungen vorlegen. Mit den regelmäßig durchzuführenden internen Audits des DSB kann der Nachweis über seine Tätigkeiten, seine Unabhängigkeit sowie seine Einbindung und Wirksamkeit im Organisationsgefüge des Cloud-Anbieters nachgewiesen werden.

Bei Personalunion zwischen DSB und Beauftragtem für Informationssicherheit kann der Cloud-Anbieter den Nachweis klar abgegrenzter Positionen durch Aufgabenbeschreibungen beider Positionen nachweisen.

Nr. 8.2 – Meldung von Datenschutzverletzungen (Art. 33 Abs. 2 und Art. 28 Abs. 3 lit. f)

Umsetzungshinweis

Die Meldung von Datenschutzverletzungen kann über geeignete Informationssysteme innerhalb des Dienstes bspw. über Nachrichtensysteme oder Newsmeldungen geschehen.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er in seinem Risiko- und Schutzkonzept dokumentiert, wie er die Meldung von Datenschutzverletzungen gewährleistet.

Nr. 8.3 – Führen eines Verarbeitungsverzeichnisses (Art. 30 Abs. 2 DSGVO)

Umsetzungshinweis

Das für jeden Cloud-Nutzer jeweils zu führende Verarbeitungsverzeichnis sollte auch die für jeden Cloud-Nutzer jeweils eingesetzten TOM zur Gewährleistung der Datensicherheit bei der Datenverarbeitung dokumentieren. Bei standardisierten Massengeschäften sollte das Verarbeitungsverzeichnis automatisiert erstellt werden.

Das Verfahrensverzeichnis kann für alle Dokumentationspflichten als Nachweis oder Nachweisbekräftigung herangezogen werden. Dieses Verzeichnis ist jedoch nicht öffentlich und richtet sich nicht an betroffene Personen, sondern ist ausschließlich nach innen und auf das Verhältnis zur Aufsichtsbehörde gerichtet. Der Cloud-Nutzer sollte, jedoch – etwa zur Auftragskontrolle nach Art. 28 Abs. 3 Satz 2 lit. h DSGVO – einen Einblick in das seinen Auftrag betreffende Verzeichnis erhalten.

Die Umsetzungshinweise aus ISO/IEC 27018 Ziff. A5.2 sind anwendbar.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, indem er die (eine repräsentative Stichprobe der) Verarbeitungsverzeichnisse vorlegt.

Nr. 8.4 – Rückgabe von Datenträgern und Löschung von Daten (Art. 28 Abs. 3 lit. h DSGVO)

Umsetzungshinweis

Auf ISO/ IEC 27018 Ziff. A 9.3. wird hingewiesen.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er dokumentiert, welches Verfahren er vorgesehen hat, nach dem er die Herausgabe der Datenträger, die Rückführung von Daten und die Löschung von Daten nach Beendigung des Auftrags durchführt. Auch kann er die Quittierung von Rückgaben oder die automatisierte Benachrichtigung über tatsächliche Löschungen der für die Auftragsverarbeitung nicht mehr benötigten personenbezogenen Daten vorlegen.

Nr. 8.5 – Einrichtung eines internen Kontrollsystems (Art. 24 DSGVO)

Umsetzungshinweis

Der Cloud-Anbieter sollte vor allem die internen Audits des DSB zu Datenschutzfragen heranziehen. Des Weiteren wird auf die Umsetzungshinweise zur regelmäßigen Überprüfung durch die oberste Leitung beim Cloud-Anbieter nach ISO/IEC 27002:2017-06, Ziff. 18.2. hingewiesen.

Der Cloud-Anbieter sollte die Wirksamkeit der internen Kontrollaktivitäten regelmäßig überprüfen. Dazu gilt es zunächst zu definieren, wie die Wirksamkeit der internen Kontrollaktivitäten gemessen werden kann. Es ist empfohlen ein standardisiertes Vorgehensmodell (z. B. ITIL oder COBIT) für die IT-Prozesse des angebotenen Cloud-Dienstes zu definieren und einzuhalten. Wird ein interner Prüfer/Auditor eingesetzt, sollte er über eine geeignete Qualifikation verfügen, objektiv und unparteiisch sein, und nicht an der Erstellung der Prüfobjekte beteiligt sein.

Bei der Bereitstellung eines Cloud-Dienstes sollten Prozesse für ein sicheres Änderungs- und Release-Management etabliert werden. Im Rahmen dieser Prozesse sollte ein Cloud-Anbieter u.a. eine dokumentierte Eignungsprüfung und einen Abnahmeprozess bei der (Weiter-)Entwicklung und Änderung (insb. Patches und System-Updates) an seinem Dienst durchführen, um nachteilige Auswirkungen aufgrund der Änderungen zu vermeiden und die Konformität zur Datenschutz-Grundverordnung fortlaufend sicherzustellen. Die Geltungsbereiche, Rollen und Verbindlichkeiten im Rahmen des Änderungs- und Release-Managements sollten zwischen Cloud-Anbieter und -Nutzer klar definiert und aufeinander abgestimmt sein.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er dokumentiert, welches interne Kontrollsystem er eingerichtet hat.

Nr. 8.6 – Auswahl und Einsatz geeigneter Personen (Art. 28 Abs. 3 Satz 2 lit. e und f DSGVO)

Umsetzungshinweis

Um die fachliche Kompetenz der Mitarbeiter zu erhalten, sollten regelmäßige Mitarbeiterschulungen (ca. 1 Mal pro Jahr) zu datenschutzrechtlichen und informationssicherheitstechnischen Themen durchgeführt werden. Zudem sollten Mitarbeiterschulungen zur konkreten Technik des Cloud-Dienstes durchgeführt werden, um sicherzustellen, dass Mitarbeiter alle eingesetzten Techniken, Komponenten und Funktionalitäten beherrschen.

Nachweis

Der Cloud-Anbieter kann den Nachweis der erforderlichen Fachkunde seiner Mitarbeiter durch einschlägige Qualifikationsnachweise erbringen. Sensibilisierungs- und Schulungsmaßnahmen von Mitarbeitern kann er durch die Dokumentation erfolgter Schulungen nachweisen.

Kapitel IV: Datenschutz durch Systemgestaltung

Nr. 9 – Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

Nr. 9.1 – Datenschutz durch Systemgestaltung (Art. 25 Abs. 1 DSGVO i.V.m. Art. 5 Abs. 1 lit. f DSGVO)

Umsetzungshinweis

Zur Umsetzung von Datenminimierung (SDM 7.1) verweist Art. 25 Abs. 1 DSGVO auf das Mittel der Pseudonymisierung (Nr. 2.7). Weitere Mittel sind u.a. die Anonymisierung (Nr. 2.8) und die Verschlüsselung (Nr. 2.9). Datenminimierung kann auch erreicht werden, indem die Menge der erfassten Attribute der betroffenen Personen, Verarbeitungsoptionen in Verarbeitungsprozessschritten und Möglichkeiten der Kenntnisnahme vorhandener Daten reduziert werden. Ein Cloud-Anbieter sollte soweit möglich Verarbeitungsprozesse automatisieren, um eine Kenntnisnahme verarbeiteter Daten und die Einflussnahme zu begrenzen. Es empfiehlt sich auch, automatische Sperr- und Löschroutinen zu implementieren.

Zur Umsetzung der anderen Grundsätze der Datenverarbeitung sollte der Cloud-Anbieter andere geeignete Mittel und Gestaltungsprinzipien anwenden. Soweit der Cloud-Anbieter eine Datenschutz-Folgenabschätzung durchgeführt hat, können sich Gestaltungsanforderungen aus der Pflicht ergeben, die festgestellten Risiken zu minimieren. Bei der (Weiter-)Entwicklung seines Dienstes sollten Datenminimierung und Datensicherheit zentrale Bestandteil des Software-Entwicklungsprozesses sein, d. h, eingesetzte Programme oder Module sind durch z. B. Reviews, automatisierte Tests, Vulnerability-Tests etc. zu sichern. Zudem können Sicherheitsreifegradmodelle wie etwa Building Security In Maturity Model (BSIMM2), Software Assurance Maturity Model (SAMM) oder Systems Security Engineering Capability Maturity Model (SSE-CMM) für den Entwicklungsprozess des Cloud-Services herangezogen werden.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er dokumentiert, welche Gestaltungsprinzipien und -maßnahmen er vorgesehen hat und welche Erwägungen bei Ergreifen oder Unterlassen von Gestaltungsmaßnahmen ihn geleitet haben. Auch mit der transparenten Dienstbeschreibung kann der Cloud-Anbieter seine datenschutzgerechten Systemgestaltungen und Voreinstellungen nachweisen. Die Dokumentationen in den obligatorisch zu führenden Verarbeitungsverzeichnissen nach Art. 30 Abs. 2 DSGVO und Nr. 8.3 des Kriterien-Katalogs können als Nachweis für die dort aufgeführten Systemgestaltungen dienen.

Nr. 9.2 – Datenschutz durch Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Umsetzungshinweis

Die Voreinstellungen sollten so konzipiert sein, dass durch diese nur personenbezogene Daten erhoben, gespeichert und zugänglich gemacht werden, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist. Soweit der Cloud-Anbieter eine Datenschutz-Folgenabschätzung durchgeführt hat, können sich Anforderungen an die Voreinstellungen aus der Pflicht ergeben, die festgestellten Risiken zu minimieren.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er dokumentiert, welche Voreinstellungen er aus welchen Erwägungen gewählt hat.

Kapitel V: Subauftragsverarbeitung

Nr. 10 – Subauftragsverhältnisse

Nr. 10.1 – Weitere Auftragsverarbeitern des Cloud-Anbieters (Subauftragsverarbeitung) (Art. 28 Abs. 2 DSGVO)

Umsetzungshinweis

Bei standardisierten Massengeschäften können die Cloud-Nutzer bei Änderungen in den Subauftragsverarbeitungen automatisiert, z.B. über eine automatisch generierte E-Mail, informiert werden. In den AGB von Cloud-Anbietern im Massengeschäft kann z.B. auch vorab eine Generalzustimmung für etwaige Änderungen in der Subauftragsverarbeitung, die vorbehalten werden, eingeholt werden. Dabei ist infolge der o.g. automatisierten Information jedem Cloud-Nutzer ein jederzeitiges Kündigungsrecht zuzugestehen, da ein Einspruch (i.S.d. Art. 28 Abs. 2 Satz 2 Hs. 2 DSGVO) von einem einzelnen Cloud-Nutzer im Massengeschäft die Beauftragung eines weiteren oder anderen Auftragsverarbeiters durch den Cloud-Anbieter nicht verhindert.

Die Umsetzungshinweise aus ISO/IEC 27002 Ziff. 15 sind anwendbar.

Nachweis

Der Cloud-Anbieter kann den Nachweis über die rechtskonforme weitere Datenverarbeitung dadurch erbringen, dass er die erteilte Zustimmung der Cloud-Nutzer und die Verträge zu den weiteren Auftragsverarbeitungen (Sub-Cloud-Verträge) mitsamt der für die Konformitätsprüfung erforderlichen Angaben (Dauer, Art und Zweck, Ort der weiteren Verarbeitung, Angaben über den weiteren Auftragsverarbeiter und dessen Dienstbeschreibung) vorlegt.

Nr. 10.2 – Rechtsverbindliche Vereinbarung als Grundlage der Subauftragsverarbeitung (Art. 28 Abs. 4 DSGVO)

Umsetzungshinweis

Die Anforderungen an die rechtsverbindliche Vereinbarung über die Auftragsverarbeitung und an das Hauptauftragsverhältnis sind entsprechend in den Subauftragsverarbeitungen durch den Cloud-Anbieter umzusetzen.

Nachweis

Der Cloud-Anbieter kann den Nachweis über die rechtskonforme weitere Datenverarbeitung dadurch erbringen, dass er die rechtsverbindliche Vereinbarung über die Auftragsverarbeitung und die rechtsverbindliche Vereinbarung über die Sub-Auftragsverarbeitung mitsamt der für die Konformitätsprüfung erforderlichen Angaben (Dauer, Art und Zweck, Ort der weiteren Verarbeitung, Angaben über den weiteren Auftragsverarbeiter und dessen Dienstbeschreibung) vorlegt.

Nr. 10.3 – Information des Cloud-Nutzers (Art. 28 Abs. 2 Satz 2 DSGVO)

Umsetzungshinweis

Der Cloud-Anbieter als Hauptauftragsverarbeiter sollte für jede Verlängerung der Auftragsverarbeitungsleistungskette eine detaillierte Dokumentation über die involvierten Subauftragsverarbeiter unter Angabe von Identität inklusiver ladungsfähiger Anschrift und der ausgeführten Tätigkeiten verfassen, sodass nachvollzogen werden kann, welcher (Sub-)Auftragsverarbeiter jeweils in den datenschutzkritischen Dienstteilen involviert ist und welche Verarbeitungsvorgänge jeweils von wem ausgeführt werden.

Zur Darstellung der involvierten Subauftragsverarbeiter eignen sich Informationsportale innerhalb oder außerhalb des angebotenen Cloud-Dienstes. Diese sollten fortlaufend gepflegt und aktualisiert werden.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er dokumentiert, wie er den Cloud-Nutzer bei beabsichtigter Änderung von Subauftragsverarbeitern informiert. Außerdem kann er seine detaillierte Dokumentation über die involvierten Subauftragsverarbeiter unter Angabe von Identität, ladungsfähiger Anschrift und der ausgeführten Tätigkeiten vorlegen, mit deren Hilfe nachvollzogen werden kann, welcher (Sub-)Auftragsverarbeiter jeweils in den datenschutzkritischen Dienstteilen involviert ist und welche Verarbeitungsvorgänge jeweils von wem ausgeführt werden.

Nr. 10.4 – Auswahl und Kontrolle der Subauftragsverarbeiter (Art. 28 Abs. 4 Satz 1 DSGVO)

Umsetzungshinweis

Soweit der Cloud-Anbieter nicht auf Zertifikate seiner Subauftragsverarbeiter vertrauen kann, sollte er sich selbst von der Einhaltung der datenschutzrechtlichen Anforderungen durch die Subauftragsverarbeiter überzeugen. Insoweit sind die Umsetzungshinweise (implementation guidance) von ISO/IEC 27017 Ziff. 15.1.2, 15.1.3 und ISO/IEC 27002 Ziff. 15 anwendbar.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er Zertifikate der Subauftragnehmer oder sonstige Unterlagen vorlegt, aus denen sich die Gewähr zur Einhaltung der Datenschutz-Grundverordnung ergibt. Hierbei kann eine transparente Dienstbeschreibung des jeweiligen Subauftragsverarbeiters hilfreich sein.

Nr. 10.5 – Gewährleistung der Unterstützungsfunktionen (Art. 28 Abs. 4 Satz 1 i.V.m. Art. 28 Abs. 3 Satz 2 DSGVO)

Umsetzungshinweis

Der Cloud-Anbieter sollte wegen des gesteigerten Risikos bei weiteren Auftragsverarbeitungen interne Dokumentationen führen und die Verarbeitungsprozesse protokollieren. Dies dient auch der Selbstkontrolle des Cloud-Anbieters bei der Pflichtenerfüllung auf den weiteren Auftragsstufen.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er eine Dokumentation vorlegt, aus der sich ergibt, in welche Pflichten er weitere Auftragsverarbeiter einbindet. Protokolle zur Pflichterfüllung infolge der Einschaltung von weiteren Auftragsverarbeitern sind hilfreich.

Kapitel VI: Auftragsverarbeitung außerhalb der EU und des EWR

Nr. 11 – Datenübermittlung

Nr. 11.1 – Geeignete Garantien für die Datenübermittlung (Art. 46 Abs. 2 lit. f i.V.m. Art. 42 Abs. 1 und 2 DSGVO)

Umsetzungshinweis

-

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er Dokumente über ausreichende Garantien nach Art. 46 Abs. 2 DSGVO vorlegt. Eine Zertifizierung nach Art. 42 Abs. 2 DSGVO, die diesem oder einem vergleichbaren anerkannten Kriterienkatalog entspricht, kann ebenfalls als Nachweis dienen.

Nr. 11.2 – Vertreterbenennung (Art. 27 i.V.m. Art. 3 Abs. 2 DSGVO)

Umsetzungshinweis

-

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er die schriftliche Benennung eines Vertreters vorlegt.