European Cloud Service
Data Protection Certification

Ermittlungsmethoden für den AUDITOR-Kriterienkatalog

- Fassung 1.00 -

Stand 05.06.2024

Weitere AUDITOR-Dokumente:

- Zertifizierungsgegenstand (Kurz- und Langfassung)
- Kriterienkatalog
- Konformitätsbewertungsprogramm
- Modularitätskonzept
- Schutzklassenkonzept

Online verfügbar: www.auditor-cert.de

Beitrag zum Forschungsprojekt „European Cloud Service Data Protection Certification (AUDITOR)“, das aufgrund eines Beschlusses des Deutschen Bundestages vom Bundesministerium für Wirtschaft und Klimaschutz gefördert wird (FKZ 01MT17003).

Gefördert durch:

aufgrund eines Beschlusses
des Deutschen Bundestages

Autoren

Ali Sunyaev[a], Alexander Roßnagel[b], Sebastian Lins[a], Natalie Maier-Reinhardt[b], Johannes Müller[b], Heiner Teigeler[a]

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

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

Inhaltsverzeichnis

Abkürzungsverzeichnis

Abs.	Absatz
AGB	Allgemeine Geschäftsbedingungen
Art.	Artikel
BDSG	Bundesdatenschutzgesetz neue Fassung (Geltung ab 25.5.18)
DSGVO	EU-Datenschutz-Grundverordnung (Geltung ab 25.5.18)
EG	Erwägungsgrund
EU	Europäische Union
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
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 *Evaluator* die Funktionsbezeichnung als Neutrum zu lesen und meint nicht einen ausschließlich maskulinen Personenbezug).

A. Leitfaden zur Prüfung des AUDITOR-Kriterienkatalogs

1. Einleitung

Die AUDITOR-Zertifizierung liefert einen Nachweis über die Konformität von Datenverarbeitungsvorgängen von Cloud-Anbietern mit den Anforderungen der EU-Datenschutzgrundverordnung (DSGVO). Gemäß Art. 43 Abs. 1 Satz 1 DSGVO können Zertifizierungsstellen neben Aufsichtsbehörden Zertifizierungen erteilen. Eine Zertifizierungsstelle darf ihre Tätigkeit jedoch nur aufnehmen, wenn sie durch die Deutsche Akkreditierungsstelle GmbH in Zusammenarbeit mit der zuständigen Aufsichtsbehörde akkreditiert wurde. Voraussetzung der Akkreditierung ist die Einhaltung der Anforderungen nach Art. 43 Abs. 2 DSGVO und der ergänzenden Anforderungen der Datenschutzkonferenz zur Akkreditierung nach Art. 43 Abs. 3 DSGVO i.V.m. DIN EN ISO/IEC 17065.

Maßgeblich für die Akkreditierung ist ein Konformitätsbewertungsprogramm, das für jedes Zertifizierungsverfahren erstellt werden muss. Das AUDITOR-Konformitätsbewertungsprogramm beschreibt die von der Zertifizierungsstelle zu erfüllenden Grundsätze und umfasst im Wesentlichen Anforderungen an die Zertifizierungsstelle und den Zertifizierungsprozess. Der AUDITOR-Kriterienkatalog stellt hingegen den Prüfstandard für die Datenschutz-Zertifizierung von Cloud-Diensten gemäß den Anforderungen der EU-Datenschutz-Grundverordnung (DSGVO) dar. Dieser enthält Kriterien, Erläuterungen, Umsetzungshinweise und Nachweise. Die *„Kriterien“* bezeichnen die normativen Voraussetzungen, die zu erfüllen sind, um ein Zertifikat auf der Grundlage des AUDITOR-Kriterienkatalogs zu erhalten. 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 nachgewiesen 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 dem Dokument zu erbringen.

Dieses Dokument liefert Hinweise zur Durchführung von Ermittlungsmethoden, um festzustellen, ob die Kriterien des AUDITOR-Kriterienkatalog eingehalten werden. Das Dokument ist daher gemäß der Gliederung des Kriterienkatalogs strukturiert. Es stellt eine zentrale Erweiterung des AUDITOR-Konformitätsbewertungsprogramms dar.

2. Nutzung des Leitfadens

Die Kriterien stellen die Prüfanforderungen dar und können sich auf unterschiedliche Ermittlungsobjekte beziehen wie Tabelle 1 zu entnehmen ist. So bildet beispielsweise in Kapitel 1 des Kriterienkatalogs die rechtsverbindliche Vereinbarung über die Auftragsverarbeitung das Ermittlungsobjekt, während in Kapitel 2 bei der Gewährleistung der Datensicherheit nach Nr. 2 regelmäßig vorwiegend Softwarearchitektur, Infrastruktur und Prozesse eine Rolle spielen werden. Abbildung 1 stellt schematisch die Einordnung von Ermittlungsobjekten dar.

Ermittlungsobjekt	**Beschreibung**
Rechtsverbindliche Vereinbarungen	Bei rechtsverbindlichen Vereinbarungen als Ermittlungsobjekt werden die Eigenschaften und Inhalte von Verträgen oder Vereinbarungen mit Cloud-Nutzern oder Subauftragsverarbeitern bewertet.
Prozess	Ein Prozess oder eine entsprechende und realitätsnahe Prozessdokumentation kann überprüft werden, um die Konformität mit den Zertifizierungskriterien zu bestätigen.
Anbietereigenschaften	Eine Prüfung von Anbietereigenschaften umfasst die Begutachtung von Eigenschaften und Ausprägungen des Cloud-Anbieters, bspw. die zugrundeliegende Organisationsstruktur.
Diensteigenschaften	Zu den Diensteigenschaften gehören insbesondere Cloud-Dienst-Features und -Funktionen, die für den Cloud-Nutzer unmittelbar sichtbar sind und überprüft werden müssen.
Infrastruktur	Eine Überprüfung kann Infrastrukturkomponenten umfassen, also physische Objekte, wie bspw. Hardware-Komponenten oder die Rechenzentrumsinfrastruktur.
Softwarearchitektur	Die Prüfung von Softwarekomponenten umfasst virtuelle Objekte, bspw. Quellcode sowie die Zusammenstellung und Interaktionen der einzelnen Komponenten der Datenverarbeitungsvorgänge.
Entwicklungsumgebung	Die Prüfung der Entwicklungsumgebung umfasst eingesetzte Entwicklungsmethoden, sichere und vom Produktivsystem getrennte Test- und Entwicklungsumgebung, und Abnahmetests.
Personal	Die Prüfung von Mitarbeitern kann notwendig sein, um bspw. deren fachliche oder persönliche Eignung sicherzustellen.

(Datenschutz-) Managementsystem	Die Prüfung des (Datenschutz-)Managementsystems ist notwendig, um zu erkennen, ob der Cloud-Anbieter für das Management der relevanten Aspekte seiner Tätigkeiten, Produkte und Dienstleistungen ein System umgesetzt hat, das im Einklang mit der Politik der Organisation und den Zertifizierungskriterien steht.

Tabelle 1. Übersicht über mögliche Ermittlungsobjekte innerhalb eines Datenverarbeitungsvorgangs.

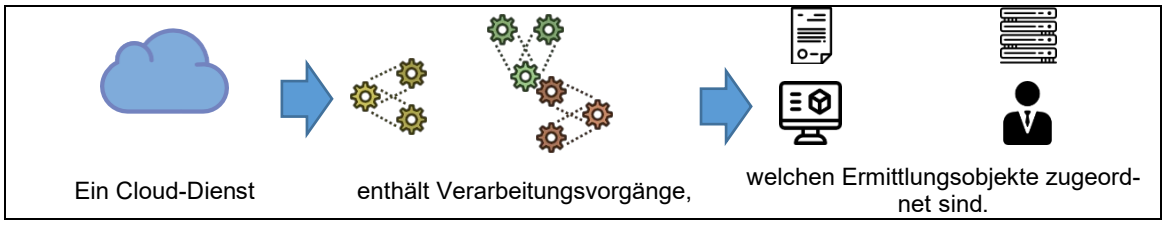

Abbildung 1. Schematische Darstellung zur Einordnung von Ermittlungsobjekten.

Zu jedem Kriterium werden *„Ermittlungsmethoden"* und eine Beschreibung der *„Ermittlung"* angegeben. Im Rahmen der Ermittlung werden eine oder mehrere Ermittlungsmethoden (z.B. Dokumentprüfung oder Audit) durchgeführt, um vollständige Informationen über die Erfüllung der im AUDITOR-Kriterienkatalog festgelegten Kriterien durch die Datenverarbeitungsvorgänge oder ihrer Stichproben zu erhalten. Im Folgenden werden mögliche Ermittlungsmethoden gemäß des AUDITOR-Konformitätsbewertungsprogramms zusammengefasst, welche im Rahmen einer Zertifizierung Anwendung finden können:

1. **Dokumentprüfung** (im Sinne der ISO/IEC 17020). Mit der Dokumentprüfung überprüft der Evaluator die Einhaltung der Zertifizierungskriterien anhand der Angaben in der Dokumentation des Cloud-Anbieters. Ein Cloud-Anbieter legt entsprechende Dokumente, (technische) Logs, Testate oder andere Dokumentationen vor. Insbesondere findet hierbei eine Rechtsanalyse statt (bspw. der rechtsverbindlichen Vereinbarungen), um sicherzugehen, dass die geltenden rechtlichen Kriterien erfüllt werden. Zudem können im Rahmen einer Dokumentprüfung auch Personenzertifikate (im Sinne der ISO/IEC 17024) zum Kompetenznachweis für das Personal bzw. einer natürlichen Person (bspw. des Datenschutzbeauftragten) und zur Gewährleistung eines angemessenen Datenschutzniveaus überprüft werden. Eine Dokumentprüfung ist stets mit geeigneten Ermittlungsmethoden zu ergänzen, um sicherzustellen, dass die dokumentierten Anweisungen, Verfahren, Regeln etc. auch fortlaufend vom Cloud-Anbieter umgesetzt werden.

2. **Inspektion** (im Sinne der ISO/IEC 17020). Im Rahmen einer Inspektion wird die Konformität eines Produktes oder Prozesses mit spezifischen Anforderungen (hier DSGVO und den Zertifizierungskriterien) untersucht. Inspektionsparameter schließen Fragen zur Quantität, Qualität, Sicherheit, Zweckmäßigkeit sowie fortdauernden Einhaltung der Sicherheit von in Betrieb befindlichen Anlagen oder Systemen ein. In Bezug auf die AUDITOR-Datenschutzzertifizierung wird mittels einer (rechtlichen) Inspektion insbesondere die Einhaltung von geeigneten technischen und organisatorischen Maßnahmen gem. Art. 32 Abs. 1 lit. a) bis d) DSGVO überprüft. Die Inspektion kann alle Phasen im Rahmen der Lebensdauer der Ermittlungsobjekte betreffen, einschließlich der Entwicklungsphase. Bei der Inspektion können bspw. Datenverarbeitungsvorgänge im Rahmen einer Dienstnutzung durchgeführt werden, um die Funktionsweise und die Ergebnisse der Vorgänge beurteilen zu können. Ein Evaluator vergleicht hierbei die zu erwartenden Ergebnisse gemäß der vorliegenden Dokumentation mit den tatsächlichen Ergebnissen, welche durch eine Dienstnutzung erbracht werden. Er erhält somit keinen Einblick in die internen Verarbeitungsschritte der Verarbeitungsvorgänge (‚Black-Box-Test'). Daneben kann ein Vorgang oder eine Vorgangsreihe auch angestoßen und die tatsächliche Ausführung überwacht (‚monitoring') oder Logs der Vorgangsausführung überprüft werden (‚White-Box-Test').

3. **Prüfung** (im Sinne der ISO/IEC 17025:2017). Eine Prüfung umfasst Tests oder Messungen zur Untersuchung des Datenverarbeitungsvorgangs bzw. des Ermittlungsobjektes und zur Feststellung ihrer Übereinstimmung mit den Zertifizierungskriterien. So kann eine Assetprüfung durchgeführt werden, indem bei der Prüfung ein Asset (z.B. Hardware oder Softwarecode und ggf. die dazugehörige Dokumentation) untersucht wird. Die Prüfung kann in Begleitung oder unter Anweisung eines Mitarbeiters des Cloud-Anbieters oder eigenständig durch den Evaluator durchgeführt werden. Der Cloud-Anbieter ist vorab über die Prüfung zu informieren und stellt den Evaluator bspw. notwendige Zugänge (bspw. Test-Accounts) oder (technische) Logs über die Ausführung des Vorgangs zur Durchführung der Prüfung bereit. Insofern notwendig, wählt der Evaluator geeignete Testdaten. Hierzu zählen zufällig erzeugte Werte, die eine realistische und funktionskonforme Prüfung des Vorgangs ermöglichen. Ein Evaluator kann zur Prüfung und Überwachung des Vorgangs (‚monitoring') geeignete (ggf. extern bereitgestellte) Testierungs- und Auditierungsprodukte und -dienstleistungen nutzen (s. ISO/IEC 17025:2017 Tz. 6.6). Die eingesetzten Produkte und Dienstleistungen zur Prüfung sind im Ermittlungsbericht zu dokumentieren. Bei invasiven Ermittlungsverfahren oder Verfahren, die zu einer Beeinträchtigung von Datenverarbeitungsvorgängen des Cloud-Dienstes führen könnten, ist eine Abstimmung mit dem Cloud-Anbieter notwendig. Der Cloud-Anbieter ist verpflichtet den

Evaluator bei der Durchführung zu unterstützen. In Bezug auf die AUDITOR-Datenschutzzertifizierung wird mittels einer (rechtlichen) Prüfung insbesondere die Einhaltung von geeigneten technischen und organisatorischen Maßnahmen gem. Art. 32 Abs. 1 lit. a) bis d) DSGVO überprüft. Bspw. kann mittels Sicherheitstests die korrekte und starke Verschlüsselung von Daten festgestellt werden. Bei der Durchführung von Sicherheitstests sei weiterführend auf die ISO/IEC 15408:2009 und ISO/IEC 18045:2008-018 hingewiesen.

4. **Audit** (im Sinne der ISO/IEC 17021-1:2015). Ein Audit wird zum Zweck der Zertifizierung des (Datenschutz-)Managementsystems des Cloud-Anbieters durchgeführt (s. ISO/IEC 17021-1:2015 Tz. 3.4), um zu erkennen, dass der Cloud-Anbieter für das Management der relevanten Aspekte seiner Tätigkeiten, Produkte und Dienstleistungen ein System verwendet, das im Einklang mit der Politik der Organisation sowie den Zertifizierungskriterien steht. Audits können vor Ort, aus der Ferne oder in einer Kombination aus beidem durchgeführt werden (s. ISO 19011:2018-10 Tz 5.5.3). Der Einsatz dieser Methoden sollte angemessen ausgewogen sein, unter anderem auf Grundlage der Berücksichtigung der damit verbundenen Risiken und Chancen. Im Rahmen des Audits können insbesondere Befragungen, Beobachtungen und Prüfungen durchgeführt werden, um Informationen über Wissen und Fertigkeiten zu ermitteln sowie festzustellen, ob Prozesse und das Managementsystem beim Cloud-Anbieter gelebt werden. Die Befragung von Mitarbeitern des Cloud-Anbieters oder anderen Personen, die mit der Erbringung der Datenverarbeitungsvorgänge befasst sind, kann zur Sachverhaltsermittlung einzelner Aspekte und zur Überprüfung der Richtigkeit der Dokumentation eingesetzt werden (s. ISO/IEC 17021-1:2015 Tz. B.4). Sie soll insbesondere zur Überprüfung bei vom Evaluator als kritisch erkannten Aspekten eingesetzt werden. Befragungen können schriftlich oder persönlich durchgeführt werden. Sie sollen jedenfalls hinsichtlich zentraler Aspekte als mündliche Befragung durchgeführt werden. Soweit eine persönliche Befragung unverhältnismäßig wäre, kann sie in Form von Videokonferenzen durchgeführt werden. Eine Person bei der Erfüllung einer Aufgabe zu beobachten, kann durch die damit dargelegte Anwendung von Wissen und Fertigkeiten zur Erzielung eines gewünschten Ergebnisses direkte Nachweise für die Kompetenz liefern (s. ISO/IEC 17021-1:2015 Tz. B.5). Schriftliche, mündliche und praktische Prüfungen können gute und gut dokumentierte Nachweise für vorhandenes Wissen und — je nach angewendeter Methodik — auch für Fertigkeiten liefern (s. ISO/IEC 17021-1:2015 Tz. B.6). Eine Vor-Ort-Prüfung umfasst die Inaugenscheinnahme der Verfahren und technischen Einrichtungen in den Räumlichkeiten des Cloud-Anbieters. In Bezug auf die AUDITOR-Datenschutzzertifizierung sollen insbesondere (rechtliche) Audits durchgeführt werden, um eine korrekte Einrichtung, Aufrechterhaltung und Pflege eines Datenschutz-Managementsystems (im Sinne von Art. 24 und 25, 32, 33, 34 sowie 37 bis 39 DSGVO) zu prüfen. Die Sicherstellung eines Datenschutz-Managementsystems sollte der fortwährenden Sicherstellung des Datenschutzniveaus des zertifizierten Cloud-Dienstes dienen. Für weiterführende Literatur zur Durchführung von Audits sei insbesondere auf die ISO/IEC 17021-1:2015 Tz. 9.4 und ISO 19011:2018-10 verwiesen. Für die Durchführung von Audits aus der Ferne sei auf IAF MD 4:2018 verwiesen.

5. **Entwicklungs- und Designprüfung** (im Sinne der ISO/IEC 17020). Eine Entwicklungsprüfung umfasst die Prüfung von Entwicklungsmethoden und -verfahren sowie bei Bedarf eine Prüfung der Testsysteme und -umgebungen, welche bei der Entwicklung von Hard- und Software zur Erbringung der Datenverarbeitungsvorgänge eingesetzt werden. Bei der Designprüfung können unter anderem die gewählte Architektur, Datenbankdiagramme, Datenflussdiagramme, Designentscheidungen aber auch die Konfiguration des Cloud-Dienstes zur Erbringung des Datenverarbeitungsvorgangs überprüft werden. Eine Entwicklungs- und Designprüfung sollte auch eine Rechtsanalyse umfassen, um sicherzugehen das die geltenden rechtlichen Kriterien erfüllt werden. So kann eine rechtliche Entwicklungs- und Designprüfung insbesondere im Rahmen der Prüfung zur Erfüllung des Art. 25 DSGVO oder zur Überprüfung der Datenschutz-Folgenabschätzung erforderlich sein.

Im Folgenden werden pro Kriterium geeignete Ermittlungsmethoden aufgezeigt. Bei der Ermittlung müssen die relevanten internationalen Normen zur Ermittlungsart berücksichtigt werden. Die relevanten internationalen Normen sind für die Prüfung ISO/IEC 17025, für die Inspektion ISO/IEC 17020, für die Durchführung von Audits von Managementsystemen ISO/IEC 17021 und für Personenzertifizierungen ISO/IEC 17024. Ein Evaluator prüft abhängig vom Zertifizierungsgegenstand und konkreten Ermittlungsobjekt die Eignung und Anwendung der jeweiligen Methode. Ein Evaluator muss sicherstellen, dass nicht nur eine ausreichende Dokumentation als Nachweis vorliegt, sondern auch, dass die dokumentierten Maßnahmen umgesetzt und ‚gelebt' werden. Insbesondere bei Ermittlungstätigkeiten im Rahmen der AUDITOR-Datenschutzzertifizierung sollte eine fortlaufende Rechtsanalyse durchgeführt werden. So soll bspw. im Rahmen einer Dokumentprüfung nicht nur die Prüfung von Vereinbarungen, sondern vor allem auch durch geeignete weitere Ermittlungsmethoden die konkrete Umsetzung beim Cloud-Anbieter als Auftragsverarbeiter überprüft werden, um sicherzugehen das die geltenden rechtlichen Kriterien erfüllt werden. Ermittlungsmethoden können bei Bedarf kombiniert werden, um (zusätzliche) fundierte Informationen über das Ermittlungsobjekt zu erheben. Die Ermittlung kann gemäß den Richtlinien des Konformitätsbewertungsprogramms stichprobenartig erfolgen.

B. Kriterien und Ermittlungsmethoden für die Auftragsverarbeitung

Kapitel I: Rechtsverbindliche Vereinbarung zur Auftragsverarbeitung

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 UAbs. 1 Satz 1 und Abs. 9 DSGVO)

Kriterium

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

(2) Die rechtsverbindliche Vereinbarung zur Auftragsverarbeitung ist schriftlich oder in einem elektronischen Format[1] abzufassen.

(3) Diese rechtsverbindliche Vereinbarung zur Auftragsverarbeitung muss die Kriterien dieses Kapitels (Nr. 1.2 bis 1.8) erfüllen, wobei die in diesen Kriterien geforderten Festlegungen auch in sonstigen Dokumenten getroffen werden können, wenn diese als Bestandteile der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung einbezogen worden sind.

Ermittlungsmethoden

- Dokumentprüfung, insbesondere Rechtsanalyse
- Inspektion

Ermittlung

Der Evaluator prüft den Abschluss von standardisierten Vereinbarungen anhand eines Auszuges von Vereinbarungen aus der Datenbank (oder einem anderen Speicherort der Vereinbarungen). Auch sollte ein stichprobenartiger Abgleich des Vertragsabschlussdatums mit dem Zeitstempel der initialen Nutzerdatensatzerzeugung durchgeführt werden. Sollten keine standardisierten Vereinbarungen geschlossen worden sein, prüft ein Evaluator im Rahmen der Dokumentprüfung alle oder eine repräsentative Stichprobe von rechtsverbindlichen Vereinbarungen, die ein Cloud-Anbieter mit den Cloud-Nutzern geschlossen hat.

Eine repräsentative Stichprobe sollte mindestens so umfassend gewählt werden, dass durch eine vergleichende Begutachtung einer Auswahl an Vereinbarungen mit hoher Wahrscheinlichkeit ausgeschlossen werden kann, dass eine weitere Vereinbarung wesentlich abweicht. Der Stichprobenumfang ist somit auch abhängig von der Gesamtanzahl an geschlossenen Vereinbarungen. In der Regel sollte eine Stichprobengröße von 3% angestrebt werden. Die individuellen Vereinbarungen können zu Gruppen zusammengefasst werden, wobei aus jeder Gruppe von Vereinbarungen eine ausreichende Anzahl an Vereinbarungen geprüft werden muss. Vereinbarungen können unter anderem hinsichtlich des Gegenstands, der Dauer, der Art und den Zweck der Verarbeitung in Gruppen eingeteilt werden.

Außerdem muss der Evaluator anhand einer geeigneten Dokumentation (z.B. Prozessdokumentation, Funktionsdokumentation, Protokolldateien oder Logs) prüfen, ob der Cloud-Anbieter technische oder organisatorische Vorkehrungen getroffen hat, die einen automatischen Vereinbarungsschluss vor der eigentlichen Dienstnutzung sicherstellen (bspw. in Bezug auf einen Vereinbarungs- bzw. Registrierungsprozesses mit potenziellen Cloud-Nutzern). Anhand dieser Funktionsdokumentation muss für einen Evaluator ersichtlich werden, dass ein potenzieller Cloud-Nutzer einen Datenverarbeitungsvorgang nur dann durchführen kann, wenn eine rechtsverbindliche Vereinbarung gemäß den Vorgaben des Kriterienkatalogs geschlossen wird.

Zudem sollte ein Evaluator eine Inspektion in Form einer testweisen Durchführung eines entsprechenden Vereinbarungs- bzw. Registrierungsprozesses vornehmen, um sicherzustellen, dass die in der Dokumentation angegebenen Konzepte auch in dem Cloud-Dienst realisiert wurden. Im Rahmen der testweisen Durchführung sollte ein Evaluator auch überprüfen, ob durch Vorsatz oder Fehlverhalten das Abschließen einer Vereinbarung umgangen werden kann.

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

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

Kriterium

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

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

Ermittlungsmethoden

- Dokumentprüfung, insbesondere Rechtsanalyse
- Inspektion

Ermittlung

Durch eine Dokumentprüfung (insb. Durchsicht vom Cloud-Anbieter bereitgestellten Vertragsmustern, -vorlagen oder -instanzen) und Inspektion in Form einer Dienstnutzung (insb. Einsicht ob Inhalte bei Dienstnutzung angezeigt werden) prüft der Evaluator, ob der Gegenstand und die Dauer des Auftrags festgelegt werden und dem Cloud-Nutzer auf geeignete Weise kommuniziert werden.

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

Kriterium

In der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung werden Art und Zweck der vorgesehenen Verarbeitung von Daten im Auftrag, die Art der verarbeiteten Daten sowie die Kategorien betroffener Personen festgelegt.

Ermittlungsmethoden

- Dokumentprüfung, insbesondere Rechtsanalyse
- Inspektion

Ermittlung

Durch eine Dokumentprüfung (insb. Durchsicht vom Cloud-Anbieter bereitgestellten Vertragsmustern, -vorlagen oder -instanzen) und eine Inspektion in Form einer Dienstnutzung (insb. Einsicht ob Inhalte bei Dienstnutzung angezeigt werden) prüft der Evaluator, ob der Umfang, die Art und der Zweck der Datenverarbeitung, die Art der verarbeiteten Daten sowie die Kategorien betroffener Personen festgelegt werden und dem Cloud-Nutzer auf geeignete Weise kommuniziert werden.

Nr. 1.4 – Festlegung von Weisungsbefugnissen (Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. a und h, UAbs. 2 DSGVO)

Kriterium

(1) Die rechtsverbindliche Vereinbarung über die Auftragsverarbeitung sieht vor, dass die personenbezogenen Daten nur auf dokumentierte Weisung des Cloud-Nutzers – auch in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation – verarbeitet werden, sofern der Cloud-Anbieter nicht durch Unionsrecht oder mitgliedstaatliches Recht zur Datenverarbeitung verpflichtet ist.

(2) Für den Fall, dass der Cloud-Anbieter durch Unionsrecht oder mitgliedstaatliches Recht zur Datenverarbeitung verpflichtet ist, sieht die rechtsverbindliche Vereinbarung über die Auftragsverarbeitung die Pflicht des Cloud-Anbieters vor, dem Cloud-Nutzer die rechtlichen Anforderungen vor der Verarbeitung mitzuteilen, sofern das jeweilige Recht die Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(3) Für den Fall, dass die rechtsverbindliche Vereinbarung zur Auftragsverarbeitung weisungsgebundene Übermittlungen personenbezogener Daten an Drittländer oder internationale Organisationen auf Weisung des Verantwortlichen vorsieht, legt die rechtsverbindliche Vereinbarung über die Auftragsverarbeitung fest, welche Instrumente nach Art. 45 DSGVO oder Art. 46 Abs. 2 und 3 DSGVO für die Übermittlungen genutzt und ggf. welche zusätzlichen Maßnahmen ergriffen werden sollen, um ein angemessenes Schutzniveau sicherzustellen.

(4) Wird eine rechtsverbindliche Vereinbarung zur Auftragsverarbeitung im Rahmen standardisierter Massengeschäfte auf der Basis von allgemeinen Geschäftsbedingungen geschlossen, hat der Cloud-Anbieter – bevor die rechtsverbindliche Vereinbarung zur Auftragsverarbeitung geschlossen wird – 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.

(5) In der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung verpflichtet sich der Cloud-Anbieter zur Information des Cloud-Nutzers, wenn er der Ansicht ist, dass eine Weisung des Cloud-Nutzers gegen datenschutzrechtliche Vorschriften verstößt.

Ermittlungsmethoden

- Dokumentprüfung, insbesondere Rechtsanalyse
- Inspektion

Ermittlung

Durch eine Dokumentprüfung (insb. Durchsicht vom Cloud-Anbieter bereitgestellter Vertragsmuster, -vorlagen oder -instanzen) und Inspektion in Form einer Dienstnutzung (insb. Einsicht ob Inhalte bei Dienstnutzung angezeigt werden) prüft der Evaluator, ob eine Dienstbeschreibung die durch den Cloud-Nutzer technisch ausführbaren Dienstleistungen und Weisungsbefugnisse beschreibt und festlegt wer zur Erteilung von Weisungen befugt ist; und wer auf Seiten des Cloud-Anbieters mit der Entgegennahme der Weisungen betraut ist, und wie diese Festlegungen dem Cloud-Nutzer auf geeignete Weise kommuniziert werden. Auch prüft der Evaluator, ob der Cloud-Anbieter Informationen zur nicht weisungsgebundenen Verarbeitung aufgrund rechtlicher Pflichten aus Unions- oder mitgliedstaatlichem Recht und zur Festlegung geeigneter Garantien für die Datenübermittlung in Drittländer oder internationale Organisationen in rechtsverbindlichen Vereinbarungen offenlegt und sich vertraglich verpflichtet, den Cloud-Nutzer zu informieren, wenn er der Auffassung ist, dass eine Weisung des Cloud-Nutzers gegen datenschutzrechtliche Vorschriften verstößt.

Im Rahmen einer Dokumentenprüfung (insb. Durchsicht vom Cloud-Anbieter bereitgestellter Vertragsmuster, -vorlagen, -instanzen oder geschlossener Verträge) prüft der Evaluator weiterhin, welche Instrumente nach Art. 45 DSGVO oder Art. 46 Abs. 2 und 3 DSGVO für die Übermittlungen personenbezogener Daten an Drittländer oder internationale Organisationen genutzt werden und ggf. welche zusätzlichen vertraglichen, organisatorischen und/oder technischen Maßnahmen vertraglich festgelegt werden, wenn die genannten Instrumente alleine nicht ausreichend sind, um ein angemessenes Schutzniveau herzustellen.

Nr. 1.5 – Ort der Datenverarbeitung (indirekt Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. a und h DSGVO)

Kriterium

(1) In der rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung wird festgelegt, ob sich der Ort der Datenverarbeitung innerhalb der EU oder des EWR oder in einem Drittland befindet.[2]

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

(3) In der rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung wird festgelegt, dass in den Fällen, in denen sich während ihres Geltungszeitraums der Ort der Verarbeitung ändert, der Cloud-Anbieter diese Änderung dem Cloud-Nutzer unverzüglich mitteilt.

(4) Die rechtsverbindliche Vereinbarung zur Auftragsverarbeitung muss vorsehen, dass der Cloud-Nutzer effektiv einer Änderung hinsichtlich der Orte der Verarbeitung widersprechen kann, wenn diese substantielle Auswirkungen[3] auf die zuvor durchgeführten Beurteilungen haben.

Ermittlungsmethoden

- Dokumentprüfung, insbesondere Rechtsanalyse
- Inspektion

[2] Dazu gehört auch der Ort, der von durch weiteren Auftragsverarbeitern (Subauftragsverarbeiter) durchgeführten Verarbeitungstätigkeiten, wenn der Cloud-Anbieter einen anderen Auftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten im Auftrag des für die Verarbeitung Verantwortlichen beauftragt.
[3] Eine substantielle Auswirkung auf die zuvor durchgeführten Bewertungen liegt vor, wenn der neue Ort der Verarbeitung eine Datenübermittlung außerhalb der EU/des EWR nach sich ziehen würde.

Ermittlung

Durch eine Dokumentprüfung (insb. Durchsicht vom Cloud-Anbieter bereitgestellten Vertragsmustern, -vorlagen oder -instanzen) und Inspektion in Form einer Dienstnutzung (insb. Einsicht ob Inhalte bei Dienstnutzung angezeigt werden) prüft der Evaluator, ob der Ort der Datenverarbeitung (innerhalb der EU/ des EWR oder das konkrete Drittland) und die Verpflichtung zur Meldung und Widerspruch durch den Cloud-Nutzer bei Änderungen des Ortes festgelegt und dem Cloud-Nutzer auf geeignete Weise kommuniziert werden.

Nr. 1.6 – Verpflichtung zur Vertraulichkeit (Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. b und h DSGVO)

Kriterium

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 über das Ende ihres Beschäftigungsverhältnisses hinaus verpflichtet werden, sofern sie nicht bereits einer angemessenen vergleichbaren gesetzlichen Verschwiegenheitspflicht unterliegen.

Ermittlungsmethoden

- Dokumentprüfung, insbesondere Rechtsanalyse
- Inspektion

Ermittlung

Ein Evaluator prüft durch eine Dokumentprüfung (insb. Durchsicht vom Cloud-Anbieter bereitgestellten Vertragsmustern, -vorlagen oder -instanzen), dass der Cloud-Anbieter sich rechtsverbindlich dazu verpflichtet hat, die zur Verarbeitung von personenbezogenen Daten befugten Personen vor Aufnahme der datenverarbeitenden Tätigkeit zur Vertraulichkeit zu verpflichten, sofern sie nicht bereits einer angemessenen vergleichbaren gesetzlichen Verschwiegenheitspflicht unterliegen. Durch eine Inspektion in Form einer testweisen Dienstnutzung kann ein Evaluator prüfen, ob diese Inhalte festgelegt und dem Cloud-Nutzer in der rechtsverbindlichen Vereinbarung angezeigt werden.

Nr. 1.7 – Technisch-organisatorische Maßnahmen, Unterbeauftragung und Unterstützung (Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. c, h i.V.m. Kap. III und Art. 32 bis 36 DSGVO)

Kriterium

(1) Die dem Schutzniveau der ausgelagerten Datenverarbeitung angemessenen TOM werden in einer rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung festgelegt.

(2) Die rechtsverbindliche Vereinbarung über die Auftragsverarbeitung enthält die Angabe, ob der Cloud-Anbieter eine Pseudonymisierung, Anonymisierung oder Verschlüsselung (Nr. 2.7, Nr. 2.8 und Nr. 2.9) der zu verarbeitenden personenbezogenen Daten vornimmt. Die Angabe sollte klarstellen, ob diese Mechanismen auch gegenüber den Mitarbeitern des Cloud-Anbieters wirksam sind, die Zugang zu personenbezogenen Daten haben können.

(3) Der Cloud-Anbieter legt in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung fest, auf welchem Niveau er nach einem physischen oder technischen Zwischenfall die Daten des Cloud-Nutzers und den Cloud-Dienst wiederherstellen und dem Cloud-Nutzer Zugang zum Cloud-Dienst und zu den Daten sicherstellen 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 und TOM zur Unterstützung des Cloud-Nutzers bei der Erfüllung der Betroffenenrechte gemäß Nr. 6, bei der Durchführung einer Datenschutz-Folgenabschätzung gemäß Nr. 7 und zur Erfüllung der Meldepflicht bei Datenschutzverletzungen nach Nr. 8.2 werden in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung festgelegt.[4]

[4] Dieses Kriterium würde nicht für den Cloud-Nutzer gelten, der unter die Haushaltsausnahme fällt. Der Cloud-Anbieter als Auftragsverarbeiter ist gut beraten, das Kriterium als vorhanden und potenziell zu erfüllen zu betrachten, um auf solche Veränderungen in der Rolle eines Cloud-Nutzers, der zum für die Verarbeitung Verantwortlichen wird, reagieren zu können.

Ermittlungsmethoden

- Dokumentprüfung, insbesondere Rechtsanalyse
- Inspektion

Ermittlung

Durch eine Dokumentprüfung (insb. Durchsicht vom Cloud-Anbieter bereitgestellten Vertragsmustern, -vorlagen oder -instanzen) und eine Inspektion in Form einer Dienstnutzung (insb. Einsicht, ob Inhalte bei Dienstnutzung angezeigt werden) prüft ein Evaluator, ob die Verfahren, Prozesse und TOM zur Unterstützung des Cloud-Nutzers bei der Erfüllung seiner Pflichten nach Art. 33-36 DSGVO festgelegt und dem Cloud-Nutzer auf geeignete Weise kommuniziert werden. Hierfür können die entsprechenden Dokumentationen der Verfahren und Prozesse, wie die zur Meldung von Datenschutzverletzungen an Cloud-Nutzer, geprüft werden.

Darüber hinaus muss der Evalautor prüfen, ob der Cloud-Anbieter die eingesetzten TOM zu Gewährleistung der Datensicherheit nach Art. 32 DSGVO in der Vereinbarung festgelegt und hinreichend beschrieben hat. Hinreichend bedeutet, dass alle TOM beschrieben werden und eine Detaillierungsstufe erreicht wird, welche auf der einen Seite keine sensiblen oder sicherheitskritischen Informationen preisgibt aber auf der anderen Seite einem Cloud-Nutzer genügend Informationen zur Beurteilung der Risikolage und der Angemessenheit der TOM ermöglicht. So kann die Angabe der TOM an den Gewährleistungszielen ausgerichtet sein. Zur Beurteilung der Einhaltung der Bedingungen aus Art. 28 Abs. 2 und 4 DSGVO prüft der Evaluator die vom Cloud-Anbieter bereitgestellten Vertragsmuster, -vorlagen oder -instanzen zur Beauftragung von Subauftragnehmern im Rahmen einer Dokumentenprüfung auf Vollständigkeit nach Art. 28 Abs. 3 DSGVO und Zulässigkeit. Siehe hierzu auch die Ermittlungsmethoden für die Kriterien Nr. 10.1. bis 10.5.

Nr. 1.8 – Rückgabe von Datenträgern und Löschung von Daten; Nachweis der Einhaltung der Vorschriften und Ermöglichung von und Mitwirkung an Audits (Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. g und h DSGVO)

Kriterium

(1) Die Pflichten des Cloud-Anbieters zur Rückgabe aller Datenträger[5] (die personenbezogene Daten enthalten), Rückführung von allen personenbezogenen Daten und irreversiblen Löschung von personenbezogenen Daten nach Ende der Auftragsverarbeitung sind in einer rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung festzulegen.

(2) Die Pflichten des Cloud-Anbieters, alle Informationen zur Verfügung zu stellen, die für den Nachweis der Einhaltung der in Art. 28 DSGVO erforderlich sind und die Audits, einschließlich Inspektionen, durch den für die Verarbeitung Verantwortlichen oder einen von ihm beauftragten Prüfer zulassen, müssen in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung festgelegt sein.

Ermittlungsmethoden

- Dokumentprüfung, insbesondere Rechtsanalyse
- Inspektion

Ermittlung

Durch eine Dokumentprüfung (insb. Durchsicht vom Cloud-Anbieter bereitgestellten Vertragsmustern, -vorlagen oder -instanzen) und Inspektion in Form einer Dienstnutzung (insb. Einsicht ob Inhalte bei Dienstnutzung angezeigt werden) prüft ein Evaluator, ob die Pflichten des Cloud-Anbieters zur Rückgabe von Datenträgern, Rückführung von Daten und Löschung von Daten nach Ende der Auftragsverarbeitung dem Cloud-Nutzer auf geeignete Weise kommuniziert werden. Gleichermaßen prüft er, ob die Zulassung von Audits, einschließlich Inspektionen, durch den für die Verarbeitung Verantwortlichen in der Vereinbarung enthalten sind.

Durch eine Dokumentprüfung prüft der Evaluator, ob der Cloud-Anbieter Nachweise zur Verfügung stellt, aus denen hervorgeht, dass er aktiv Maßnahmen zur Bereitstellung von Informationen ergreift und Audits durch den für die Verarbeitung Verantwortlichen oder andere von ihm beauftragte Auditoren zulässt und dazu beiträgt.

[5] ISO/IEC 2382:2015, Informationstechnik - Vokabular, 2121321, "Datenträger": Material, in oder auf dem Daten aufgezeichnet werden können und von dem Daten abgerufen werden können.

Kapitel II: Rechte und Pflichten des Cloud-Anbieters

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

Nr. 2.1 – Datensicherheitskonzept (Art. 24, 25, 28, 32, 35 i.V.m. Art. 5 Abs. 1 lit. f und Abs. 2 DSGVO)

Kriterium

(1) Der Cloud-Anbieter führt eine Risikoanalyse nach dem Stand der Technik in Bezug auf die Datensicherheit durch und unterhält ein Datensicherheitskonzept[6] entsprechend seiner Schutzklasse, das den spezifischen Risiken seiner Datenverarbeitungsvorgänge, die sich insbesondere durch Vernichtung, Verlust, Veränderung, unbefugte Offenlegung von und unbefugten Zugang zu personenbezogenen Daten ergeben können, angemessen ist. Im Rahmen der Risikobeurteilung muss der Cloud-Anbieter insbesondere die für Kriterium Nr.2 spezifischen Risikoszenarien berücksichtigen und entsprechende TOM umsetzen.

(2) Der Cloud-Anbieter unterhält eine Beschreibung aller Datenkategorien, für die er eine Verarbeitung durch seinem Cloud-Dienst anbieten kann.

(3) Die in Nr. 2 geforderten Angaben können außer im Datensicherheitskonzept auch in sonstigen Dokumenten getroffen werden, solange diese als rechtsverbindlich für die Auftragsverarbeitung zwischen Cloud-Anbieter und Cloud-Nutzer vereinbart worden sind. Die Anforderungen an das Datensicherheitskonzept gelten auch für diese sonstigen Dokumente.

(4) Im Datensicherheitskonzept stellt der Cloud-Anbieter dar, welche TOM er umgesetzt hat, um die bestehenden Datensicherheitsrisiken abzustellen oder einzudämmen. Der Cloud-Anbieter schildert auch die Abwägungen, die er vorgenommen hat, um zu diesen Maßnahmen zu gelangen.

(5) Das Datensicherheitskonzept ist schriftlich oder in einem elektronischen Format zu dokumentieren.

(6) Das Datensicherheitskonzept ist in regelmäßigen Abständen (d.h. mindestens jährlich und nach jeder erheblichen Veränderung) auf Aktualität und Angemessenheit zu überprüfen und bei Bedarf zu aktualisieren. Falls das Datensicherheitskonzept aktualisiert werden muss, muss der Cloud-Anbieter den Cloud-Nutzer vor Umsetzung des Updates informieren.

(7) Das Datensicherheitskonzept beschreibt, welche Datenverarbeitungsvorgänge vom Cloud-Anbieter selbst durchgeführt werden und welche Datenverarbeitungsvorgänge von Subauftragsverarbeitern durchgeführt werden.

(8) Das Datensicherheitskonzept beschreibt, welche Datenverarbeitungsvorgänge in der Verantwortung des Cloud-Anbieters liegen und welche der Verantwortung des Cloud-Nutzers unterliegen.

(9) Soweit das Datensicherheitskonzept Sicherheitsmaßnahmen des Cloud-Nutzers verlangt, sind diese dem Cloud-Nutzer vor dem Beginn der Datenverarbeitung oder vor Änderungen an diesen schriftlich oder in einem elektronischen Format mitzuteilen.

Ermittlungsmethoden

- Dokumentprüfung, insbesondere Rechtsanalyse
- Inspektion
- Audit

Ermittlung

Ein Evaluator prüft mittels Dokumentprüfung das Vorhandensein und die Inhalte des Datensicherheitskonzepts. In der Dokumentation wird insbesondere geprüft, ob das Verfahren zur Risikobeurteilung beschrieben und mit der DSGVO vereinbar ist, ob die Risikoermittlung korrekt durchgeführt wurde und ob alle identifizierten Risiken und Risikoszenarien (und ggf. Chancen) mit Angabe einer Schwere pro Risiko aufgeführt werden. Weiterhin wird geprüft, ob Abwägungen geschildert werden, die ein Cloud-Anbieter vorgenommen hat, und ob die TOM zur Adressierung von Risiken beschrieben sind (beispielsweise Dokumentation von geplanten Maßnahmen in internem Ticketsystem des Unternehmens und Verweis auf durch diese Maßnahmen adressierte Risiken). Ein Evaluator sollte

[6] Ein Datensicherheitskonzept dokumentiert u.a. Schutzprinzipien, identifizierte Risiken und festgelegte TOMs zum Schutz der verarbeiteten Daten. In englischen Sprachfassungen ist auch der Begriff „data security program“ geläufig.

auch Dokumente über Prozesse im Falle der Risikorealisierung (z.B. in Form von Unternehmensrichtlinien) überprüfen. Zudem prüft der Evaluator, ob im Datensicherheitskonzept der Verantwortungsbereich vom Cloud-Anbieter und Subauftragsverarbeiter und Cloud-Nutzer getrennt und hinreichend beschrieben werden.

Auch prüft ein Evaluator durch eine Dokumentenprüfung die Liste der vom Cloud-Anbieter verarbeiteten Datenkategorien auf Konsistenz und Vollständigkeit durch einen stichprobenartigen Abgleich der vorgelegten Beschreibung mit den geschlossenen Vereinbarungen über die Auftragsverarbeitung, aus denen sich die Art der im Auftrag des Cloud-Nutzers verarbeiteten Daten ergibt. Durch eine Dokumentenprüfung prüft ein Evaluator, ob das gebotene Schutzniveau des Cloud-Dienstes für die im Auftrag der Cloud-Nutzer verarbeiteten Daten angemessen ist.

Unterstützend kann im Rahmen eines Audits eine Befragung durchgeführt werden, um die oben genannten Punkte auf Vollständigkeit und Umsetzung im Unternehmen zu überprüfen.

Soweit das Datensicherheitskonzept Sicherheitsmaßnahmen des Cloud-Nutzers verlangt, prüft ein Evaluator, ob diese den Cloud-Nutzer in Schriftform oder in einem elektronischen Format mitgeteilt wurden. Hierzu prüft er vorhandener Protokolle, Verträge, Prozessspezifikationen zur Mitteilung oder andere, relevante Dokumentationen des Cloud-Anbieters. Eine Befragung des verantwortlichen Personals im Rahmen eines Audits hinsichtlich der Bekanntheit der Sicherheitsmaßnahmen des Cloud-Nutzers und Mitteilungsrichtlinien kann durchgeführt werden, um festzustellen, ob auch zukünftig Cloud-Nutzer in diesen Fällen informiert werden. Wird der Cloud-Nutzer elektronisch informiert, bspw. im Rahmen des Online-Registrierungsprozesses des Cloud-Dienstes, kann ein Evaluator durch Inspektion in Form einer Dienstnutzung ebenfalls die konforme Mitteilung des Cloud-Nutzers prüfen.

Aus den vorgelegten Dokumenten muss der Evaluator schließen können, ob das Datensicherheitskonzept aktuell ist und fortlaufend weiterentwickelt wurde und weiterhin wird (bspw. durch Zeitstempel, Versionierungshistorie oder Protokolle der Weiterentwicklung). Auch kann mittels Befragung oder Beobachtung während eines Audits geprüft werden, ob das Datensicherheitskonzept (mindestens jährlich und nach jeder erheblichen Veränderung) aktualisiert und auf Angemessenheit überprüft wird. Falls das Datensicherheitskonzept aktualisiert wurde, prüft der Evaluator ob der Cloud-Kunde vorab informiert wurde (bspw. über Nachrichten, Protokolle etc.).

Weiterhin muss der Evaluator aus den vorgelegten Dokumenten schließen können, dass die eingesetzten Maßnahmen dem Stand der Technik entsprechen und angemessen sind. Die Angemessenheit der einzelnen im Datensicherheitskonzept genannten TOM und ihre Umsetzung werden nach den nachfolgenden Nummern des Katalogs durch einen Evaluator geprüft.

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

Schutzklasse 1

(1) Der Cloud-Anbieter stellt durch risikoangemessene TOM sicher, dass Räume und Anlagen gegen Schädigung durch höhere Gewalt[7] gesichert werden und Unbefugten der Zutritt zu Räumen und Datenverarbeitungsanlagen verwehrt wird, um unbefugte Kenntnisnahmen personenbezogener Daten und Einwirkungsmöglichkeiten auf die Datenverarbeitungsanlagen auszuschließen.

(2) Der Cloud-Anbieter überprüft den Zutritt zu Räumen und Datenverarbeitungsanlagen durch eine Zwei-Faktor-Authentifizierung.

(3) Die Maßnahmen sind geeignet, um den Zutritt Unbefugter aufgrund technischer oder organisatorischer Fehler, einschließlich Bedienfehler, des Cloud-Anbieters oder fahrlässiger Handlungen Dritter auszuschließen. Der Cloud-Anbieter muss mindestens eine Reihe von Sicherheitsanforderungen für jede Sicherheitszone umsetzen und dokumentieren.

(4) Der Cloud-Anbieter überprüft die Erforderlichkeit der Berechtigungen für den Zutritt zu Räumen und Anlagen in regelmäßigen Abständen (mindestens jährlich oder bei wesentlichen Veränderungen) auf Aktualität und Angemessenheit und aktualisiert sie bei Bedarf.

(5) Jeder befugte Zutritt wird protokolliert.

Schutzklasse 2 und 3

(6) Die Kriterien von Schutzklasse 1 sind erfüllt.

[7] Nach einer auf verschiedenen Gebieten des Unionsrechts entwickelten ständigen Rechtsprechung sind unter „höherer Gewalt“ ungewöhnliche und unvorhersehbare Ereignisse zu verstehen, auf die derjenige, der sich darauf beruft, keinen Einfluss hat und deren Folgen trotz Anwendung der gebotenen Sorgfalt nicht hätten vermieden werden können, vgl. ECLI:EU:C:2017:39, Rn. 53.

(7) Zusätzlich ergreift der Cloud-Anbieter geeignete Maßnahmen, um Schädigungen nicht nur durch höhere Gewalt, sondern auch durch fahrlässige Handlungen Befugter auszuschließen. Der Zutritt ist vor vorsätzlichen Handlungen Unbefugter hinreichend sicher geschützt, was Schutz gegen Zutrittsversuche durch bekannte Angriffsszenarien, Täuschung und Gewalt einschließt.

(8) Jeder unbefugte Zutritt und jeder Zutrittsversuch sind nachträglich feststellbar.

Ermittlungsmethoden

- Dokumentprüfung
- Inspektion
- Prüfung
- Audit

Ermittlung

Der Evaluator führt insbesondere eine Durchsicht der relevanten Dokumentation zum Schutz vor Schädigung durch höhere Gewalt und zur Zutrittskontrolle durch, dazu zählt unter anderem die Dokumentation der TOM im Datensicherheitskonzept, Betriebskontinuitätskonzepte, Berechtigungskonzepte, und Verfahrensanweisungen/Konzepte/Richtlinien zu z.B. Wachschutz, Videoüberwachung, Besucherregelungen, Einbruchsmeldeanlagen, Schließsysteme und Berechtigungen.

Die Implementierung der geeigneten TOM zum Schutz vor Schädigung durch höhere Gewalt wird durch repräsentative Stichproben im Rahmen eines Audits festgestellt und auf Angemessenheit überprüft. Die Inspektion und/oder Prüfung oder Besichtigung von Serverräumen und die Beurteilung getroffener Maßnahmen (bspw. Brandfrüherkennungs- und Löschanlagen, Feuchtigkeits- und Temperatursensoren) können durchgeführt werden.

Die Implementierung und der (fortlaufende) Betrieb von Zutrittskontrollen werden im Rahmen von Inspektionen, Prüfungen und eines Vor-Ort-Audits durch repräsentative Stichproben festgestellt und auf Angemessenheit überprüft. Dabei prüft ein Evaluator die Verfügbarkeit und Zuverlässigkeit von definierten Zutrittskontrollen und die Bekanntheit von Anweisungen bei Mitarbeitern, gleicht die Dokumentation mit der tatsächlichen Umsetzung der Maßnahmen vor Ort ab (z.B. Wachschutz aktiv, Videoüberwachung vorhanden, Aufzeichnungen und Protokolle vorhanden), und führt eine Begehung der Standorte durch. Bei dem Vor-Ort-Audit ist die entsprechende Schutzklasse zu berücksichtigen.

Unterstützend kann der Evaluator einen Penetrationstest von Zutrittskontrollsystemen oder ähnliche Sicherheitstests sowie eine Kontrolle der Einbindung derartiger Anlagen in den Sicherheitsprozess durchführen.

In Bezug auf das Personal führt ein Evaluator eine Dokumentprüfung und Befragung im Rahmen eines Audits durch, um festzustellen ob Schulungen und Sensibilisierungsmaßnahmen (bspw. zur Social Engineering Prävention) durchgeführt werden, um auf Kenntnis über entsprechende Verhaltensregeln (z.B. Umgang mit betriebsfremden Personen) zu prüfen, und um die Pflege und Aktualität der Maßnahmendokumentation (z.B. Aktualität von Schlüsselbüchern) zu überprüfen.

Für Schutzklasse 2 und 3 prüft ein Evaluator durch eine Dokumentprüfung die Prozessdokumentation zur Protokollierung von unbefugten Zutritten und Zutrittsversuchen, um festzustellen, ob eine fortlaufende Protokollierung vorgenommen wird. Die tatsächliche Protokollierung kann durch die Inspektion oder Prüfung von Zutritts- und Ereignisprotokollen oder elektronischer Prüfpfade überprüft werden, insofern diese stattgefunden haben. Im Rahmen des Vor-Ort-Audits und einer Befragung oder Beobachtung von Mitarbeitern kann ein Evaluator prüfen, ob unbefugte Zutritte und Zutrittsversuch nachträglich festgestellt werden. Für Schutzklasse 2 und 3 gelten diese Prüfungen analog zur Feststellung, ob auch jeder autorisierte Zutritt protokolliert wurde.

Nr. 2.3 – Zugangskontrolle[8] (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 sicher, dass Unbefugte keinen Zugang zu Datenverarbeitungssystemen erhalten und auf diese einwirken können. Dies gilt auch für Sicherungskopien, soweit diese personenbezogene Daten enthalten.

(2) Der Cloud-Anbieter überprüft die Erforderlichkeit der Berechtigungen für den Zugang zu Datenverarbeitungssystemen in regelmäßigen Abständen (mindestens jährlich oder bei wesentlichen Veränderungen) auf Aktualität und Angemessenheit und aktualisiert sie bei Bedarf.

[8] Der Zugang bezieht sich auf jede Form der Annäherung an Datenverarbeitungssysteme. Im Gegensatz dazu bezieht sich der Zugriff auf jede Form der tatsächlichen Nutzung von Datenverarbeitungssystemen.

(3) Der Cloud-Anbieter überprüft den Zugang von Befugten über das Internet durch eine Zwei-Faktor- Authentifizierung. Der Zugang über das Internet wird über Transportverschlüsselung nach dem Stand der Technik umgesetzt.

Die Maßnahmen zur Zugangskontrolle sind so ausgestaltet um im Regelfall den Zugang zu Datenverarbeitungssystemen durch Unbefugte aufgrund technischer oder organisatorischer Fehler, einschließlich Bedienfehler, des Cloud-Anbieters oder fahrlässiger Handlungen des Cloud-Nutzers oder Dritter auszuschließen. Die Maßnahmen müssen sicherstellen, dass durch die Dokumentation und Umsetzung von Verfahren zur Vergabe, Aktualisierung und Aufhebung von Zugriffsrechten ein unbefugter Zugang zu Datenverarbeitungssystemen verhindert wird.

Schutzklasse 2

(4) Die Kriterien von Schutzklasse 1 sind erfüllt.

(5) Gegen zu erwartenden vorsätzlichen unbefugten Zugang besteht ein Schutz, der zu erwartende Zugangsversuche ausschließt. Dazu gehören insbesondere ein hinreichender Schutz gegen bekannte Angriffsszenarien sowie Maßnahmen, die einen unbefugten Zugang im Regelfall nachträglich feststellbar machen.

Schutzklasse 3

(6) Die Kriterien von Schutzklasse 1 und Schutzklasse 2 sind erfüllt.

(7) Der Cloud-Anbieter schließt den unbefugten Zugang zu Datenverarbeitungssystemen aus. Dies schließt regelmäßig Maßnahmen zur aktiven Erkennung von Angriffen ein. Jeder unbefugte Zugang und entsprechende Versuche sind nachträglich feststellbar.

Ermittlungsmethoden

- Dokumentprüfung
- Inspektion
- Prüfung
- Audit

Ermittlung

Der Evaluator führt eine Durchsicht der Dokumentation zur Zugangskontrolle durch, darunter bspw. Dokumentation der TOM im Datensicherheitskonzept, Berechtigungskonzepte, Verfahrensanweisungen, Richtlinien/Konzepten zu Kennwörtern, Dokumentation zu Authentifizierungs- und Verschlüsselungskonzepten bei dem Zugriff (berechtigter Mitarbeiter), und zu Zugangsberechtigungen.

Die Implementierung und der (fortlaufende) Betrieb von Zugangskontrollen werden im Rahmen eines Vor-Ort-Audits, Inspektionen und Prüfungen durch repräsentative Stichproben festgestellt und auf Angemessenheit gemäß der Schutzklasse überprüft. Durch eine Befragung des Personals im Rahmen des Audits sollte geprüft werden, ob dieses Kenntnis über entsprechende Verhaltensregeln (z.B. des Verbots der Weitergabe von Passwörtern) hat, und ob Maßnahmen auch gemäß der Dokumentation durchgeführt werden (z.B. Prüfung des Entzuges von Zugangsrechten nach Austritt von Mitarbeitern aus der Organisation). Im Rahmen einer Prüfung in Form einer Assetprüfung können auch Zugangsschnittstellen auf Sicherheit überprüft werden (bspw. Sperrung von Computern von Mitarbeitern).

Wird ein Fernzugang über das Internet ermöglicht, so wird dieser gesondert auf Sicherheit und Angemessenheit geprüft. Unterstützend können Sicherheitstests (bspw. Prüfung auf Verschlüsselung) durchgeführt werden.

Aus den vorgelegten Dokumenten muss der Evaluator schließen können, ob das Zugangskonzept und die Berechtigungen aktuell sind und fortlaufend aktualisiert werden (bspw. durch Zeitstempel, Versionierungshistorie oder Protokolle der Aktualisierung). Auch kann strichprobenartig die Aktualität und Angemessenheit von Berechtigung überprüft werden. Mittels Befragung oder Beobachtung während eines Audits kann geprüft werden, ob Prozesse zur Aktualisierung der Zugangsberechtigungen durchgeführt werden und Mitarbeiter die entsprechenden Richtlinien kennen.

Für Schutzklasse 2 und 3 prüft ein Evaluator durch eine Dokumentprüfung die Prozessdokumentation zur Feststellung von unbefugten Zugängen. Die tatsächliche Feststellung im Regelfall kann durch die Inspektion oder Prüfung von Zugangs- und Ereignisprotokollen oder elektronischer Prüfpfade überprüft werden, insofern unbefugte Zugänge stattgefunden haben. Im Rahmen des Vor-Ort-Audits und einer Befragung oder Prüfung kann ein Evaluator prüfen, ob unbefugte Zugänge im Regelfall nachträglich festgestellt werden können. Für Schutzklasse 3 prüft ein Evaluator analog, ob jeder unbefugte Zugang und entsprechende Versuche nachträglich feststellbar sind.

Nr. 2.4 – Zugriffskontrolle[9]
(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 personenbezogene Daten nehmen können und unbefugte Einwirkungen auf personenbezogene Daten ausgeschlossen werden. Dies gilt auch für Datensicherungen, soweit sie personenbezogene Daten enthalten.

(2) Der Cloud-Anbieter ermöglicht es dem Cloud-Nutzer, dass dieser verschiedene zweckbezogene Nutzerrollen für seine Mitarbeiter festlegen kann, um unbefugte Zugriffe auf personenbezogene Daten logisch auszuschließen.

(3) Der Cloud-Anbieter überprüft die Erforderlichkeit der Berechtigungen für den Zugriff auf personenbezogene Daten in regelmäßigen Abständen (mindestens jährlich oder bei wesentlichen Veränderungen) auf Aktualität und Angemessenheit und aktualisiert sie bei Bedarf.

(4) Der Cloud-Anbieter kontrolliert (d.h. überwacht und bewertet) und protokolliert alle Zugriffe auf personenbezogene Daten.

(5) Die Maßnahmen sind geeignet, um im Regelfall den Zugriff auf personenbezogene Daten durch Unbefugte aufgrund technischer oder organisatorischer Fehler, einschließlich Bedienfehler, des Cloud-Anbieters oder fahrlässiger Handlungen des Cloud-Nutzers oder Dritter auszuschließen Die Maßnahmen müssen sicherstellen, dass vorsätzliche Eingriffe in der Regel verhindert werden.

(6) Für Zugriffe von Befugten auf personenbezogene Daten über das Internet ist eine Zwei Faktor-Authentifizierung erforderlich.

(7) Der Cloud-Anbieter schützt administrative Zugriffe und Tätigkeiten auf kritischen Systemen durch einen starken Authentisierungsmechanismus und protokolliert diese. Die Fernadministration des Cloud-Dienstes durch Mitarbeiter des Cloud-Anbieters erfolgt über einen verschlüsselten Kommunikationskanal.

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

Schutzklasse 2

(9) Die Kriterien von Schutzklasse 1 sind erfüllt.

(10) Zu erwartende vorsätzliche unbefugte Zugriffe sind ausgeschlossen. Dazu gehören insbesondere ein hinreichender Schutz gegen bekannte Angriffsszenarien sowie Maßnahmen, durch die ein unberechtigter Zugriff im Regelfall nachträglich festgestellt werden kann.

(11) Sofern ein privilegierter Zugriff vorliegt, darf dieser nur in Rollen erfolgen, die von der Administration und vom Rechenzentrumsbetrieb unabhängig sind. Der privilegierte Zugriff ist mit Zwei-Faktor-Authentifizierung abzusichern und die Anzahl der Mitarbeiter mit privilegiertem Zugriff ist so gering wie möglich zu halten.

Schutzklasse 3

(12) Die Kriterien von Schutzklasse 1 und Schutzklasse 2 sind erfüllt.

(13) Unbefugte Zugriffe auf Daten sind bezogen auf die Ergebnisse der Risikoanalyse ausgeschlossen. Dies schließt regelmäßig manipulationssichere technische Maßnahmen zur Prävention und aktiven Erkennung von Angriffen ein. Jeder unbefugte Zugriff und entsprechende Versuche sind nachträglich feststellbar.

Ermittlungsmethoden

- Dokumentprüfung
- Inspektion
- Prüfung
- Audit

[9] Der Zugriff bezieht sich auf jede Form der tatsächlichen Nutzung von Datenverarbeitungssystemen. Im Gegensatz dazu bezieht sich der Zugang auf jede Form der Annäherung an Datenverarbeitungssysteme.

Ermittlung

Ein Evaluator führt eine Durchsicht der Dokumentation zur Zugriffskontrolle durch, darunter Dokumentation der TOM im Datensicherheitskonzept, Berechtigungskonzepte, Verfahrensanweisungen, Regelungen für privilegierten Zugriffe und Zugriffsrichtlinien. Hierbei wird insb. auch geprüft, ob Cloud-Nutzer verschiedene zweckbezogene Nutzerrollen festlegen können.

Insofern ein privilegierter Zugriff der Mitarbeiter des Cloud-Anbieters auf personenbezogene Daten auf Weisung des Cloud-Nutzers gegeben ist, so prüft ein Evaluator die rechtverbindlichen Vereinbarungen mit dem Cloud-Nutzer oder andere Dokumente zur Weisungsbeauftragung durch den Cloud-Nutzer, ob die Weisungen hierzu dokumentiert und geregelt sind. Im Rahmen eines Audits können auch Mitarbeiterbefragungen durchgeführt werden, um festzustellen, ob der privilegierte Zugriff nur in Rollen erfolgt, die von der Administration und vom Rechenzentrumsbetrieb unabhängig sind.

Wird ein Fernzugang über das Internet ermöglicht, so wird dieser gesondert auf Sicherheit und Angemessenheit geprüft. Hierzu können Sicherheitstests (bspw. Prüfung auf Verschlüsselung) durchgeführt werden. Auch sollten Sicherheitstests durchgeführt werden, um zu prüfen ob administrative Zugriffe und Tätigkeiten auf kritischen Systemen ausreichend stark gesichert sind. Ein Evaluator prüft stichprobenartig vorgelegte Protokolle oder Auszüge aus Datenbanken, um sicherzustellen, dass administrative Zugriffe und Tätigkeiten auf kritischen Systemen protokolliert werden.

Die Implementierung von TOM zur Zugriffskontrolle wird im Rahmen von Inspektionen, Prüfungen und ein Vor-Ort-Audit durch repräsentative Stichproben festgestellt und auf Angemessenheit gemäß der Schutzklasse überprüft. Bei der Inspektion und Prüfung können insbesondere eine Vorgangsüberwachung und die Durchführung von Datenverarbeitungsvorgängen, und bei Bedarf eine Assetprüfung durchgeführt werden. Dabei sind bspw. die Firewallkonfiguration, VPN-Zugänge, Telearbeitsplätze, Authentisierungen, und Verschlüsselungen zu testen. Auch können testweise administrative Tätigkeiten durchgeführt und ihre Protokollierung überprüft werden.

Durch eine Befragung des Personals während des Audits sollte geprüft werden, ob diese Kenntnis über entsprechende Verhaltensregeln haben (z.B. des Verbots der Weitergabe von Passwörtern), und ob Maßnahmen auch gemäß der Dokumentation durchgeführt werden (z.B. Prüfung des Entzuges von Zugriffsrechten nach Austritt von Mitarbeitern aus der Organisation). Auch kann eine Fernadministration durch Mitarbeiter testweise beobachtet werden, um die Einhaltung der Kriterien zu inspizieren.

Aus den vorgelegten Dokumenten muss der Evaluator schließen können, ob das Zugriffskonzept und die Berechtigungen aktuell sind und fortlaufend aktualisiert werden (bspw. durch Zeitstempel, Versionierungshistorie oder Protokolle der Aktualisierung). Auch kann strichprobenartig die Aktualität und Angemessenheit von Berechtigung überprüft werden. Mittels Befragung oder Beobachtung während eines Audits kann geprüft werden, ob Prozesse zur Aktualisierung der Zugriffsberechtigungen durchgeführt werden und Mitarbeiter die entsprechenden Richtlinien kennen.

Für Schutzklasse 2 und 3 prüft ein Evaluator durch eine Dokumentprüfung die Prozessdokumentation zur Feststellung von unbefugten Zugriffen. Die tatsächliche Feststellung im Regelfall kann durch die Inspektion oder Prüfung von Zugriffs- und Ereignisprotokollen oder elektronischer Prüfpfade überprüft werden, insofern unbefugte Zugriffe stattgefunden haben. Im Rahmen des Vor-Ort-Audits und einer Befragung oder Prüfung kann ein Evaluator prüfen, ob unbefugte Zugriffe im Regelfall nachträglich festgestellt werden können. Für Schutzklasse 3 prüft ein Evaluator analog, ob jeder unbefugte Zugriff und entsprechende Versuche nachträglich feststellbar sind.

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 und Abs. 2 DSGVO)

Kriterium

Schutzklasse 1

(1) Der Cloud-Anbieter setzt bei Datenübertragungsvorgängen eine Transportverschlüsselung nach dem Stand der Technik ein oder fordert dies durch entsprechende Konfiguration von Schnittstellen. Er muss zudem die offiziellen Normen oder die dem Stand der Technik entsprechenden Spezifikationen dokumentieren, die er zur Festlegung seiner TOM in Bezug auf Transportverschlüsselung nutzt. Die eingesetzte Transportverschlüsselung muss gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

(2) Die Maßnahmen sind geeignet, im Regelfall Angriffe 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 sind ferner geeignet, die fahrlässige Weitergabe von Daten an Unbefugte durch den Cloud-Anbieter und seine Mitarbeiter auszuschließen. Schutzmaßnahmen verhindern vorsätzliche Eingriffe. Bei verschlüsselter Übertragung sind die Schlüssel gemäß offizieller Normen oder des Standes der Technik sicher aufzubewahren und der Zugriff zum Schlüssel muss kontrolliert werden (Nr. 2.4).

(3) Der Cloud-Anbieter protokolliert automatisiert die Metadaten[10] aller Datenübertragungsvorgänge, einschließlich der Empfänger, auch solche vom und an den Cloud-Nutzer oder an Subauftragsverarbeiter. Nr. 2.6 (1) findet entsprechende Anwendung.

(4) Die Anforderungen dieses Kriteriums gelten auch für die Übertragung von Daten im eigenen Netzwerk des Cloud-Anbieters und seiner Subauftragsverarbeiter und zwischen diesen.

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

Schutzklasse 2

(6) Die Kriterien von Schutzklasse 1 sind erfüllt.

(7) Der Cloud-Anbieter schützt die Daten gegen vorsätzliches unbefugtes Lesen, Kopieren, Verändern oder Entfernen und schließt zu erwartende Versuche aus. Zu den Schutzmaßnahmen 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.

Schutzklasse 3

(8) Die Kriterien von Schutzklasse 1 und Schutzklasse 2 sind erfüllt.

(9) Der Cloud-Anbieter schließt unbefugtes Lesen, Kopieren, Verändern oder Entfernen von aus. Er ergreift regelmäßig Maßnahmen zur aktiven Erkennung und Abwehr von Angriffen und stellt jedes unbefugte Lesen, Kopieren, Verändern oder Entfernen von Daten und auch jeden entsprechenden Versuch nachträglich fest.

Ermittlungsmethoden

- Dokumentprüfung
- Prüfung
- Audit

Ermittlung

Ein Evaluator führt eine Durchsicht der Dokumentation zur Übertragung von Daten und Transportverschlüsselung durch, darunter bspw. die der TOM im Datensicherheitskonzept, Verfahrensanweisungen, Richtlinien, Protokoll- und Logdaten, Ergebnisprotokolle interner/externer Audits, Dokumentationen zum Stand der Technik, Übersicht zu eingesetzten Sicherheitsscannern, Dokumentation des Infrastrukturzugriffs via APIs, Dokumente zum Schlüsselmanagement (insb. Zugriff und Verwahrung der Schlüssel), Dokumente zum Transport von Datenträgern, und Dokumentation der Prozesse zur Datenweitergabe.

Es muss ein Abgleich der Dokumentation mit der tatsächlichen Umsetzung der Maßnahmen durchgeführt werden. Dabei sollte die Wirksamkeit und Aktualität der Verschlüsselung oder anderen Maßnahmen mit geeigneten Sicherheitstests (z.B. Penetrationstests) oder anderen technischen Mitteln überprüft werden. Der Evaluator prüft Protokolle über Metadaten aller Datenübertragungsvorgänge stichprobenartig für jeweils Übertragungen an den Cloud-Nutzer und an den Subauftragsverarbeiter und im eigenen Netzwerk. Falls ein Transport von Datenträgern vorgenommen wurde, prüft ein Evaluator die Protokolle zu den Transporten.

Auch eine Befragung der Mitarbeiter z.B. in Hinblick auf die Kenntnis der relevanten Richtlinien und Anweisungen und eine Stichprobenprüfung der Reaktion relevanter Mitarbeiter zur Umsetzung festgelegter Richtlinien und Anweisungen sollte durchgeführt werden.

Für Schutzklasse 2 und 3 prüft ein Evaluator durch eine Dokumentprüfung die Dokumentation zur Feststellung von unbefugten Lesen, Kopieren, Verändern oder Entfernen von personenbezogenen Daten. Die tatsächliche Feststellung im Regelfall kann durch die Prüfung von Ereignisprotokollen, Protokollen zur Abwehr und Erkennung von Angriffen, oder elektronischer Prüfpfade überprüft werden, insofern unbefugte Tätigkeiten stattgefunden haben. Für Schutzklasse 3 prüft ein Evaluator analog, ob jedes unbefugte Lesen, Kopieren, Verändern oder Entfernen von Daten und entsprechende Versuche nachträglich feststellbar sind.

[10] Metadaten beziehen sich auf Informationen, die andere Daten beschreiben. Sie liefern Kontext, Attribute und Details zu einem bestimmten Datensatz und helfen dabei, diesen zu organisieren, zu verstehen und zu verwalten. Einfacher ausgedrückt: Metadaten sind Daten über Daten.

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, f und Abs. 2 DSGVO)

Kriterium

Schutzklasse 1

(1) Der Cloud-Anbieter protokolliert Eingaben, Veränderungen und Löschungen personenbezogener Daten, die bei der bestimmungsgemäßen Nutzung des Cloud-Dienstes durch den Cloud-Nutzer oder bei administrativen Maßnahmen des Cloud-Anbieters erfolgen, um eine nachträgliche Prüfbarkeit und Nachvollziehbarkeit der Datenverarbeitung sicherzustellen. Er beachtet bei Protokollierungen die Grundsätze der Erforderlichkeit, Zweckbindung, Datenminimierung und Speicherbegrenzung. Der Cloud-Anbieter muss die Protokolldaten sicher aufbewahren.

(2) Der Cloud-Anbieter gestaltet die Protokollierung so, 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. Er sieht einen Mindestschutz gegen vorsätzliche Manipulationen an den Maßnahmen zur Nachvollziehbarkeit vor, der solche Manipulationen erschwert, indem zumindest alle Protokolldaten in einer integritätsgeschützten Form gespeichert werden, die ihre Auswertung ermöglicht.

(3) Der Cloud-Anbieter muss Verfahren zur Analyse und Überprüfung von Protokollen einrichten, um Anomalien und Vorfälle effektiv erkennen und in der Folge einen Alarm auslösen zu können. Er muss derartige Ereignisse bei der Prüfung der Risikoanalyse miteinbeziehen (Nr. 2.1 [6]).

Schutzklasse 2

(4) Die Kriterien von Schutzklasse 1 sind erfüllt.

(5) Der Cloud-Anbieter sieht gegen zu erwartende vorsätzliche Manipulationen der Protokollierungsinstanzen und gegen vorsätzliche Zugriffe auf oder Manipulationen von Protokollierungsdateien (Logs) durch Unbefugte einen Schutz vor, der zu erwartende Manipulationsversuche ausschließt. Zu diesen Schutzmaßnahmen gehören insbesondere ein hinreichender Schutz gegen bekannte Angriffsszenarien sowie Maßnahmen, durch die eine Manipulation im Regelfall (nachträglich) festgestellt werden kann.

Schutzklasse 3

(6) Die Kriterien von Schutzklasse 1 und Schutzklasse 2 sind erfüllt.

(7) Der Cloud-Anbieter schließt Manipulationen von Protokollierungsinstanzen und -dateien (Logs) aus. Er ergreift regelmäßig Maßnahmen zur aktiven Erkennung von Manipulationen und stellt jede Manipulation und auch jeden entsprechenden Versuch nachträglich fest.

Ermittlungsmethoden

- Dokumentprüfung
- Inspektion
- Prüfung
- Audit

Ermittlung

Zur Prüfung des Kriteriums führt ein Evaluator eine Dokumentprüfung durch, indem er (im Datensicherheitskonzept) prüft, wie ein Cloud-Anbieter durch Festlegung von Gegenstand und Umfang der Protokollierung, Aufbewahrung, Integritätsschutz und Löschung von Protokollen und der Verwendung der Protokolldaten die Datenschutzziele sicherstellt. Weitere Dokumente können Berechtigungskonzepte (insb. Nutzer- und Administratorenberechtigungen), Verfahrensanweisungen, Richtlinien, Protokoll- und Logdaten, Ergebnisprotokolle interner/externer Audits, und Risikoanalysen sein. Hierzu zählen auch Dokumentationen über die Anwendung von Verfahren zur Überprüfung von Protokollen (bspw. durchgeführte Anomalieprüfungen, ausgelöste Alarme etc.).

Die Implementierung dieses Protokollierungskonzepts und Verfahren zur Analyse und Überprüfung werden durch repräsentative Stichproben im Rahmen des laufenden Betriebs festgestellt und auf Angemessenheit überprüft. Insbesondere sollte durch eine Inspektion in Form einer Vorgangsüberwachung festgestellt werden, ob entsprechende Protokolleinträge bei Eingaben, Veränderungen und Löschungen personenbezogener Daten erzeugt werden. Durch die Verwendung von Sicherheitstests können auch angewendete Schutzmaßnahmen von Protokollen gegen Manipulation überprüft werden.

Unterstützend kann eine Befragung von Mitarbeitern im Rahmen eines Audits zusätzlich zum Abgleich der in der Dokumentation spezifizierten mit der tatsächlichen Durchführung der Maßnahmen durchgeführt werden.

Für Schutzklasse 2 und 3 prüft ein Evaluator durch eine Dokumentprüfung die Dokumentation zur Feststellung von Manipulationen der Protokollierungen. Die tatsächliche Feststellung im Regelfall kann durch die Inspektion oder

Prüfung von Ereignisprotokollen, Protokollen zur Abwehr und Erkennung von Manipulationen, oder elektronischer Prüfpfade überprüft werden, insofern Manipulationen stattgefunden haben. Für Schutzklasse 3 prüft ein Evaluator analog, ob jede Manipulation und möglichst auch jeder entsprechender Versuch nachträglich feststellbar sind.

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

Kriterium

Schutzklasse 1

(1) Der Cloud-Anbieter ermöglicht es dem Cloud-Nutzer, Daten zu verarbeiten, die der Cloud-Nutzer pseudonymisiert überträgt.

(2) Erfordert die Art des Auftrags mit dem Cloud-Nutzer die De-Pseudonymisierung der Daten, stellt der Cloud-Anbieter sicher, dass die De-Pseudonymisierung nur auf dokumentierte Weisung des Cloud-Nutzers erfolgt.

Schutzklasse 2 und 3

(3) Die Kriterien von Schutzklasse 1 sind erfüllt.

(4) Soweit mit dem Cloud-Nutzer vereinbart (Nr. 1.7), stellt der Cloud-Anbieter sicher, dass die Daten pseudonymisiert verarbeitet werden. Entsprechend der rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung pseudonymisiert der Cloud-Nutzer die personenbezogenen Daten selbst oder der Cloud-Anbieter führt die Pseudonymisierung auf Weisung des Cloud-Nutzers durch.

(5) Wird die Pseudonymisierung vom Cloud-Anbieter durchgeführt, so stellt dieser sicher, dass die zusätzlichen Informationen zur Identifizierung der betroffenen Person gesondert aufbewahrt werden. Der Datensatz mit der Zuordnung des Kennzeichens zu einer Person muss so geschützt werden, dass zu erwartende Manipulationsversuche ausgeschlossen werden.

(6) Ist die Pseudonymisierung der Daten auf Weisung des Cloud-Nutzers nicht gegenüber allen Mitarbeitern des Cloud-Anbieters wirksam, ist der Kreis der privilegierten Mitarbeiter auf das unbedingt Erforderliche zu begrenzen.

(7) Der Cloud-Anbieter gewährleistet, dass er die technische Entwicklung im Bereich der Pseudonymisierungsverfahren laufend verfolgt (mindestens jährlich) und seine Verfahren dem Stand der Technik[11] entsprechen (wie in den Umsetzungshinweisen beschrieben).

Ermittlungsmethoden

- Dokumentprüfung
- Inspektion
- Prüfung
- Audit

Ermittlung

Für Schutzklasse 1 prüft ein Evaluator Dokumentationen über den Prozess der Datenverarbeitung, insbesondere im Hinblick auf pseudonymisierte Daten. Im Rahmen einer Inspektion kann eine testweise Dienstnutzung mit pseudonymisierten Daten durchgeführt und die anschließende erfolgreiche Verarbeitung festgestellt werden. Erfordert die Art des Auftrags mit dem Cloud-Nutzer die De-Pseudonymisierung der Daten, prüft ein Evaluator die rechtsverbindliche Vereinbarung mit dem Cloud-Nutzer oder andere Dokumente zur Weisungserteilung des Cloud-Nutzers, ob die De-Pseudonymisierung nur auf dokumentierte Weisung des Cloud-Nutzers erfolgt. Im Rahmen einer Prüfung in Form einer Assetprüfung stellt der Evaluator fest, ob der dokumentierten Weisung bei der De-Pseudonymisierung entsprochen wird.

Für Schutzklasse 2 und 3 prüft der Evaluator das Datensicherheitskonzept, darunter wie Pseudonymisierungen vorgenommen, Identifizierungsdaten sicher aufbewahrt und gegen Manipulation geschützt, und pseudonymisierte Daten verarbeitet werden (bspw. Prüfung von Dokumentationen der TOM, Verfahrensanweisungen, Richtlinien, Protokoll- und Logdaten, Ergebnisprotokolle interner/externer Audits, und der Risikoanalyse).

Die Implementierung der Pseudonymisierungsverfahren wird für Schutzklasse 2 und 3 im Rahmen einer Inspektion und/oder Prüfung durch repräsentative Stichproben festgestellt und auf Angemessenheit überprüft. Ebenso wird

[11] Der Stand der Technik umfasst das, was derzeit als beste Praktiken, Technologien, Methoden und Strategien zum Schutz von Informationssystemen allgemein anerkannt ist. Der Stand der Technik bedeutet nicht notwendigerweise die technologisch fortschrittlichste Lösung, sondern umfasst robuste Technologien und Prozesse sowie qualifiziertes Personal, um wirksam gegen die sich fortentwickelnden Datenschutzbedrohungen zu schützen.

die korrekte Verarbeitung der pseudonymen Daten durch eine Prüfung festgestellt. Dazu sollten die Art der eingesetzten Programme, die Programmierungen zur Pseudonymisierung und deren Konfiguration im Rahmen einer Assetprüfung überprüft werden, und eine stichprobenartige Prüfung von Datensätzen durchgeführt werden.

Eine Überprüfung der Wirksamkeit der Maßnahmen zum Schutz der zusätzlichen Informationen zur Identifizierung ist ebenfalls für Schutzklasse 2 und 3 erforderlich. Hierzu können auch unterstützend Sicherheitstests Anwendung finden (bspw. Schwachstellen- und Penetrationstests).

Eine Befragung von Mitarbeitern im Rahmen eines Audits kann zusätzlich zum Abgleich der in der Dokumentation spezifizierten mit der tatsächlichen Durchführung der Maßnahmen für Schutzklasse 2 und 3 durchgeführt werden (bspw. Befolgung von Richtlinien und Schutzmaßnahmen, Bekanntheit der Weisungen zur De-Pseudonymisierung).

Durch eine Dokumentenprüfung (bspw. Protokolle, Versionierungshistorie) prüft der Evaluator für Schutzklasse 2 und 3, ob der Cloud-Anbieter die technische Entwicklung im Bereich der Pseudonymisierungsverfahren laufend verfolgt. Dies kann auch im Rahmen einer Assetprüfung bei einer Prüfung (bspw. Nachweis über Änderungen am Programmcode zur Pseudonymisierung, Aktualisierung von Bibliotheken etc.) festgestellt werden. Durch eine Befragung der Mitarbeiter sollte ebenfalls überprüft werden, ob diese die aktuellen Empfehlungen zur Pseudonymisierung kennen und umsetzten.

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

Kriterium

Schutzklasse 1

(1) Der Cloud-Anbieter stellt durch implementierte TOMs[12] sicher, dass Anonymisierung[13] (d.h. eine Re-Identifizierung personenbezogener Daten in einem anonymisierten Datensatz) nicht rückgängig gemacht werden kann.

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 zur Datenverarbeitung anonymisiert der Cloud-Nutzer die personenbezogenen Daten selbst oder der Cloud-Anbieter auf Weisung.

(3) Wird die Anonymisierung vom Cloud-Anbieter durchgeführt, so gewährleistet er, dass er die technische Entwicklung im Bereich der Anonymisierungsverfahren laufend verfolgt und seine Verfahren dem Stand der Technik[14] entsprechen.

Ermittlungsmethoden

- Dokumentprüfung
- Inspektion
- Prüfung
- Audit

Ermittlung

Für Schutzklasse 1 prüft ein Evaluator Dokumentationen über den Prozess der Datenverarbeitung, insbesondere im Hinblick auf anonyme Daten. Im Rahmen einer Inspektion kann eine testweise Dienstnutzung mit anonymen Daten durchgeführt und die anschließende erfolgreiche Verarbeitung festgestellt werden. Der Evaluator prüft vor-

[12] Technische Schutzmaßnahmen können die Verhinderung von automatischer Datenaggregation, -synthese usw. umfassen, die zur Aufhebung der Anonymisierung führen könnten, sowie die Verwaltung der Zugriffsrechte der autorisierten Mitarbeiter, um böswilliges Verhalten zu verhindern. Organisatorische Schutzmaßnahmen stellen u. a. sicher, dass Mitarbeiter kein Verhalten an den Tag legen, das auf die Aufhebung der Anonymisierung abzielt, wie z. B. das Ausfragen von Cloud-Nutzern über ihre Anonymisierungspraktiken, um potenzielle Schwachstellen oder Schwachpunkte der angewandten Anonymisierungstechniken auszunutzen.

[13] TOMs in Bezug auf die Anonymisierung müssen daher offiziellen Normen oder dem Stand der Technik entsprechen.

[14] Der Stand der Technik umfasst das, was derzeit als beste Praktiken, Technologien, Methoden und Strategien zum Schutz von Informationssystemen allgemein anerkannt ist. Der Stand der Technik bedeutet nicht notwendigerweise die technologisch fortschrittlichste Lösung, sondern umfasst robuste Technologien und Prozesse sowie qualifiziertes Personal, um wirksam gegen die sich fortentwickelnden Datenschutzbedrohungen zu schützen.

gelegte Dokumentationen über implementierte TOMs, welche sicherstellen, dass eine Anonymisierung nicht rückgängig gemacht werden kann. Eine Befragung von Mitarbeiter kann ebenfalls durchgeführt werden, um herauszufinden, ob die Wahrung der Anonymisierung sichergestellt wird.

Für Schutzklasse 2 und 3 führt ein Evaluator eine Dokumentprüfung durch, bspw. prüft er im Datensicherheitskonzept, wie der Cloud-Anbieter Anonymisierungen durchführt und anonymisierte Daten verarbeitet. Der Evaluator führt eine Durchsicht der Dokumentation zur eingesetzten/angebotenen Anonymisierungsverfahren (z.B. Dokumentation der TOM, Verfahrensanweisungen, Richtlinien, Protokoll- und Logdaten, Ergebnisprotokolle interner/externer Audits und Risikoanalyse) durch.

Die Implementierung der Anonymisierungsverfahren wird für Schutzklasse 2 und 3 im Rahmen einer Inspektion und/oder Prüfung durch repräsentative Stichproben festgestellt und auf Angemessenheit überprüft. Ebenso wird die korrekte Verarbeitung der anonymen Daten durch eine Prüfung festgestellt. Dazu sollten die Art der eingesetzten Programme, die Programmierungen zur Anonymisierung und deren Konfiguration im Rahmen einer Assetprüfung überprüft werden, und eine stichprobenartige Prüfung von Datensätzen durchgeführt werden.

Eine Befragung von Mitarbeitern im Rahmen eines Audits kann zusätzlich zum Abgleich der in der Dokumentation spezifizierten mit der tatsächlichen Durchführung der Maßnahmen für Schutzklasse 2 und 3 durchgeführt werden (bspw. Befragung hinsichtlich der Richtlinien und Regelungen zur Anonymisierung).

Durch eine Dokumentenprüfung (bspw. Protokolle, Versionierungshistorie) prüft der Evaluator für Schutzklasse 2 und 3, ob der Cloud-Anbieter die technische Entwicklung im Bereich der Anonymisierung laufend verfolgt. Dies kann auch im Rahmen einer Assetprüfung bei einer Prüfung (bspw. Nachweis über Änderungen am Programmcode zur Anonymisierung, Aktualisierung von Bibliotheken etc.) festgestellt werden. Durch eine Befragung der Mitarbeiter im Rahmen eines Audits sollte ebenfalls überprüft werden, ob diese die aktuellen Empfehlungen zur Anonymisierung kennen und umsetzten.

Nr. 2.9 – Verschlüsselung gespeicherter Daten[15] (Art. 32 Abs. 1 lit. a DSGVO)

Kriterium

Schutzklasse 1

(1) Der Cloud-Anbieter ermöglicht dem Cloud-Nutzer die Speicherung von verschlüsselten Daten.

(2) Sofern der Cloud-Anbieter Verfahren zur Verschlüsselung anbietet, muss er die Kriterien der Schutzklasse 2 erfüllen.

Schutzklasse 2

(3) Sofern der Cloud-Anbieter personenbezogene Daten des Cloud-Nutzers speichert, bietet er Verschlüsselungsverfahren an, um dem Cloud-Nutzer die Speicherung von verschlüsselten Daten zu ermöglichen oder auf dessen Weisung hin, die Daten selbst zu verschlüsseln.

(4) Ist die Verschlüsselung des Cloud-Anbieters auf Weisung des Cloud-Nutzers nicht gegenüber allen Mitarbeitern des Cloud-Anbieters wirksam, ist die Anzahl der privilegierten Mitarbeiter auf das unbedingt Erforderliche zu begrenzen.

(5) Der Cloud-Anbieter verfolgt laufend die technische Entwicklung im Bereich der Verschlüsselung. Die von ihm getroffenen Maßnahmen, insbesondere ein sicheres Schlüsselmanagement, entsprechen dem Stand der Technik[16] (wie in den Umsetzungshinweisen beschrieben).

(6) Der Cloud-Anbieter prüft fortdauernd die Eignung seiner Verschlüsselungsverfahren und aktualisiert diese bei Bedarf.

(7) Der Cloud-Anbieter überprüft die angemessene Implementierung seiner Verschlüsselungsverfahren durch geeignete Tests und dokumentiert diese.

Schutzklasse 3

(8) Es gelten die Kriterien der Schutzklasse 2. Zusätzlich werden unberechtigte Zugriffe auf den Schlüssel durch geeignete TOM ausgeschlossen.

[15] Gespeicherte Daten umfassen auch die Backups gespeicherter Daten.

[16] Der Stand der Technik umfasst das, was derzeit als beste Praktiken, Technologien, Methoden und Strategien zum Schutz von Informationssystemen allgemein anerkannt ist. Der Stand der Technik bedeutet nicht notwendigerweise die technologisch fortschrittlichste Lösung, sondern umfasst robuste Technologien und Prozesse sowie qualifiziertes Personal, um wirksam gegen die sich fortentwickelnden Datenschutzbedrohungen zu schützen.

(9) Erfolgt die Verschlüsselung durch den Cloud-Nutzer, unterstützt der Cloud-Anbieter diesen auf dessen Weisung hin bei der Verschlüsslung und Entschlüsselung der Daten. Die Unterstützung erfolgt in Form von Dokumentationen und Hilfsmaßnahmen zur Durchführung von Verschlüsselung.

(10) Der Cloud-Anbieter stellt sicher, dass seine unterstützenden Maßnahmen in Form von Dokumentationen und Hilfsmaßnahmen zur Durchführung von Verschlüsselung dem Stand der Technik[17] (wie in den Umsetzungshinweisen beschrieben) entsprechen.

Ermittlungsmethoden

- Dokumentprüfung
- Inspektion
- Prüfung
- Audit

Ermittlung

Für Schutzklasse 1 prüft ein Evaluator Dokumentationen über den Prozess der Datenverarbeitung, insbesondere im Hinblick auf die Speicherung verschlüsselter Daten. Im Rahmen einer Inspektion kann eine testweise Dienstnutzung mit verschlüsselten Daten durchgeführt und die anschließende erfolgreiche Speicherung festgestellt werden.

Für Schutzklasse 2 und 3 führt ein Evaluator eine Dokumentprüfung durch, bspw. prüft er im Datensicherheitskonzept, ob die angebotenen und angewandten Verschlüsselungsverfahren den aktuellen technischen Anforderungen entsprechen. Der Evaluator führt eine Durchsicht der Dokumentation zur eingesetzten Verschlüsselungsverfahren (z.B. Dokumentation der TOM, Verfahrensanweisungen, Richtlinien, Protokoll- und Logdaten, Ergebnisprotokolle interner/externer Audits, Risikoanalyse) durch.

Die Implementierung der Verschlüsselungsverfahren wird für Schutzklasse 2 und 3 im Rahmen einer Inspektion und/oder Prüfung durch repräsentative Stichproben festgestellt und auf Angemessenheit überprüft. Ebenso wird die korrekte Speicherung der verschlüsselten Daten durch eine Prüfung festgestellt. Dazu sollten die Art der eingesetzten Programme, die Programmierungen zur Verschlüsselung und deren Konfiguration im Rahmen einer Assetprüfung überprüft werden, und eine stichprobenartige Prüfung von Datensätzen durchgeführt werden. Die Implementierung und Sicherheit der Verschlüsselungsverfahren wird durch repräsentative technische Tests (z.B. Penetrationstests) festgestellt und auf Angemessenheit überprüft.

Eine Befragung von Mitarbeitern im Rahmen eines Audits kann zusätzlich zum Abgleich der in der Dokumentation spezifizierten mit der tatsächlichen Durchführung der Maßnahmen für Schutzklasse 2 und 3 durchgeführt werden (bspw. Befragung hinsichtlich der Richtlinien und Regelungen zur Verschlüsselung).

Durch eine Dokumentenprüfung (bspw. Protokolle, Versionierungshistorie) prüft der Evaluator für Schutzklasse 2, ob der Cloud-Anbieter die technische Entwicklung im Bereich der Verschlüsselung laufend verfolgt und die Geeignetheit des Verfahrens fortdauernd prüft und das Verfahren sowie die Dokumentation gegebenenfalls aktualisiert. Dies kann auch im Rahmen einer Assetprüfung bei einer Prüfung (bspw. Nachweis über Änderungen am Programmcode zur Verschlüsselung, Aktualisierung von Bibliotheken etc.) festgestellt werden. Durch eine Befragung der Mitarbeiter im Rahmen eines Audits sollte ebenfalls überprüft werden, ob diese die aktuellen Empfehlungen zur Verschlüsselung kennen und umsetzten. Ein Evaluator prüft anhand von Protokollen, ob der Cloud-Anbieter die Verschlüsselungstechniken durch geeignete technische Tests geprüft hat.

Für Schutzklasse 3 prüft der Evaluator Zugriffs- und Ereignisprotokolle für den Zugriff auf Schlüssel. Ein Evaluator kann weitere Dokumente für Schutzklasse 3 prüfen, wie bspw. die Nutzerdokumentation zur Ver-/Entschlüsselung, Dokumentation von Verschlüsselungsverfahren und Protokolle eines qualifizierten (ggf. durch Schulungen nachzuweisen) IT-Sicherheitsgremiums, in dem auch regelmäßig die technischen Verfahren zur Ver-/Entschlüsselung reflektiert werden.

[17] Der Stand der Technik umfasst das, was derzeit als beste Praktiken, Technologien, Methoden und Strategien zum Schutz von Informationssystemen allgemein anerkannt ist. Der Stand der Technik bedeutet nicht notwendigerweise die technologisch fortschrittlichste Lösung, sondern umfasst robuste Technologien und Prozesse sowie qualifiziertes Personal, um wirksam gegen die sich fortentwickelnden Datenschutzbedrohungen zu schützen.

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 DSGVO)

Kriterium

Schutzklasse 1

(1) Der Cloud-Anbieter verarbeitet die Daten des Cloud-Nutzers logisch oder physisch getrennt von den Datenbeständen anderer Cloud-Nutzer und von anderen Datenbeständen des Cloud-Anbieters und ermöglicht dem Cloud-Nutzer, die Datenverarbeitung nach verschiedenen Verarbeitungszwecken zu trennen (sichere Mandantentrennung).

(2) Der Cloud-Anbieter verhindert Verletzungen der Datentrennung, die durch technische oder organisatorische Fehler, einschließlich Bedienfehlern, des Cloud-Anbieters oder seiner Mitarbeiter oder fahrlässiger Handlungen des Cloud-Nutzers oder verursacht werden.

Schutzklasse 2

(3) Die Kriterien von Schutzklasse 1 sind erfüllt.

(4) Der Cloud-Anbieter muss Schutz vor bekannten Angriffsszenarien gegen das Trennungsgebot anbieten. Der Cloud-Anbieter kann vorsätzliche Verstöße gegen das Trennungsgebot im Regelfall (nachträglich) feststellen.

Schutzklasse 3

(5) Die Kriterien von Schutzklasse 1 und Schutzklasse 2 sind erfüllt.

(6) Der Cloud-Anbieter schließt eine Verletzung der Datentrennung aus. Der Cloud-Anbieter erkennt vorsätzliche Verstöße gegen die getrennte Verarbeitung.

Ermittlungsmethoden

- Dokumentprüfung
- Prüfung
- Audit

Ermittlung

Der Evaluator führt eine Durchsicht der Dokumentation zur Trennung von Daten durch, darunter z.B. die Dokumentation der TOM, Verfahrensanweisungen, Richtlinien, Ergebnisprotokolle interner/externer Audits, Risikoanalysen, und Dienstbeschreibungen.

Ein Abgleich der Dokumentation mit der tatsächlichen Umsetzung der Maßnahmen (bspw. getrennte Datenbanken) sollte durchgeführt werden. Dazu eignet sich eine Überprüfung der Trennung durch eine Prüfung in Form einer Assetprüfung (bspw. der eingesetzten Programme oder des Programmcodes, Prüfung auf getrennte Datenbanken) und Sicherheitstests (z.B. Penetrationstests zur Feststellung des Sicherheitsniveaus der Mandantentrennung). Unterstützend kann eine Befragung relevanter Mitarbeiter im Rahmen eines Audits (z.B. zur Kenntnis über Richtlinien etc.) durchgeführt werden.

Für Schutzklasse 2 und 3 prüft ein Evaluator durch eine Dokumentprüfung die Dokumentation zur Erkennung von bekannten Angriffsszenarien gegen das Trennungsgebot. Die tatsächliche Feststellung im Regelfall kann durch die Prüfung von Ereignisprotokollen, Protokollen zur Abwehr und Erkennung von Angriffen, oder elektronischer Prüfpfade überprüft werden.

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

Kriterium

(1) Der Cloud-Anbieter stellt durch risikoangemessene TOM sicher, dass nach einem physischen oder technischen Zwischenfall der Cloud-Dienst und die Daten rasch wiederhergestellt werden und verfügbar sind. Hierbei wird zwischen den Wiederherstellbarkeitsklassen 1, 2 und 3 unterschieden:

Wiederherstellbarkeitsklasse 1

Der Cloud-Anbieter sichert seinen Dienst gegen zu erwartende, naheliegende Ereignisse so zuverlässig ab und trifft Maßnahmen zu dessen Wiederherstellung, dass diese Risiken bei normalem Verlauf nicht zu einem Ausfall des Cloud-Dienstes oder einem endgültigen Datenverlust führen. Ereignisse sind zu erwar-

tend und naheliegend, wenn sie nicht vorkommen sollen, nach der Lebenserfahrung aber trotz hinreichender Vorsicht nicht ausgeschlossen werden können, wie etwa Unfälle im Straßenverkehr oder der technische Defekt von Hardware.

Wiederherstellbarkeitsklasse 2

Der Cloud-Anbieter sichert seinen Dienst gegen seltene Ereignisse so zuverlässig ab und trifft Maßnahmen zu dessen Wiederherstellung, dass diese Risiken bei normalem Verlauf der Datenverarbeitung nicht zu einem Ausfall des Cloud-Dienstes oder einem endgültigen Datenverlust führen. Ereignisse sind selten, wenn sie nicht vorkommen sollen und nach der Lebenserfahrung bei hinreichender Vorsicht wenig wahrscheinlich, aber gleichwohl in einigen Fällen zu beobachten sind, wie etwa „Jahrhunderthochwasser“ oder gezielte, umfangreiche Angriffe auf den Cloud-Dienst oder ein plötzlich erhöhtes Zugriffsvolumen.

Wiederherstellbarkeitsklasse 3

Der Cloud-Anbieter gewährleistet für seinen Dienst einen hohen Schutz (auch hinsichtlich der Wiederherstellung), der außergewöhnliche, aber nicht als theoretisch auszuschließende Ereignisse so zuverlässig absichert, dass diese Risiken bei normalem Verlauf der Datenverarbeitung nicht zu einem Ausfall des Cloud-Dienstes oder einem endgültigen Datenverlust führen. Ereignisse sind außergewöhnlich, aber nicht als theoretisch auszuschließen, wenn sie 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.

Ermittlungsmethoden

- Dokumentprüfung
- Inspektion
- Prüfung
- Audit

Ermittlung

Ein Evaluator prüft das Datensicherheitskonzept, um festzustellen, mit welchen Ereignissen der Cloud-Anbieter 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 er zur Wiederherstellbarkeit der Daten und des Cloud-Dienstes nach einem Zwischenfall ergriffen hat. Der Evaluator prüft alle vorgelegten Dokumente zur Wiederherstellbarkeit von Daten, insb. die Dokumentation der TOM, Verfahrensanweisungen, Richtlinien, Protokolle zu Testläufen der Datenwiederherstellung, Ergebnis interner/externer Audits, Risikoanalysen, und Dienstbeschreibungen.

Die Implementierung der geeigneten TOM wird durch repräsentative Stichproben im Rahmen eines Audits festgestellt und auf Angemessenheit überprüft. Eine Befragung relevanter Mitarbeiter (z.B. zur Kenntnis über Richtlinien und Verfahrensanweisungen zur Wiederherstellung etc.) kann durchgeführt werden. Die Inspektion und/oder Prüfung bzw. Besichtigung von Serverräumen und Beurteilung getroffener Maßnahmen und eingesetzter Techniken (bspw. redundante Server) zur Wiederherstellbarkeit sollte durchgeführt werden. Ein Ausfall bzw. eine Wiederherstellung kann testweise simuliert und Mitarbeiter dabei beobachtet werden, um die Übereinstimmung mit der Prozessdokumentation zu überprüfen. Hierbei vergleicht ein Evaluator auch die Dauer der Wiederherstellung mit der angegebenen Dauer in einer Strichprobe rechtsverbindlicher Vereinbarungen mit dem Cloud-Nutzer.

Der Evaluator prüft in Form einer Inspektion und/oder Prüfung, ob der Cloud-Anbieter einem Cloud-Nutzer sein Wiederherstellungskonzept zur Verfügung stellen kann. Im Rahmen eines Audits können Mitarbeiter zu diesem Informationsbereitstellungsprozess befragt werden, um sicherzustellen, dass dieser im Unternehmen gelebt wird und alle Richtlinien und Verfahrensanweisungen bekannt sind.

Nr. 3 – Sicherstellung der Weisungsbefolgung (Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. a und h; 29; 32 Abs. 4 DSGVO)

Kriterium

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

(2) Der Cloud-Anbieter gewährleistet durch TOM, dass die Verarbeitung der Daten des Cloud-Nutzers nur nach Maßgabe der Weisungen des Cloud-Nutzers erfolgt, es sei denn der Auftragsverarbeiter wird durch Unionsrecht oder mitgliedstaatliches Recht zur Datenverarbeitung verpflichtet.

(3) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf Grundlage dokumentierter Weisung des Verantwortlichen, auch in Bezug auf die Datenübermittlung an ein Drittland oder eine

internationale Organisation, sofern er nicht durch ein ihn betreffendes Unionsrecht oder mitgliedstaatliches Recht zur Datenverarbeitung verpflichtet ist; in diesem Fall soll der Auftragsverarbeiter den Verantwortlichen hinsichtlich dieser rechtlichen Verpflichtung vor der Datenverarbeitung informieren, sofern das jeweilige Recht die Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

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

Ermittlungsmethoden

- Dokumentprüfung, insbesondere Rechtsanalyse
- Inspektion
- Prüfung
- Audit

Ermittlung

Der Evaluator führt eine Durchsicht der Dokumentation zur Weisungsgebundenheit durch und prüft diese auf Rechtmäßigkeit und Korrektheit, darunter bspw. Dokumentation der TOM, Verfahrensanweisungen (insb. für Administratoren), Richtlinien, Protokollierung der Weisungen, und dokumentierte Maßnahmen zum Schutz und zur Manipulationsverhinderung.

Bei Einzelvereinbarungen mit Cloud-Nutzern führt der Evaluator eine stichprobenartige Überprüfung der rechtsverbindlichen Vereinbarungen durch, um die Umsetzung und Befolgung der dokumentierten Weisungen mit dem tatsächlichen Verhalten der Mitarbeiter und des Cloud-Dienstes zu vergleichen. Hierzu kann eine Inspektion durchgeführt werden, in dem testweise eine Weisung als Funktion im Cloud-Dienst aufgerufen wird oder entsprechende Mitarbeiter im Rahmen eines Audits zur Durchführung der Weisung testweise angewiesen werden.

Bei Massengeschäften führt der Evaluator eine Prüfung durch, wobei die Angaben in der Dienstbeschreibung zu den technisch ausführbaren Dienstleistungen und Weisungen durch Softwarebefehlen mit der tatsächlich möglichen Interaktion mit einem Cloud-Dienst verglichen werden. Hierzu kann eine Dienstnutzung oder Vorgangsüberwachung vom Evaluator durchgeführt werden, bei denen Weisungen als Softwarebefehle testweise durchgeführt werden und die Verarbeitung/das Ergebnis beobachtet wird. Auch kann der Evaluator eine Assetprüfung zur Überprüfung der Umsetzung von möglichen Softwarebefehlen zur Erteilung von Weisungen (z.B. Quellcodenanalyse) durchführen.

Ein Evaluator prüft auch stichprobenartig Protokolle über die fortlaufende Dokumentierung von erteilten Weisungen und/oder Softwarebefehlen von Cloud-Nutzern (bspw. Logeinträge, Zeitstempel, Versionierung von Logdateien).

Im Rahmen eines Audits kann eine Befragung oder Beobachtung relevanter Mitarbeiter (z.B. zur Kenntnis über Weisungen von Cloud-Nutzern und Richtlinien zur Befolgung dieser etc.) durchgeführt werden.

Der Evaluator prüft erfolgte Mitteilungen an den Cloud-Nutzer über rechtliche Anforderungen zu nicht weisungsgedeckten Verarbeitungen zur Erfüllung rechtlicher Pflichten aus dem Unionsrecht oder dem mitgliedstaatlichen Recht, soweit er über solche verfügt. Evaluatoren können auch Dokumentationen prüfen, darunter bspw. Dokumentation der TOM oder Verfahrensanweisungen, z.B., wie mit Anfragen von Ermittlungsbehörden umzugehen ist, die eine Herausgabe von Daten zum Inhalt haben oder wie der Cloud-Nutzer über diese rechtlichen Anforderungen zu informieren ist.

Nr. 4 – Hinweispflicht des Cloud-Anbieters

Nr. 4.1 – Weisungen entgegen datenschutzrechtlicher Vorschriften (Art. 28 Abs. 3 UAbs. 2 lit. h i.V.m Art. 29 DSGVO)

Kriterium

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

Ermittlungsmethoden

- Dokumentprüfung
- Audit

Ermittlung

Ein Evaluator prüft Dokumente, welche festhalten wie ein Cloud-Anbieter Weisungen prüft, Zweifel an deren datenschutzrechtlicher Zulässigkeit erkennt und den Cloud-Nutzer vor Ausführung der Weisung darauf hinweist. Dazu können die Dokumentation der TOM, Verfahrensanweisungen, Richtlinien, Protokollierung der Weisungen, Dokumentation der relevanten Mechanismen und Meldewege, und dokumentierte Prozesses zur Weisungsüberprüfung zählen. Ein Evaluator kann auch stattgefundene und dokumentierte Kommunikationen an Cloud-Nutzer im Falle der Abweichungsvermutung stichprobenartig untersuchen.

Eine Befragung relevanter Mitarbeiter (z.B. zur Kenntnis über Richtlinien und Verfahrensschritte im Falle von Zweifeln etc.) im Rahmen eines Audits kann durchgeführt werden. Darüber hinaus kann eine Beobachtung durchgeführt werden, bei der testweise eine zweifelhafte Weisung gegeben wird, und der Evaluator den Prozess zur Aufnahme und Bearbeitung der Weisung beobachtet.

Nr. 4.2 – Änderungen des Datenverarbeitungsortes (indirekt Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. a und h DSGVO)

Kriterium

Der Cloud-Anbieter informiert den Cloud-Nutzer immer unverzüglich und in der Regel im Voraus in allen Fällen, in denen sich während des Geltungszeitraums der rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung der Ort der Datenverarbeitung gegenüber dem in der rechtsverbindlichen Vereinbarung zur Auftragsvereinbarung festgelegten (Nr. 1.5) ändern wird.

Ermittlungsmethoden

- Dokumentprüfung
- Inspektion
- Audit

Ermittlung

Ein Evaluator nimmt eine Durchsicht der Dokumentation zu Informationspflichten des Cloud-Anbieters vor (z.B. Dokumentation der TOM, Verfahrensanweisungen, Richtlinien, dokumentierter Prozesses zur Kommunikation an den Cloud-Nutzer, Dokumentation der relevanten Mechanismen und Meldewege). Ein Cloud-Anbieter kann zudem stattgefundene und dokumentierte Kommunikationen an Cloud-Nutzer im Falle der Änderung des Ortes vorlegen, welche stichprobenartig vom Evaluator überprüft werden.

Durch eine Inspektion in Form einer Vorgangsüberwachung oder durch eine Beobachtung im Rahmen eines Audits kann geprüft werden, ob dem Cloud-Nutzer alle notwendigen Informationen zur Ortsänderung auf geeignete Weise kommuniziert werden. Hierzu kann testweise eine geplante Ortsänderung simuliert werden. Eine Befragung relevanter Mitarbeiter (z.B. zur Kenntnis über Richtlinien etc.) kann durchgeführt werden.

Nr. 5 – Sicherstellung der Vertraulichkeit beim Personal (Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. b und h 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 rechtsverbindlichen 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.

Ermittlungsmethoden

- Dokumentprüfung
- Audit

Ermittlung

Ein Evaluator prüft die Prozessdokumentationen zur Verpflichtung auf Vertraulichkeit sowie zur Anpassungen von Verpflichtungserklärungen (bspw., wenn sich Zugriffs- und Verarbeitungsbefugnisse ändern). Ein Evaluator kann auch eine Durchsicht des Musterdokuments zur Verschwiegenheitserklärung der Mitarbeiter durchführen. Durch die Vorlage von Arbeitsverträgen mit entsprechenden Regelungen bzw. zusätzlicher Verträge und Unternehmensrichtlinien kann ein Evaluator stichprobenartig die Umsetzung der Maßnahmen prüfen.

Im Rahmen eines Audits ist die Einhaltung dieser Vorgaben in allen Prozesskonstellationen durch repräsentativ stichprobenartige Interviews zu überprüfen. So kann ein Evaluator Mitarbeiter, die zur Verarbeitung von personenbezogenen Daten befugt sind, befragen, ob diese zur Vertraulichkeit verpflichtet wurden und ihnen bekannt ist, welche Vertraulichkeitspflichten damit einhergehen. Auch kann eine Beobachtung bei einer testweisen Änderung von Verarbeitungsbefugnissen durchgeführt werden, um die Anpassungen von Verpflichtungserklärungen zu simulieren.

Nr. 6 – Unterstützung des Cloud-Nutzers bei der Wahrung der Betroffenenrechte[18]

Nr. 6.1 – Informationserteilung[19] (Art. 13 oder 14 i.V.m. Art. 12 Abs. 1 und Art. 5 Abs. 1 lit. a DSGVO)

Kriterium

(1) Der Cloud-Anbieter stellt durch TOM sicher, dass der Cloud-Nutzer die Möglichkeit hat, die betroffene Person zeitgerecht, verständlich und in klarer und einfacher Sprache über die Datenverarbeitung zu informieren oder dies durch den Cloud-Anbieter vornehmen zu lassen.

(2) Der Cloud-Anbieter dokumentiert die vom Cloud-Nutzer erhaltenen Weisungen zur Umsetzung der Informationspflicht des Cloud-Nutzers oder wenn er ihn dabei unterstützt.

Ermittlungsmethoden

- Dokumentprüfung
- Inspektion
- Audit

Ermittlung

Der Evaluator prüft Dokumente zu Maßnahmen, die ein Cloud-Anbieter ergriffen hat, um dem Cloud-Nutzer die Informationserteilung gegenüber einer betroffenen Person zu ermöglichen oder die Information durch den Cloud-Anbieter mitteilen zu lassen (z.B. Mechanismen und Meldewege, Dienstbeschreibungen). Auch können anhand von Prozessdokumentationen und Protokollen die tatsächlich durchgeführten Informationserteilung überprüft werden.

Im Rahmen einer Inspektion kann der Evaluator eine Probeinformationserteilung durchführen, um zu prüfen, dass diese möglich ist (bspw. durch eine technische Funktion innerhalb des Cloud-Dienstes oder durch manuelle Anfragen beim Cloud-Dienst-Support).

Der Evaluator sollte Protokolle über die fortlaufende Dokumentierung von erteilten Weisungen und/oder Softwarebefehlen von Cloud-Nutzern zur Umsetzung der Informationserteilung (bspw. Logeinträge, Zeitstempel, Versionierung von Logdateien) prüfen. Im Rahmen eines Audits kann auch eine Befragung oder Beobachtung relevanter Mitarbeiter (z.B. zur Kenntnis über Weisungen von Cloud-Nutzern und Richtlinien zur Befolgung dieser etc.) durchgeführt werden.

Nr. 6.2 – Auskunftserteilung[20] (Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. e i.V.m. Art. 15 DSGVO)

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.

---

[18] Dieses Kriterium würde nicht für den Cloud-Nutzer gelten, der unter die Haushaltsausnahme fällt. Der Cloud-Anbieter als Auftragsverarbeiter ist gut beraten, das Kriterium als vorhanden und potenziell zu erfüllen zu betrachten, um auf solche Veränderungen in der Rolle eines Cloud-Nutzers, der zum für die Verarbeitung Verantwortlichen wird, reagieren zu können.

[19] Dieses Kriterium würde nicht für den Cloud-Nutzer gelten, der unter die Haushaltsausnahme fällt. Der Cloud-Anbieter als Auftragsverarbeiter ist gut beraten, das Kriterium als vorhanden und potenziell zu erfüllen zu betrachten, um auf solche Veränderungen in der Rolle eines Cloud-Nutzers, der zum für die Verarbeitung Verantwortlichen wird, reagieren zu können.

[20] Dieses Kriterium würde nicht für den Cloud-Nutzer gelten, der unter die Haushaltsausnahme fällt. Der Cloud-Anbieter als Auftragsverarbeiter ist gut beraten, das Kriterium als vorhanden und potenziell zu erfüllen zu betrachten, um auf solche Veränderungen in der Rolle eines Cloud-Nutzers, der zum für die Verarbeitung Verantwortlichen wird, reagieren zu können.

(2) Der Cloud-Anbieter dokumentiert die vom Cloud-Nutzer erhaltenen Weisungen zur Umsetzung der Auskunftserteilungspflicht des Cloud-Nutzers oder wenn er ihn dabei unterstützt.

Ermittlungsmethoden

- Dokumentprüfung
- Inspektion
- Audit

Ermittlung

Der Evaluator prüft Dokumentationen über Maßnahmen zur Auskunftserteilung gegenüber einer betroffenen Person oder zur Erteilung der Auskunft durch den Cloud-Anbieter. Insb. sollte der Evaluator Einsicht in die Dokumentation der relevanten Mechanismen und Meldewege, Dienstbeschreibungen erhalten. Ein Evaluator sollte exemplarische Datensätze und Protokolle zu getätigten Weisungen und darauffolgenden Auskünften sichten.

Im Rahmen einer Inspektion kann eine repräsentative Probeauskunft durchgeführt werden, um zu prüfen, ob eine Auskunftserteilung und Bereitstellung der Daten möglich ist (bspw. durch eine technische Funktion innerhalb des Cloud-Dienstes oder durch manuelle Anfragen beim Cloud-Dienst-Support). Im Rahmen eines Audits kann auch anhand von Befragungen (z.B. zur Kenntnis über Verfahrensschritte etc.) und Beobachtungen geprüft werden, ob bei einem Antrag Auskunft erteilt werden kann.

Nr. 6.3 – Berichtigung und Vervollständigung[21] (Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. e i.V.m. Art. 16 DSGVO)

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 dokumentiert die vom Cloud-Nutzer erhaltenen Weisungen zur Umsetzung der Berichtigungs- und Vervollständigungspflicht des Cloud-Nutzers oder wenn er ihn dabei unterstützt.

Ermittlungsmethoden

- Dokumentprüfung
- Inspektion
- Audit

Ermittlung

Der Evaluator prüft Dokumentationen über Maßnahmen zur Berichtigung und Vervollständigung von Daten (z.B. Dokumentation der relevanten Mechanismen und Meldewege, Dienstbeschreibungen). Ein Evaluator sollte exemplarische Datensätze und Protokolle zu getätigten Weisungen und darauffolgende Berichtigungen oder Vervollständigungen sichten.

Im Rahmen einer Inspektion kann eine repräsentative Probeberichtigung und -vervollständigung durchgeführt werden, um zu prüfen, ob eine Berichtigung und Vervollständigung von Daten möglich ist (bspw. durch eine technische Funktion innerhalb des Cloud-Dienstes oder durch manuelle Anfragen beim Cloud-Dienst-Support). Im Rahmen eines Audits kann auch anhand von Befragungen (z.B. zur Kenntnis über Verfahrensschritte etc.) und Beobachtungen geprüft werden, ob eine Berichtigung oder Vervollständigung durchgeführt werden kann.

Nr. 6.4 – Löschung (Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. e i.V.m. Art. 17 Abs. 1 DSGVO)

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, sodass die personenbezogenen Daten irreversibel gelöscht sind und aus ihnen keine Informationen über die betroffene Person gewonnen werden können. Der Cloud-Anbieter stellt sicher, dass die Löschung unwiderruflich erfolgt, indem er Maßnahmen nach dem Stand der Technik erfolgt.

[21] Dieses Kriterium würde nicht für den Cloud-Nutzer gelten, der unter die Haushaltsausnahme fällt. Der Cloud-Anbieter als Auftragsverarbeiter ist gut beraten, das Kriterium als vorhanden und potenziell zu erfüllen zu betrachten, um auf solche Veränderungen in der Rolle eines Cloud-Nutzers, der zum für die Verarbeitung Verantwortlichen wird, reagieren zu können.

(2) Der Cloud-Anbieter stellt sicher, dass die Löschung von personenbezogenen Daten nicht nur im aktiven Datenbestand vorgenommen wird, sondern auch in Kopien und Datensicherungen.

(3) Der Cloud-Anbieter hat sicherzustellen, dass nach einer Wiederherstellung von Daten, die bereits im aktiven Datenbestand, aber noch nicht in der Datensicherung gelöscht waren, eine erneute Löschung der betroffenen Daten erfolgt.

(4) Der Cloud-Anbieter dokumentiert die vom Cloud-Nutzer erhaltenen Weisungen zur Umsetzung der Verpflichtung in Bezug auf das Rechts auf Löschung oder wenn er ihn dabei unterstützt.

Ermittlungsmethoden

- Dokumentprüfung
- Inspektion
- Audit

Ermittlung

Der Evaluator prüft Dokumentationen über Maßnahmen zur Löschung von Daten (z.B. Dokumentation der relevanten Mechanismen und Meldewege, Löschkonzepte, Dienstbeschreibungen). Ein Evaluator sollte exemplarische Datensätze und Protokolle zu getätigten Weisungen und darauffolgenden Löschung sichten.

Im Rahmen einer Inspektion kann eine repräsentative Probelöschung durchgeführt werden, um zu prüfen, ob eine (vollständige und unwiderrufliche) Löschung von Daten möglich ist (bspw. durch eine technische Funktion innerhalb des Cloud-Dienstes oder durch manuelle Anfragen beim Cloud-Dienst-Support). Im Rahmen eines Audits kann auch anhand von Befragungen (z.B. zur Kenntnis über Verfahrensschritte etc.) und Beobachtungen geprüft werden, ob eine Löschung durchgeführt werden kann.

Nr. 6.5 – Einschränkung der Verarbeitung[22] (Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. e i.V.m. Art. 18 Abs. 1 DSGVO)

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 dokumentiert die vom Cloud-Nutzer erhaltenen Weisungen zur Umsetzung des Rechts auf Einschränkung der Verarbeitung oder wenn er ihn dabei unterstützt.

Ermittlungsmethoden

- Dokumentprüfung
- Inspektion
- Audit

Ermittlung

Der Evaluator prüft Dokumentationen über Maßnahmen zur Einschränkung der Verarbeitung von Daten (z.B. Dokumentation der relevanten Mechanismen und Meldewege, Dienstbeschreibungen). Ein Evaluator sollte exemplarische Datensätze und Protokolle zu getätigten Weisungen und darauffolgender Einschränkung sichten.

Im Rahmen einer Inspektion kann eine repräsentative Einschränkung durchgeführt werden, um zu prüfen, ob eine Einschränkung von der Datenverarbeitung möglich ist (bspw. durch eine technische Funktion innerhalb des Cloud-Dienstes oder durch manuelle Anfragen beim Cloud-Dienst-Support). Im Rahmen eines Audits kann auch anhand von Befragungen (z.B. zur Kenntnis über Verfahrensschritte etc.) und Beobachtungen geprüft werden, ob eine Einschränkung durchgeführt werden kann.

[22] Dieses Kriterium würde nicht für den Cloud-Nutzer gelten, der unter die Haushaltsausnahme fällt. Der Cloud-Anbieter als Auftragsverarbeiter ist gut beraten, das Kriterium als vorhanden und potenziell zu erfüllen zu betrachten, um auf solche Veränderungen in der Rolle eines Cloud-Nutzers, der zum für die Verarbeitung Verantwortlichen wird, reagieren zu können.

Nr. 6.6 – Mitteilungspflicht bei Berichtung, Löschung oder Einschränkung der Verarbeitung[23] (Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. e i.V.m. Art. 19 DSGVO)

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 dokumentiert die vom Cloud-Nutzer erhaltenen Weisungen zur Umsetzung der Mitteilungspflicht bei Berichtigung, Löschung oder Einschränkung der Verarbeitung oder wenn er ihn dabei unterstützt.

Ermittlungsmethoden

- Dokumentprüfung
- Inspektion
- Audit

Ermittlung

Der Evaluator prüft Dokumentationen über Maßnahmen zur Mitteilung (z.B. Dokumentation der relevanten Mechanismen und Meldewege, Dienstbeschreibungen). Ein Evaluator sollte exemplarische Datensätze und Protokolle zu getätigten Weisungen und darauffolgender Mitteilung sichten.

Im Rahmen einer Inspektion kann eine repräsentative Weisung zur Mitteilung durchgeführt werden, um zu prüfen, ob eine Mitteilung möglich ist (bspw. durch eine technische Funktion innerhalb des Cloud-Dienstes oder durch manuelle Anfragen beim Cloud-Dienst-Support). Im Rahmen eines Audits kann auch anhand von Befragungen (z.B. zur Kenntnis über Verfahrensschritte etc.) und Beobachtungen geprüft werden, ob eine Weisung zur Mitteilung durchgeführt werden kann.

Nr. 6.7 – Datenübertragung[24] (Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. e i.V.m. Art. 20 Abs. 1 und 2 DSGVO)

Kriterium

(1) Der Cloud-Anbieter stellt sicher, dass der Cloud-Nutzer (in Abhängigkeit von dessen Weisung) die Möglichkeit hat, entweder 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 dokumentiert die vom Cloud-Nutzer erhaltenen Weisungen zur Umsetzung des Rechts auf Datenübertragbarkeit oder wenn er ihn dabei unterstützt.

Ermittlungsmethoden

- Dokumentprüfung
- Inspektion
- Audit

Ermittlung

Der Evaluator prüft Dokumentationen über Maßnahmen zur Datenübertragung (z.B. Dokumentation der relevanten Mechanismen, Exportformate, Dienstbeschreibungen). Ein Evaluator sollte exemplarische Datensätze und Protokolle zu getätigten Weisungen und darauffolgender Datenübertragung sichten.

Im Rahmen einer Inspektion kann eine repräsentative Datenübertragung mit Testdaten durchgeführt werden, um zu prüfen, ob eine Übermittlung der Daten möglich ist (bspw. durch eine technische Funktion innerhalb des Cloud-Dienstes oder durch manuelle Anfragen beim Cloud-Dienst-Support). Im Rahmen eines Audits kann auch anhand

[23] Dieses Kriterium würde nicht für den Cloud-Nutzer gelten, der unter die Haushaltsausnahme fällt. Der Cloud-Anbieter als Auftragsverarbeiter ist gut beraten, das Kriterium als vorhanden und potenziell zu erfüllen zu betrachten, um auf solche Veränderungen in der Rolle eines Cloud-Nutzers, der zum für die Verarbeitung Verantwortlichen wird, reagieren zu können.

[24] Dieses Kriterium würde nicht für den Cloud-Nutzer gelten, der unter die Haushaltsausnahme fällt. Der Cloud-Anbieter als Auftragsverarbeiter ist gut beraten, das Kriterium als vorhanden und potenziell zu erfüllen zu betrachten, um auf solche Veränderungen in der Rolle eines Cloud-Nutzers, der zum für die Verarbeitung Verantwortlichen wird, reagieren zu können.

von Befragungen (z.B. zur Kenntnis über Verfahrensschritte etc.) und Beobachtungen geprüft werden, ob eine Datenübertragung durchgeführt werden kann.

Nr. 6.8 – Widerspruch[25]
(Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. e i.V.m. Art. 21 Abs. 1 und Art. 32 Abs. 1 lit. b DSGVO)

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 dokumentiert die vom Cloud-Nutzer erhaltenen Weisungen zur Umsetzung des Widerspruchrechts oder wenn er ihn dabei unterstützt.

Ermittlungsmethoden

- Dokumentprüfung
- Inspektion
- Audit

Ermittlung

Der Evaluator prüft Dokumentationen über Maßnahmen zur Entgegennahme von Widersprüchen sowie Beendigung der Verarbeitung (z.B. Dokumentation der relevanten Mechanismen und Meldewege, Dienstbeschreibungen). Ein Evaluator sollte exemplarische Datensätze und Protokolle zu getätigten Weisungen und ggf. darauffolgender Beendigung der Verarbeitung sichten. Es sollte im Zuge dessen auch geprüft werden, dass keine weiteren Protokolle über Verarbeitungen nach der Beendigung vorliegen (z.B. weitere Zugriffe auf Daten innerhalb eines Zugriffsprotokolls), um sicherzugehen, dass die Verarbeitung beendet wurde.

Im Rahmen einer Inspektion kann ein repräsentativer Widerspruch durchgeführt werden, um zu prüfen, ob der Cloud-Anbieter dem Cloud-Nutzer alle Daten zur Entscheidungsfindung bereitstellen kann und ggf. eine Beendigung der Verarbeitung möglich ist (bspw. durch eine technische Funktion innerhalb des Cloud-Dienstes oder durch manuelle Anfragen beim Cloud-Dienst-Support). Im Rahmen eines Audits kann auch anhand von Befragungen (z.B. zur Kenntnis über Verfahrensschritte etc.) und Beobachtungen geprüft werden, ob und wie eine Widerspruchsweisung durchgeführt werden kann. Gleichermaßen prüft ein Evaluator, ob ein Cloud-Anbieter 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.

Nr. 6.9 – Generelle Informationspflicht und Informationspflicht bei Untätigkeit oder verzögerter Antragsbearbeitung[26]
(Art. 12 Abs. 3 und 4, Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. e i.V.m. Art. 15 bis 21 DSGVO)

Kriterium

(1) Der Cloud-Anbieter stellt durch TOM sicher, dass der Cloud-Nutzer die Möglichkeit hat, die betroffene Person über die auf Antrag gemäß den Art. 15 bis 21 DSGVO ergriffenen Maßnahmen unverzüglich, spätestens innerhalb eines Monats nach Antragseingang, zu informieren. Die Information kann alternativ durch den Cloud-Anbieter vorgenommen werden.

(2) Der Cloud-Anbieter stellt durch TOM sicher, dass der Cloud-Nutzer die Möglichkeit hat, die betroffene Person zu informieren, falls er ihren Antrag nach Art. 15 bis 21 DSGVO nicht rechtzeitig, spätestens innerhalb eines Monats beantwortet. Die Information bezieht sich auf die Fristverlängerung und die Gründe hierfür. Die Information kann alternativ durch den Cloud-Anbieter vorgenommen werden.

(3) Der Cloud-Anbieter stellt durch TOM sicher, dass der Cloud-Nutzer die Möglichkeit hat, die betroffene Person, spätestens innerhalb eines Monats darüber zu informieren, falls er keine Maßnahmen ergreift, um einen Antrag nach Art. 15 bis 21 DSGVO zu beantworten. Die Information der betroffenen Person bezieht

[25] Dieses Kriterium würde nicht für den Cloud-Nutzer gelten, der unter die Haushaltsausnahme fällt. Der Cloud-Anbieter als Auftragsverarbeiter ist gut beraten, das Kriterium als vorhanden und potenziell zu erfüllen zu betrachten, um auf solche Veränderungen in der Rolle eines Cloud-Nutzers, der zum für die Verarbeitung Verantwortlichen wird, reagieren zu können.

[26] Dieses Kriterium würde nicht für den Cloud-Nutzer gelten, der unter die Haushaltsausnahme fällt. Der Cloud-Anbieter als Auftragsverarbeiter ist gut beraten, das Kriterium als vorhanden und potenziell zu erfüllen zu betrachten, um auf solche Veränderungen in der Rolle eines Cloud-Nutzers, der zum für die Verarbeitung Verantwortlichen wird, reagieren zu können.

sich auf die Gründe der Untätigkeit des Cloud-Nutzers und die Möglichkeit bei der Aufsichtsbehörde Beschwerde oder einen gerichtlichen Rechtsbehelf einzulegen. Die Information kann alternativ durch den Cloud-Anbieter vorgenommen werden.

Ermittlungsmethoden

- Dokumentprüfung
- Inspektion
- Audit

Ermittlung

Der Evaluator prüft Dokumente zu Maßnahmen, die ein Cloud-Anbieter ergriffen hat, um dem Cloud-Nutzer die Informationserteilung gegenüber einer betroffenen Person zu ermöglichen oder die Information durch den Cloud-Anbieter mitteilen zu lassen (z.B. Mechanismen und Meldewege, Dienstbeschreibungen). Auch können anhand von Prozessdokumentationen und Protokollen die durchgeführten Informationserteilungen überprüft werden, auch auf Vollständigkeit der erteilten Informationen und ihre rechtzeitige Erteilung.

Im Rahmen einer Inspektion kann der Evaluator eine Probeinformationserteilung durchführen, um zu prüfen, dass diese möglich ist (bspw. durch eine technische Funktion innerhalb des Cloud-Dienstes oder durch manuelle Anfragen beim Cloud-Dienst-Support) und alle erforderlichen Informationen liefert.

Der Evaluator sollte Protokolle über die fortlaufende Dokumentierung von erteilten Weisungen und/oder Softwarebefehlen von Cloud-Nutzern zur Umsetzung der Informationserteilung (bspw. Logeinträge, Zeitstempel, Versionierung von Logdateien) prüfen. Im Rahmen eines Audits kann auch eine Befragung oder Beobachtung relevanter Mitarbeiter (z.B. zur Kenntnis über Weisungen von Cloud-Nutzern und Richtlinien zur Befolgung dieser) durchgeführt werden.

Nr. 7 – Unterstützung bei der Datenschutz-Folgenabschätzung[27] (Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. f i.V.m. Art. 35 und 36 DSGVO)

Kriterium

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

(2) Ist dem Cloud-Anbieter durch eine vorher beim Cloud-Nutzer durchgeführte Datenschutz-Folgenabschätzung 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.

Ermittlungsmethoden

- Dokumentprüfung
- Audit

Ermittlung

Ein Evaluator sollte insbesondere eine Durchsicht der Dokumentation zu Informationspflichten durchführen, darunter Hilfsdokumente für Cloud-Nutzer (bspw. Dienstbeschreibungen, TOM, Datenflussmodelle und -analysen), durchgeführte Datenschutz-Folgenabschätzungen und entsprechende Gesprächsprotokolle, Dokumentation der getroffenen Vorkehrungen, Verfahrensverzeichnisse, Verfahrensanweisungen, und Richtlinien. Insbesondere muss der Evaluator bei der Dokumentenprüfung sicherstellen, dass notwendige Informationen vorliegen oder vom Cloud-Anbieter in kurzer Zeit generiert werden können.

[27] Dieses Kriterium würde nicht für den Cloud-Nutzer gelten, der unter die Haushaltsausnahme fällt. Der Cloud-Anbieter als Auftragsverarbeiter ist gut beraten, das Kriterium als vorhanden und potenziell zu erfüllen zu betrachten, um auf solche Veränderungen in der Rolle eines Cloud-Nutzers, der zum für die Verarbeitung Verantwortlichen wird, reagieren zu können.

Ein Abgleich der Dokumentation und rechtsverbindlichen Vereinbarung mit der tatsächlichen Umsetzung der Maßnahmen muss durchgeführt werden. Eine Befragung relevanter Mitarbeiter im Rahmen eines Audits (z.B. zur Kenntnis über Richtlinien etc.) ist erforderlich. Durch eine Beobachtung kann überprüft werden, ob und wie Mitarbeiter eine testweise Anfrage eines Cloud-Nutzers zur Datenschutz-Folgenabschätzung bearbeiten.

Kapitel III: Datenschutz-Managementsystem des Cloud-Anbieters

Nr. 8 – Datenschutz-Managementsystem

Nr. 8.1 – Benennung, Stellung und Aufgaben eines Datenschutzbeauftragten (Art. 37 bis 39 DSGVO, § 38 Abs. 1; Abs. 2 i.V.m. § 6 Abs. 5 Satz 2 BDSG)

Kriterium

(1) Der Cloud-Anbieter muss einen Datenschutzbeauftragten (DSB) benennen, wo die Kerntätigkeit in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche, regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen.

(2) Der Cloud-Anbieter muss einen DSB benennen, wo die Kerntätigkeit in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 besteht.

(3) Der Cloud-Anbieter muss einen DSB benennen, soweit er in der Regel mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt.

(4) Der Cloud-Anbieter muss einen DSB benennen, wenn er Datenverarbeitungen vornimmt, die einer Datenschutz-Folgenabschätzung nach Artikel 35 DSGVO unterliegen, unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen.

(5) Der Cloud-Anbieter muss einen DSB benennen, wenn er personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung verarbeitet, unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen.

(6) Ist der Cloud-Anbieter zur Benennung eines DSB verpflichtet, benennt er diesen 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.

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

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

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

(10) 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.

(11) Der Cloud-Anbieter stellt sicher, dass der DSB seinen Aufgaben nach Art. 39 Abs. 1 DSGVO im angemessenen Umfang nachkommen kann, einschließlich der Unterrichtung und Beratung, der Überwachung der Einhaltung der Vorschriften sowie der Zusammenarbeit mit der Aufsichtsbehörde und der Funktion als Kontaktstelle für diese.

(12) Der Cloud-Anbieter stellt sicher, dass der DSB bei der Erfüllung seiner Aufgaben über das Ende seines Rechtsverhältnisses mit dem Cloud-Anbieter hinaus an die Wahrung der Geheimhaltung oder Vertraulichkeit gebunden ist. Dies umfasst insbesondere die Pflicht des DSB zur Verschwiegenheit über die Identität der betroffenen Person sowie über die Umstände, die Rückschlüsse auf die betroffene Person zulassen, soweit er nicht davon durch die betroffene Person befreit wird.

(13) Der Cloud-Anbieter veröffentlicht die Kontaktdaten des DSB und teilt diese Daten der Aufsichtsbehörde mit.

(14) Der Cloud-Anbieter stellt sicher, dass andere Aufgaben oder Pflichten des DSB zu keinem Interessenkonflikt mit seiner Tätigkeit als DSB führen.

Ermittlungsmethoden

- Dokumentprüfung, insbesondere Rechtsanalyse
- Audit

Ermittlung

Ein Evaluator prüft die Dokumentation über die Gründe für die Benennung eines DSB.

Ein Evaluator prüft interne und auch externe Dokumente, um die Ernennung des DSB und die Veröffentlichung seiner Kontaktdaten festzustellen. Externe Dokumente können beispielsweise das Impressum oder auch die Datenschutzerklärung auf der Webseite des Cloud-Anbieters sein. Da diese Angaben ggf. jedoch optional sind, sollten auch interne Dokumente wie z.B. die Vorlage der Bestätigung einer erfolgreichen Meldung des DSB bei der Aufsichtsbehörde, die Stellenbeschreibung des DSB; Benennungsurkunden; Fachkundenachweise (bspw. Zeugnisse, Schulungsnachweise); Aufgaben- und Verfahrensbeschreibungen; Richtlinien; Organigramm, welches die Einordnung des DSB beschreibt; Bereitstellung von Protokollen über die Mitarbeitersensibilisierung zur Rolle des DSB; Gesprächsprotokolle mit DSB zur Überprüfung der Anforderungserfüllung; und Tätigkeitsberichte ein geeignetes Mittel zur Überprüfung der tatsächlichen Ernennung sein.

Zudem soll eine Befragung des DSB und weiterer Mitarbeiter des Unternehmens im Rahmen eines Audits dazu genutzt werden, die Ernennung des DSB und die Bekanntheit des DSB im Unternehmen zu überprüfen.

Zur Überprüfung der fachlichen Qualifikation des DSB legt der Cloud-Anbieter dem Evaluator relevante Dokumente, die zum Nachweis des Fachwissenns führen, zur Dokumentprüfung vor. Hierzu zählt ein aktueller unterzeichneter Lebenslauf des DSB, der alle relevanten Punkte, die relevantes Fachwissen hinsichtlich des Themas Datenschutz nachweisen, aufführen. Des Weiteren können durch Zeugnisse (Studium oder vergleichbar) oder Zertifikate bzw. Teilnahmebestätigungen von datenschutzrelevanten Lehrgängen / Schulungen die Qualifikation des DSB nachgewiesen werden. Eine Befragung mit dem DSB kann während einer Vor-Ort-Auditierung ebenfalls Aufschluss über Eignung und Stellung des DSB geben.

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. Hierzu sollten entsprechende Auditprotokolle zur Prüfung vorgelegt werden. Mittels einer Befragung wird der DSB hinsichtlich der Anerkennung und Funktionen seiner Position als DSB befragt. Zusätzlich können beispielsweise Dokumente, die zur Protokollierung der geleisteten Arbeitsstunden im Tätigkeitsfeld des DSB nachweisen, hinzugezogen werden. Des Weiteren können Dokumente, die durch den Arbeitgeber geförderte Schulungen hinsichtlich datenschutzrechtlicher Themen die Unterstützung des Cloud-Anbieters untermauern. Im Rahmen einer Vor-Ort-Auditierung kann festgestellt werden, ob der DSB über die erforderliche Ausstattung und Unterstützung verfügt.

Die Adressaten von Berichten des DSB (bspw. Meldungen von Datenschutzverstößen) sollen per Dokumentprüfung ermittelt werden. Hierzu können die internen Dokumente oder auch E-Mails, die vom DSB verfasst wurden, als Grundlage verwendet werden. Adressaten müssen die höchsten Managementebene gem. Organigramm oder vergleichbaren Anhaltspunkten sein. Mittels Befragung des Managements kann überprüft werden, ob der DSB ihnen direkt berichtet.

Zur Beurteilung der Vertraulichkeitspflicht kann ein Evaluator im Rahmen einer Dokumentenprüfung die entsprechende, unterzeichnete Benennungsurkunde des DSB mit den geforderten Inhalten überprüfen und den DSB zu seiner Vertraulichkeitspflicht befragen.

Der Evalautor befragt den DSB hinsichtlich der Einbindung in Themen, die Auswirkungen auf den Schutz personenbezogener Daten haben. Zusätzlich können beispielsweise Sitzungsprotokolle von relevanten Sitzungen eine Anwesenheit und Einbindung des DSB nachweisen.

Mittels einer Befragung wird der DSB hinsichtlich seiner Aufgaben befragt, um auszuschließen, dass es zu einem Interessenkonflikt kommt. Zusätzlich können beispielsweise Dokumente, die zur Protokollierung der geleisteten Arbeitsstunden im Tätigkeitsfeld des DSB nachweisen, hinzugezogen werden. Zur Prüfung möglicher Interessenkonflikte kann die Ressourcenverfügbarkeit, die Befragung relevanter Mitarbeiter, und Einsicht der Dokumentation der relevanten Mechanismen und Meldewege durchgeführt werden. Mittels einer Befragung wird der DSB hinsichtlich der Weisungsbefugnisse von Vorgesetzten oder anderen Mitarbeitern im Rahmen seiner Tätigkeiten als DSB befragt. 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. Hierzu sollten entsprechende Auditprotokolle zur Prüfung vorgelegt werden.

Nr. 8.2 – Meldung von Datenschutzverletzungen[28] (Art. 33 Abs. 2 und Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. f DSGVO)

Kriterium

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

(2) Der Cloud-Anbieter bestimmt, wer zuständig ist, über die Mitteilung an den Cloud-Nutzer zu entscheiden und diese vorzunehmen. Die zuständigen Stellen sind für Mitarbeiter und Subauftragsverarbeiter in einer Weise erreichbar, dass Mitteilungen über etwaige Verstöße zeitnah entgegengenommen und bearbeitet werden können.

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

Ermittlungsmethoden

- Dokumentprüfung
- Inspektion
- Audit

Ermittlung

Ein Evaluator prüft das Datensicherheitskonzept und darin beschriebene TOMs zur Gewährleistung der Meldung von Datenschutzverletzungen. Er kann zudem weitere Dokumentation zu Informationspflichten und Meldepflichten des Cloud-Anbieters prüfen, darunter bspw. Prozessdokumentation für Information an Nutzer, Verfahrensverzeichnisse, Verfahrensanweisungen, Richtlinien und Schulungsunterlagen.

Die Implementierung dieses Konzepts kann durch eine Inspektion oder Beobachtung einer Probemeldung an einen Evaluator als simulierter Cloud-Nutzer geprüft werden. Gleichermaßen sollte überprüft werden, ob eine Meldung von Datenschutzverletzungen testweise durch einen Evaluator möglich ist und Verstöße zeitnah entgegengenommen und bearbeitet werden. Auch können anhand von Protokollen über in der Vergangenheit stattgefundene Kommunikationen an den Nutzer geprüft werden. Im Rahmen einer Vor-Ort-Auditierung sollte geprüft werden, ob ausreichend Ressourcen vorliegen, um eine rasche Bearbeitung von Meldungen sicher zu stellen.

Im Rahmen einer Dokumentenprüfung sollte der Evaluator zudem prüfen, dass sich der Cloud-Anbieter vertraglich verpflichtet hat, Datenschutzverletzungen an den Cloud-Nutzer zu melden. Hierfür sollten die Regelungen in den Vertragsmustern oder geschlossenen Verträgen stichprobenartig geprüft werden (s. hierzu auch Nr. 1.7).

Die Kompetenz der Mitarbeiter sollte durch eine Prüfung der Dokumentation von Fähigkeiten (bspw. Zeugnissen) oder erfolgter Schulungen und durch Mitarbeiterbefragungen nachgewiesen werden. Auch kann der Evaluator das Organigramm bzw. einer Übersicht zur Personalsituation in verantwortlichen Bereichen mit entsprechender dokumentierter Qualifikation des Personals prüfen. Dabei muss der Evaluator auch durch Befragungen prüfen, ob Verantwortlichkeiten klar kommuniziert und geregelt sind (bspw. wer ist verantwortlich über die Mitteilung an den Cloud-Nutzer zu entscheiden und diese vorzunehmen?).

Nr. 8.3 – Führen eines Verarbeitungsverzeichnisses (Art. 30 Abs. 2 bis 5 DSGVO)

Kriterium

(1) Der Cloud-Anbieter führt ein Verarbeitungsverzeichnis, wenn er 250 oder mehr Personen beschäftigt.

(2) Der Cloud-Anbieter führt ein Verarbeitungsverzeichnis, wenn die Verarbeitung, die er vornimmt, wahrscheinlich zu einem Risiko für die Rechte und Freiheiten der betroffenen Personen führt.

(3) Der Cloud-Anbieter führt ein Verarbeitungsverzeichnis, wenn die Verarbeitung nicht nur gelegentlich erfolgt.

(4) Der Cloud-Anbieter führt ein Verarbeitungsverzeichnis, wenn die Verarbeitung besondere Kategorien von Daten im Sinne von Artikel 9 Absatz 1 DSGVO oder personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten im Sinne von Artikel 10 DSGVO umfasst.

[28] Dieses Kriterium würde nicht für den Cloud-Nutzer gelten, der unter die Haushaltsausnahme fällt. Der Cloud-Anbieter als Auftragsverarbeiter ist gut beraten, das Kriterium als vorhanden und potenziell zu erfüllen zu betrachten, um auf solche Veränderungen in der Rolle eines Cloud-Nutzers, der zum für die Verarbeitung Verantwortlichen wird, reagieren zu können.

(5) Ist der Cloud-Anbieter zur Führung eines Verarbeitungsverzeichnisses verpflichtet, führt er in diesem alle Kategorien von Verarbeitungen auf, die er im Auftrag von Cloud-Nutzern vornimmt. Das Verzeichnis enthält die in Art. 30 Abs. 2 lit. a bis d DSGVO aufgelisteten Inhalte.

(6) Der Cloud-Anbieter verfügt über Prozesse zur Aktualisierung des Verarbeitungsverzeichnisses, wenn neue Kategorien von Verarbeitungen, die er im Auftrag des Cloud-Nutzers vornimmt, eingeführt werden oder wegfallen, sich die Angaben nach Art. 30 Abs. 2 lit. a bis d DSGVO bei aufgeführten Kategorien von Verarbeitungen oder bei bestehenden Cloud-Nutzern, in deren Auftrag Verarbeitungen durchgeführt werden, ändern und Cloud-Nutzer, in deren Auftrag Verarbeitungen durchgeführt werden, hinzukommen oder wegfallen.

(7) Um das Verarbeitungsverzeichnis aktualisieren zu können, verfügt der Cloud-Anbieter über Prozesse zur Zusammenarbeit zwischen den an den Verarbeitungen beteiligten Fachabteilungen, den Cloud-Nutzern, in deren Auftrag Verarbeitungen durchgeführt werden sowie deren Vertretern und ggf. den DSB der Cloud-Nutzer und regelt hierfür die internen Zuständigkeiten.

(8) Das Verarbeitungsverzeichnis ist schriftlich oder in einem elektronischen Format zu führen und die Aufbewahrungs- oder Speicherorte sind bekannt.

(9) Das Verarbeitungsverzeichnis ist der Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen. Der Cloud-Anbieter verfügt über Prozesse zur Entgegennahme, Bearbeitung und Beantwortung von Anfragen von Aufsichtsbehörden und regelt hierfür die internen Zuständigkeiten.

(10) Ist der Cloud-Anbieter zur Benennung eines Vertreters und zur Führung eines Verarbeitungsverzeichnisses verpflichtet, stellt er sicher, dass auch der Vertreter ein Verarbeitungsverzeichnis führt und die Kriterien nach Abs. 1 bis 5 einhält.

Ermittlungsmethoden

- Dokumentprüfung
- Audit

Ermittlung

Ein Evaluator prüft die Dokumentation über die Gründe für die Führung eines Verarbeitungsverzeichnisses.

Ein Evaluator prüft die vorgelegten Verarbeitungsverzeichnisse auf Vollständigkeit, Form (schriftlich oder elektronisches Format) und Aktualität (bspw. Zeitstempel, Versionierungshistorie). Ist eine standardisierte Vereinbarung mit dem Cloud-Nutzer geschlossen, prüft der Evaluator das zugrundeliegende standardisierte Verarbeitungsverzeichnis. Sollten keine standardisierten Vereinbarungen mit einem Cloud-Nutzer geschlossen worden sein, prüft ein Evaluator im Rahmen der Dokumentprüfung alle oder eine repräsentative Stichprobe von Verarbeitungsverzeichnissen von Cloud-Nutzern. Eine repräsentative Stichprobe sollte mindestens so umfassend gewählt werden, dass durch eine vergleichende Begutachtung einer Auswahl an Verzeichnissen und Vereinbarungen mit hoher Wahrscheinlichkeit ausgeschlossen werden kann, dass ein weiteres Verzeichnis unzureichend ist. Der Stichprobenumfang ist somit auch abhängig von der Gesamtanzahl an Verzeichnissen. Die individuellen Verzeichnisse können zu Gruppen zusammengefasst werden, wobei aus jeder Gruppe von Verzeichnissen eine ausreichende Anzahl an Verzeichnissen geprüft werden muss. Verzeichnisse können unter anderem hinsichtlich des Gegenstands, der Dauer, der Art und den Zweck der Verarbeitung in Gruppen eingeteilt werden.

Ein Evaluator prüft die Prozessbeschreibungen des Cloud-Anbieters hinsichtlich des Vorgehens und der Vollständigkeit der Fälle, in denen Verarbeitungsverzeichnisse zu aktualisieren sind.

Ein Evaluator prüft im Rahmen einer Dokumentenprüfung die Zusammenarbeit der für das Verarbeitungsverzeichnis maßgeblichen Akteure. Hierfür kann der Evaluator Prozessbeschreibungen, Organigramme, Aufgabenverteilungspläne oder sonstige Dokumente prüfen.

Im Rahmen einer Dokumentenprüfung prüft ein Evaluator die Prozesse zur Entgegennahme, Bearbeitung und Beantwortung von Anfragen von Aufsichtsbehörden zu Verarbeitungsverzeichnissen. Hierfür kann der Evaluator Prozessbeschreibungen, Organigramme, Aufgabenverteilungspläne oder sonstige Dokumente prüfen.

Unterstützend kann ein Evaluator im Rahmen eines Audits Befragungen der Mitarbeiter durchführen, um die Verzeichnisse auf Vollständigkeit und Aktualität zu prüfen und zu beurteilen, ob die Zusammenarbeit der für das Verarbeitungsverzeichnis maßgeblichen Akteure entsprechend der Prozessbeschreibung erfolgt und die Speicherorte der Verarbeitungsverzeichnisse bekannt sind.

Sofern der Cloud-Anbieter angibt, aufgrund von Art. 30 Abs. 5 DSGVO nicht zur Führung von Verarbeitungsverzeichnissen verpflichtet zu sein, führt der Evaluator im Rahmen eines Audits eine Befragung oder Dokumentenprüfung zur Feststellung der Anzahl der Mitarbeiter des Cloud-Anbieters vor. Im Rahmen einer Dokumentenprüfung z.B. der Dokumentation der Risikoermittlung im Rahmen der Art. 24, 25 oder 32 DSGVO oder der geschlossenen Verträge nach Art. 28 DSGVO prüft der Evaluator, ob trotz einer Mitarbeiterzahl von unter 250 Mitarbeitern, die Verarbeitung des Cloud-Anbieters ein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt, die

Verarbeitung nicht nur gelegentlich erfolgt oder Verarbeitungen besonderer Kategorien von Daten nach Art. 9 oder 10 DSGVO vorgenommen werden, die zur Führung eines Verarbeitungsverzeichnisses verpflichten.

Nr. 8.4 – Rückgabe von Datenträgern und Löschung von Daten; Nachweis der Einhaltung und Ermöglichung von sowie Mitwirkung an Audits (Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. g und h DSGVO)

Kriterium

(1) Der Cloud-Anbieter stellt durch geeignete Maßnahmen sicher, dass die Rückgabe überlassener Datenträger (die personenbezogene Daten enthalten), die Rückführung von personenbezogenen Daten und die Löschung der beim Cloud-Anbieter gespeicherten personenbezogenen Daten nach Abschluss der Auftragsverarbeitung oder nach Weisung des Cloud-Nutzers erfolgen, sofern nicht nach nationalem oder Unionsrecht eine Verpflichtung zur Datenspeicherung besteht. Dieses Kriterium würde nicht für den Cloud-Nutzer gelten, der unter die Haushaltsausnahme fällt. Der Cloud-Anbieter als Auftragsverarbeiter ist gut beraten, das Kriterium als vorhanden und potenziell zu erfüllen zu betrachten, um auf solche Veränderungen in der Rolle eines Cloud-Nutzers, der zum für die Verarbeitung Verantwortlichen wird, reagieren zu können.

(2) Der Cloud-Anbieter stellt durch geeignete Maßnahmen sicher, dass er in der Lage ist, alle Informationen, die für den Nachweis der Einhaltung der in Art. 28 DSGVO enthaltenen Verpflichtungen erbringen zu können und dass er Audits, einschließlich Inspektionen, durch den Verantwortlichen oder einen anderen von diesem beauftragten Prüfer zulässt und dazu beiträgt.

Ermittlungsmethoden

- Dokumentprüfung
- Inspektion
- Prüfung
- Audit

Ermittlung

Ein Evaluator für eine Dokumentprüfung durch, darunter Prüfung von Verfahrensanweisungen und Richtlinien zur Herausgabe der Datenträger, zur Rückführung und Löschung von Daten nach Beendigung des Auftrags (z.B. Dokumentation der TOM, Datenlöschkonzepte, Verfahrensverzeichnisse, Prozessdokumentation für die Daten(träger)behandlung, Verfahrensanweisungen, Richtlinien, Dokumentierte Weisungen). Auch kann ein Evaluator die Quittierung von Rückgaben oder die automatisierte Benachrichtigung über tatsächliche Löschungen der für die Auftragsverarbeitung nicht mehr benötigten personenbezogenen Daten prüfen.

Durch eine Inspektion und/oder Prüfung (bspw. Quellcodeanalyse, Analyse von Datenbanken) oder testweisen Löschung und Rückführung kann festgestellt werden, ob eine Rückführung und Löschung der personenbezogenen Daten nach Abschluss der Auftragsverarbeitung oder nach Weisung des Cloud-Nutzers erfolgt. Eine Befragung relevanter Mitarbeiter im Rahmen eines Audits (z.B. zur Kenntnis über Richtlinien etc.) kann zu weiteren Informationen und Einblicke über die Durchführung der Maßnahmen führen.

Unterstützend können Sicherheitstests durchgeführt werden um zu prüfen, dass Daten hinreichend sicher gelöscht wurden.

Der Evaluator prüft geeignete Dokumentationen die belegen, dass der Cloud-Anbieter aktiv Maßnahmen ergreift, um die für Artikel 28 DSGVO erforderlichen Informationen zur Verfügung zu stellen und Audits durch den Verantwortlichen oder andere von ihm beauftragte Auditoren zulässt und dazu beiträgt. Durch eine Mitarbeiterüberprüfung kann die Umsetzung der Dokumentation überprüft werden.

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

Kriterium

(1) Der Cloud-Anbieter überprüft die Umsetzung aller in diesem Katalog geprüften Kriterien regelmäßig (mindestens jährlich und nach jeder wesentlichen Veränderung) in einem internen Revisionsverfahren. Hierfür legt der Cloud-Anbieter Kontrollverfahren und Zuständigkeiten fest und handelt bei Befunden aus Audits mit präventiven und korrektiven Maßnahmen

(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.

Ermittlungsmethoden

- Dokumentprüfung
- Audit

Ermittlung

Der Evaluator führt eine Durchsicht der Dokumentation zur Durchführung von Revisionen durch den Cloud-Anbieter durch (z.B. TOM, Verfahrensverzeichnisse, Verfahrensanweisungen, Richtlinien, Rollenbeschreibungen, Revisions- und Ergebnisprotokolle, Terminplanung für interne Revisionen). Zudem kann die Durchführung eines internen Revisionsverfahrens durch repräsentative Stichproben anhand geeigneter Prozessdokumentationen sichergestellt werden. Auch kann ein Evaluator den Zeitpunkt von (öffentlich bekannten) Änderungen des Cloud-Dienstes (bspw. Change- und Patchlogs) mit den Zeitstempeln von Protokollen interner Kontrollverfahren abgleichen.

Die Praxis der internen Kontrollen kann durch Befragungen mit dem DSB und Verantwortlichen im Rahmen eines Audits festgestellt werden. Dabei prüft ein Evaluator insbesondere auch, ob Mitarbeiter ihre zugeteilte Verantwortlichkeit gemäß Dokumentation bewusst ist und entsprechende Kontrollverfahren von ihnen durchgeführt werden.

Ferner wird geprüft, ob bei Befunden aus Audits auch präventive oder korrektive Maßnahmen umgesetzt worden sind. Hierzu können entsprechende Dokumentationen überprüft werden oder Mitarbeiter befragt werden. Ein Befund kann simuliert werden, um die Prozessabläufe anschließend zu beobachten.

Nr. 8.6 – Auswahl und Einsatz geeigneter Personen (Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. e und f DSGVO)

Kriterium

(1) Der Cloud-Anbieter betraut nur Mitarbeiter mit der Durchführung von Verarbeitungsvorgängen, die fachlich für die Erfüllung ihrer jeweiligen Aufgaben befähigt sind 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.

(3) Der Cloud-Anbieter stellt sicher, dass Mitarbeiter fortlaufend im Themenfeld Datenschutz und Datensicherheit geschult werden.

Ermittlungsmethoden

- Dokumentprüfung
- Audit

Ermittlung

Ein Evaluator prüft die erforderliche Fachkunde der Mitarbeiter durch einschlägige Qualifikationsnachweise (z.B. Mustervereinbarung, Dokumentation über Eignungsvoraussetzungen, Schulungsunterlagen, Teilnahmenachweise, Rollen- und Berechtigungskonzepte, Verfahrensanweisungen, Richtlinien, Rollenbeschreibungen). Sensibilisierungs- und Schulungsmaßnahmen von Mitarbeitern können durch die Dokumentation erfolgter Schulungen nachgewiesen werden.

Die Feststellung der Umsetzung von Regeln kann im Rahmen einer Vor-Ort-Prüfung (z.B. Clean Desk Grundsatz, Bildschirmsperren) und Befragungen der Mitarbeiter (bspw. Prüfung auf Fachkunde, Bekanntheit der Richtlinien, potenzielle Interessenkonflikte) durchgeführt werden.

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 führt eine Risikoanalyse für alle Verarbeitungstätigkeiten des angebotenen Dienstes durch und verfügt im Rahmen seines angebotenen Dienstes über TOM zur praktikablen und zielführenden Umsetzung der Grundsätze des Art. 5 DSGVO (Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz, Zweckfestlegung und Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Systemdatenschutz und Verantwortlichkeit).

(2) Der Cloud-Anbieter unterhält Prozesse um darstellen zu können, dass personenbezogene Daten auf transparente Weise in Bezug auf die betroffenen Personen verarbeitet werden (Prinzip der Transparenz). Er muss zudem Prozesse etablieren, welche die aktive Überwachung seiner Einhaltung des Stand der Technik auf allen Ebenen der konzeptionellen Zielsetzung seiner Dienste[29], ihrer Architektur und ihrer Systemgestaltung sicherstellen.

(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 (unter Beachtung der Datenminimierung, s. Nr. 2.6 [1]) und Transparenz der Datenverarbeitungen, auch in den verlängerten Leistungsketten durch etwaige Subauftragsverhältnisse, gewährleistet ist.

Ermittlungsmethoden

- Dokumentprüfung
- Inspektion
- Prüfung
- Audit
- Entwicklungs- und Designprüfung

Ermittlung

Zur Überprüfung des Datenschutzes durch Systemgestaltung kann ein Evaluator eine Vielzahl an Ermittlungsmethoden anwenden.

Im Rahmen einer Dokumentprüfung prüft ein Evaluator die Dokumentation der datenschutzrechtlichen Risikoanalyse des Cloud-Anbieters. Anhand der Verarbeitungsverzeichnisse, Datenflussdiagrammen oder Dienstbeschreibungen des angebotenen Dienstes prüft ein Evaluator, ob die Risikoanalyse alle Verarbeitungstätigkeiten des Cloud-Anbieters erfasst.

Durch eine Dokumentprüfung stellt ein Evalautor auch fest, welche Gestaltungsprinzipien und -maßnahmen ein Cloud-Anbieter vorgesehen hat, um die festgestellten Risiken zu minimieren und die Einhaltung der Datenschutzgrundsätze zu gewährleisten. Aus den Dokumenten des Cloud-Anbieters sollte der Evaluator auch nachvollziehen können, welche Erwägungen den Cloud-Anbieter beim Ergreifen oder Unterlassen von Gestaltungsmaßnahmen geleitet haben, damit die Angemessenheit der Abwägung geprüft werden kann. Relevante Dokumentationen umfassen die Risikoanalyse, Dienstbeschreibungen, das Datensicherheitskonzept, Rollen- und Berechtigungskonzepte, Prozessbeschreibungen, Verfahrensanweisungen, Richtlinien, der Mustervertrag für Subauftragsverarbeiter, Ergebnisprotokolle von internen Audits und Subauftragsverarbeiterkontrollen, Dokumentationen des Information Security Management Systems, TOM, Incident-Response-Management Dokumentationen und Datenschutz-Folgenabschätzungen. Die Dokumentationen in den obligatorisch zu führenden Verarbeitungsverzeichnissen nach Art. 30 Abs. 2 DSGVO und Nr. 8.3 dieses Katalogs können zudem als Nachweis für die dort aufgeführten Systemgestaltungen dienen. Auch können Protokolle und andere Nachweise zur Durchführung von organisatorischen Gestaltungsprozessen geprüft werden.

Der Abgleich der Dokumentation mit der tatsächlichen Umsetzung der Maßnahmen sollte durch Inspektionen, Prüfungen und (Vor-Ort-)Auditierungen durchgeführt werden. So können unter anderem eine Dienstnutzung (bspw. Überprüfung der Funktionen und Maßnahmen gemäß Dienstbeschreibung), eine Vorgangsüberwachung (bspw. Sicherstellung von Verschlüsselung) und eine Assetprüfung (bspw. Quellcodeanalyse, Analyse von Systemschnittstellen und Hardwarekomponenten) durchgeführt werden, um eingesetzte Hard- oder Software und die Durchführung der Datenverarbeitungsvorgänge auf Umsetzung der Grundsätze in den Systemen zu prüfen. Auch sollte eine Befragung oder Beobachtung relevanter Mitarbeiter durchgeführt werden, um diese auf Kenntnis über Richtlinien und Verfahrensschritte sowie deren Kompetenzen und Verantwortlichkeiten zu prüfen. Auch das Management sollte befragt werden, um sicherzustellen, dass der Datenschutz durch Systemgestaltung als Zielsetzung im Unternehmen verankert ist und wie Entscheidungsprozesse und Abwägungen getroffen werden.

Darüber hinaus sollte eine Entwicklungs- und Designprüfung durchgeführt werden um festzustellen, ob die datenschutzrechtlichen Anforderungen bereits bei der Entwicklung des Systems berücksichtigt werden. Hierzu können Evaluatoren eingesetzte Entwicklungsmethoden und -verfahren (insb. Abnahmekriterien und Anforderungslisten) anhand von Dokumentationen und Befragungen mit Mitarbeitern prüfen. Eine Prüfung von Testsystemen und -umgebungen (bspw. auf Angemessenheit und Sicherheit) kann bei Bedarf durchgeführt werden. Bei der Designprüfung kann unter anderem die gewählte Architektur, Datenbankdiagramme, Datenflussdiagramme, Designentscheidungen aber auch die Konfiguration und Einstellung des Cloud-Dienstes zur Erbringung des Datenverarbeitungsvorgangs überprüft werden.

Ein Evaluator prüft anhand von Prozessdokumentationen (bspw. Protokolle über Entscheidungen, Zeitstempeln, Versionierungshistorie, Change-Logs) und Befragungen der Mitarbeiter (bspw. Bekanntheit der Richtlinien und

[29] Konzeptionelle Zielsetzungen sind solche, die auf das jeweilige Modell der angebotenen Dienste abzielen, d. h. das Angebot von Software-, Plattform- oder Infrastrukturdiensten usw.

Trennung der Verantwortlichkeiten), wie der Stand der Technik überwacht wird und wie Änderungen des Stands der Technik zu Anpassungen von Maßnahmen im angebotenen Dienst führen.

Unterstützend können Sicherheitstests angewendet werden, um bspw. die Sicherheit und Angemessenheit von Gestaltungsmaßnahmen beurteilen zu können.

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

Kriterium

(1) Der Cloud-Anbieter stellt durch seine Voreinstellungen im jeweiligen Dienst sicher, dass nur personenbezogene Daten verarbeitet werden, die für den jeweiligen Verarbeitungszweck erforderlich sind im Hinblick auf die Menge der erhobenen personenbezogenen Daten, der Umfang ihrer Verarbeitung und die Dauer ihrer Speicherung und auch der Zugang zu den personenbezogenen Daten auf das Maß beschränkt wird[30], das erforderlich ist, um den Verarbeitungszweck des Cloud-Nutzers zu erfüllen.

(2) Der Cloud-Anbieter stellt durch Voreinstellungen sicher, dass personenbezogene Daten nicht ohne Eingreifen der betroffenen Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden und hierbei keine unangemessenen Risiken[31] für die betroffenen Personen durch eine zu umfassende Zugänglichmachung[32] von personenbezogenen Daten entstehen.

Ermittlungsmethoden

- Dokumentprüfung
- Inspektion
- Prüfung
- Audit
- Entwicklungs- und Designprüfung

Ermittlung

Zur Überprüfung des Datenschutzes durch Voreinstellungen kann ein Evaluator eine Vielzahl an Ermittlungsmethoden anwenden.

Durch eine Dokumentprüfung stellt ein Evalautor fest, welche Voreinstellungen ein Cloud-Anbieter aus welchen Erwägungen gewählt hat. Dabei sollte eine Durchsicht der Dokumentation der TOM, des Datensicherheitskonzepts, Standardeinstellungen des Cloud-Dienstes, Verfahrensanweisungen, Richtlinien/Konzepten zu Kennwörtern, Authentifizierungen, Zugangs- und Zugriffsberechtigungen, Trennung von Testsystemen, und der dokumentierten Entwicklung des Cloud-Dienstes vorgenommen werden. Auch können Protokolle und andere Nachweise zur Durchführung von technischen Voreinstellungen oder organisatorischen Gestaltungsprozessen geprüft werden.

Der Abgleich der Dokumentation mit der tatsächlichen Umsetzung der Maßnahmen sollte durch Inspektionen, Prüfungen und (Vor-Ort-)Auditierungen durchgeführt werden. Es können unter anderem eine Dienstnutzung (bspw. Überprüfung der Standardkonfiguration darauf, dass nicht erforderliche Verarbeitungsvorgänge deaktiviert sind und Vorauswahl bei Datenfeldern), eine Vorgangsüberwachung (bspw. Umsetzung der Maßnahmen zur Trennung der Entwicklungssysteme) und eine Assetprüfung (bspw. Quellcodeanalyse, Analyse von Systemschnittstellen und Hardwarekomponenten) durchgeführt werden, um Voreinstellungen zu prüfen. Auch sollte eine Befragung oder Beobachtung relevanter Mitarbeiter durchgeführt werden, um diese auf Kenntnis über Richtlinien und Verfahrensschritte, durchgeführte Sensibilisierung zum Datenschutz, auf datenschutz-vorsichtiges Verhalten sowie deren Kompetenzen und Verantwortlichkeiten (insb. in Hinblick auf die Notwendigkeit der Verarbeitung von Daten) zu prüfen. Auch das Management sollte befragt werden, um sicherzustellen, dass der Datenschutz durch Voreinstellung als Zielsetzung im Unternehmen verankert ist.

Darüber hinaus sollte eine Entwicklungs- und Designprüfung durchgeführt werden um festzustellen, ob die datenschutzrechtlichen Anforderungen und Voreinstellungen bereits bei der Entwicklung des Systems berücksichtigt werden. Hierzu können Evaluatoren eingesetzte Entwicklungsmethoden und -verfahren (insb. Abnahmekriterien und gewählte Voreinstellungen) anhand von Dokumentationen und Befragungen mit Mitarbeitern prüfen. Eine Prü-

[30] In Bezug auf Letzteres muss der Cloud-Anbieter sicherstellen, dass Personen, die unter seiner Aufsicht handeln, nur auf einer Need-To-Know-Basis auf personenbezogenen Daten zugreifen können, d.h. wenn sie diese kennen müssen.

[31] Unangemessene Risiken ergeben sich aus der Nichtberücksichtigung des Stands der Technik, der Kosten der Umsetzung und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Risiken unterschiedlicher Wahrscheinlichkeit und Schwere für die Rechte und Freiheiten natürlicher Personen, die von der Verarbeitung ausgehen.

[32] Eine „zu umfassende Zugänglichmachung“ liegt vor, wenn ein technischer oder persönlicher Zugriff einen Einblick in mehr Informationen zulässt als für den jeweiligen Zweck der Verarbeitung erforderlich.

fung von Testsystemen und -umgebungen (bspw. auf Umsetzung von Voreinstellungen) kann bei Bedarf durchgeführt werden. Bei der Designprüfung können unter anderem Datenflussdiagramme, Designentscheidungen aber auch die Konfiguration und Einstellung des Cloud-Dienstes zur Erbringung des Datenverarbeitungsvorgangs überprüft werden.

Unterstützend können Sicherheitstests angewendet werden, um bspw. die Sicherheit und Angemessenheit von Gestaltungsmaßnahmen beurteilen zu können.

Kapitel V: Subauftragsverarbeitung

Nr. 10 – Subauftragsverhältnisse

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

Kriterium

(1) Der Cloud-Anbieter verfügt über einen definierten Prozess, der sicherstellt, dass ein Cloud-Dienst unter Einbeziehung von Subauftragsverarbeitern nur dann erbracht wird, wenn und soweit der Cloud-Nutzer seine vorherige gesonderte oder allgemeine Genehmigung in die Subauftragsverarbeitung erteilt hat. Die Genehmigung muss schriftlich oder im elektronischen Format erfolgen. Im Falle einer allgemeinen schriftlichen Genehmigung muss der Cloud-Anbieter den Cloud-Nutzer über jede beabsichtigte Veränderung in Bezug auf die Ergänzung oder den Ersatz eines Auftragsverarbeiters informieren und auf diese Weise dem Cloud-Nutzer die Möglichkeit geben, derartigen Veränderungen zu widersprechen.

(2) Erfolgt eine vorherige gesonderte Genehmigung der Subauftragsverarbeitung, hat der Cloud-Anbieter sicherzustellen, dass alle Subauftragsverarbeiter namentlich und mit ladungsfähiger Anschrift benannt werden sowie die Verarbeitungen, für die sie eingesetzt werden sollen, festgelegt sind.

(3) Der Cloud-Anbieter stellt sicher, dass alle von ihm beauftragten Subauftragsverarbeiter, die durch den Cloud-Anbieter im Rahmen seiner Risikobewertung oder aufgrund der Zertifizierungskriterien definierten TOM umsetzen. Der Cloud-Anbieter muss zudem sicherstellen, dass dieselben Verpflichtungen zwischen ihm und den Subauftragsverarbeitern, wie sie in der rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung oder in einem anderen Rechtsinstrument niedergelegt sind, jedem Glied der Kette der Subauftragsverarbeiter auferlegt sind.

Ermittlungsmethoden

- Dokumentprüfung, insbesondere Rechtsanalyse
- Audit

Ermittlung

Ein Evaluator führt eine Dokumentprüfung durch, indem er die erteilten Zustimmungen der Cloud-Nutzer nachprüft. Bei standardisierten Cloud-Diensten sind die standardisierten rechtsverbindlichen Vereinbarungen und ggf. darin enthaltenen Generalzustimmungen zu prüfen. Bei individualen Vereinbarungen mit Cloud-Nutzern müssen diese stichprobenartig und vorhandene Vereinbarungsvorlagen überprüft werden. Sollten weitere Dokumentationen der Einwilligung vorliegen, sind diese stichprobenartig zu prüfen. Schließlich kann überprüft werden, ob eine Änderung der Vereinbarungsvorlagen oder Generalzustimmungen durchgeführt wurde, nachdem eine neue Vereinbarung mit einem Subauftragsverarbeiter geschlossen wurde (bspw. Zeitstempel, Versionierung, Change-Log). Im Falle einer Veränderung prüft der Evaluator, ob Nachweise über die Kommunikation mit dem Cloud-Nutzer vorliegen. Falls vorliegend prüft der Evaluator, ob Widersprüche durch Cloud-Nutzer abgeben wurden.

Im Rahmen eines Audits kann der Evaluator zudem eine Befragung der zuständigen Mitarbeiter durchführen, um zu prüfen, ob der festgelegte Prozess zur Einbeziehung und Änderung von Subauftragsverarbeitern bekannt ist und gelebt wird. Dazu zählt insb. auch die Information des Cloud-Nutzers. Die Ermittlungen in Bezug auf die Verpflichtung des/der Subauftragsverarbeiters/Subauftragsverarbeiter werden in den folgenden Kriterien durchgeführt.

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.

Ermittlungsmethoden

- Dokumentprüfung, insbesondere Rechtsanalyse

Ermittlung

Der Evaluator sollte eine Einsichtnahme in das Verzeichnis eingesetzter Subauftragsverarbeiter bekommen und eine stichprobenartige Prüfung geschlossener Vereinbarungen mit Subauftragsverarbeitern durchführen. Ein Evaluator prüft die Vereinbarungen zu den Subauftragsverarbeitern mitsamt der für die Konformitätsprüfung erforderlichen Angaben auf Vollständigkeit und Zulässigkeit der Inhalte nach Art. 28 Abs. 3 und 4 DSGVO (Prüfung auf u.a. Dauer, Art und Zweck, Ort der weiteren Verarbeitung, Angaben über den Auftragsverarbeiter und dessen Dienstbeschreibung, Angaben über weitere eingebundene Subauftragsverarbeiter und jeweils dessen Dienstbeschreibung sowie die Verpflichtung zur Einhaltung). Für die jeweiligen Subauftragsverarbeiter sollten vorliegende Dokumente der TOM, das Datensicherheitskonzept oder Zertifikate stichprobenartig geprüft werden. Weitere relevante Dokumente können bei der Prüfung einbezogen werden, darunter der Mustervertrag zur Auftragsverarbeitung mit Subauftragsverarbeiter, Richtlinien und Anweisungen, weitere Garantien der Subauftragsverarbeiter, interne Kontrollbereiche des Cloud-Anbieters über Subauftragsverarbeiterkontrollen, das Datenschutzkonzept, oder die Risikoabschätzung bei der Unterbeauftragung.

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

Kriterium

(1) Wird die Genehmigung zur Subauftragsverarbeitung in allgemeiner Form erteilt, informiert der Cloud-Anbieter den Cloud-Nutzer über die Identität aller von ihm eingeschalteten Subauftragsverarbeiter (einschließlich ladungsfähiger Anschrift) und über die Verarbeitungen, die diese vornehmen sollen.

(2) Der Cloud-Anbieter informiert den Cloud-Nutzer 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.

Ermittlungsmethoden

- Dokumentprüfung
- Inspektion
- Audit

Ermittlung

Ein Evaluator prüft die Dokumente, die schildern, wie ein Cloud-Anbieter den Cloud-Nutzer Informationen über eingebundene Subauftragsverarbeiter zur Verfügung stellt (bspw. in den rechtsverbindlichen Vereinbarungen, in Form von Generalzustimmungen, in Informationsportale) und bei beabsichtigter Änderung von Subauftragsverarbeitern informiert sowie Einsprüche von Cloud-Nutzer entgegennimmt und bearbeitet. Außerdem prüft er die Dokumentation über die involvierten Subauftragsverarbeiter auf Vollständigkeit (bspw. der Angabe von Identität, ladungsfähiger Anschrift und der ausgeführten Verarbeitungen). Der Evaluator kann auch eine Durchsicht weiterer relevanter Dokumente vornehmen, bspw. Mustervereinbarung mit Cloud-Nutzern, Dokumentationen der Einwilligung von Cloud-Nutzern sowie der Ausübung des Widerspruchsrecht, und weitere Richtlinien. Er kann Einsichtnahme in das Verzeichnis eingesetzter Subauftragnehmer bekommen, stichprobenartige Prüfungen geschlossener Cloud-Nutzer-Vereinbarungen durchführen, und die Verfügbarkeit der Informationen für den Cloud-Nutzer prüfen. Schließlich kann überprüft werden, ob eine Änderung der Vereinbarungsvorlagen oder Generalzustimmungen mit Cloud-Nutzern durchgeführt wurde, nachdem eine neue Vereinbarung mit einem Subauftragsverarbeiter geschlossen wurde (bspw. Zeitstempel, Versionierung, Change-Log). Protokolle über mitgeteilte Änderungen der Einbindung von Subauftragsverarbeitern oder bearbeitete Einsprüche sollten vom Evaluator geprüft werden, insofern vorhanden.

Durch eine Inspektion in Form einer Vorgangsüberwachung oder durch eine Beobachtung im Rahmen eines Audits kann geprüft werden, ob dem Cloud-Nutzer alle notwendigen Informationen zur Einbindung von Subauftragsverarbeiter auf geeignete Weise kommuniziert werden. Hierzu kann testweise eine Anfrage von einem Cloud-Nutzer durch einen Evaluator simuliert werden. Gleichermaßen kann die Bearbeitung eines Einspruchs durch einen Cloud-Nutzers überprüft werden. Eine Befragung relevanter Mitarbeiter (z.B. zur Kenntnis über Richtlinien, Entgegennahme von Anfragen und Einsprüchen des Cloud-Nutzers etc.) kann durchgeführt werden.

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

Kriterium

(1) Der Cloud-Anbieter stellt sicher, dass nur solche Subauftragsverarbeiter in die Auftragsverarbeitung einbezogen werden, die die Gewähr für die Einhaltung der in der rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung niedergelegten datenschutzrechtlichen Verpflichtungen an die von ihnen zu erbringende Leistung bieten.

(2) Der Cloud-Anbieter überzeugt sich davon, dass alle eingesetzten Subauftragsverarbeiter die in der rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung niedergelegten datenschutzrechtlichen Verpflichtungen an die von ihnen zu erbringende Leistung erfüllen.

Ermittlungsmethoden

- Dokumentprüfung
- Inspektion
- Audit

Ermittlung

Ein Evaluator prüft vorhandene Dokumente der eingesetzten Subauftragsverarbeiter (befolgte Verhaltensregeln, Zertifikate, rechtsverbindliche Vereinbarungen, Dienstbeschreibungen, Datensicherheitskonzepte, sonstige Garantien), aus denen sich die Gewähr zur Einhaltung der Datenschutz-Grundverordnung ergibt. Darüber hinaus prüft er Dokumente über die Auswahl (bspw. Protokolle über Auswahlüberlegungen und -entscheidungen) und der Durchführung von eigenen Kontrollen (bspw. Protokolle der Subauftragsverarbeiterkontrollen).

Im Sinne einer Inspektion kann eine Beauftragung und Kontrolle eines Subauftragsverarbeiters simuliert werden, bei der ein Evalautor prüft, ob die Verfahrensschritte vollständig und korrekt durchlaufen werden. Hierbei können unterschiedliche Test-Subauftragsverarbeiter gewählt werden, z.B. ein Unternehmen, welches die datenschutzrechtlichen Anforderungen nicht erfüllt, sodass der Auswahlprozess diese Problematik offenbaren sollte. Im Zuge dessen, können auch Kompetenzen der Mitarbeiter und korrekte Zuständigkeiten und Verantwortlichkeiten überprüft werden.

Unterstützend kann im Rahmen eines Audits eine Befragung der Mitarbeiter zur Durchführung der Kontrolle von Subauftragsverarbeitern durchgeführt werden (bspw. Bekanntheit von Verfahrensschritten und Garantien der Subauftragsverarbeiter). Auch kann geprüft werden, ob einzelne Fachabteilungen weitere Subauftragsverarbeiter beauftragt haben oder einsetzen, welche jedoch bisher dem Evaluator nicht bekannt waren.

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

Kriterium

(1) Der Cloud-Anbieter stellt sicher, dass auch bei der Einschaltung von (mehreren) Subauftragsverarbeitern seine Unterstützungsfunktionen im vereinbarten Umfang sowie seine Pflichten als Hauptauftragsverarbeiter erfüllt werden.

(2) Der Cloud-Anbieter stellt sicher, dass seine Unterstützungsfunktionen und seine Verpflichtungen als der Hauptauftragsverarbeiter im vereinbarten Umfang erfüllt werden, auch wenn (mehrere) Subauftragsverarbeiter beauftragt sind.

Ermittlungsmethoden

- Dokumentprüfung
- Audit

Ermittlung

Ein Evaluator prüft vorgelegte Dokumente zu Verfahren und Vorkehrungen des Cloud-Anbieters zur Einbindung von Subauftragsverarbeitern, darunter rechtsverbindliche Vereinbarungen mit Subauftragsverarbeitern, Prozessdokumentationen zur Einbindung, Datensicherheitskonzepte und Informationen über Ansprechpartner der Subauftragsverarbeiter, Risikoanalysen oder Dokumente zur Verantwortlichkeitstrennung für einzelne Verarbeitungsprozesse. Protokolle zur Pflichterfüllung infolge der Einschaltung von weiteren Auftragsverarbeitern sollten geprüft werden.

Unterstützend kann im Rahmen eines Audits eine Befragung der Mitarbeiter zur Einbindung von Subauftragsverarbeitern bei den Unterstützungsfunktionen und Pflichten als Hauptauftragsverarbeiter durchgeführt werden (bspw. Bekanntheit von Verfahrensschritten und Ansprechpartner der Subauftragsverarbeiter).

Kapitel VI: Datenverarbeitung außerhalb der EU und des EWR

Nr. 11 – Datenübermittlung[33]

Nr. 11.1 – Geeignete Garantien für die Datenübermittlung; Maßnahmen zum Schutz vor der Offenlegung gegenüber staatlichen Stellen von Drittländern (Art. 45, 46 und Art. 48 DSGVO)

Kriterium

(1) Der Cloud-Anbieter kann personenbezogene Daten in Drittländer oder an internationale Organisationen übermitteln, sofern er überprüft hat, dass 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 und der Cloud-Anbieter regelmäßig (mindestens jährlich) prüft, ob der Angemessenheitsbeschluss fort gilt und die in Frage stehende Übermittlung über den benannten Beschluss erfasst wird.

(2) Alternativ kann die Datenübermittlung stattfinden, wenn der Cloud-Anbieter nach Überprüfung von Rechtslage und Praxis im Drittland sicherstellt, dass die in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung festgelegten geeigneten Garantien im Sinne des Art. 46 Abs. 2 oder 3 DSGVO verwendet werden und diese geeigneten Garantien ein angemessenes Datenschutzniveau sicherstellen, das dem der Datenschutz-Grundverordnung gleichwertig ist.

(3) Reichen nach Überprüfung von Rechtslage und Praxis im Drittland die in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung[34] festgelegten geeigneten Garantien im Sinne des Art. 46 Abs. 2 oder 3 DSGVO nicht aus, um ein angemessenes Datenschutzniveau sicherzustellen, das dem der Datenschutz-Grundverordnung gleichwertig ist, ergreift der Cloud-Anbieter zusätzliche Maßnahmen, um dieses angemessene Datenschutzniveau sicherzustellen. Andernfalls darf keine Datenübermittlung stattfinden. Der Cloud-Anbieter muss dafür sorgen, dass der Cloud-Nutzer die durchgeführte Bewertung erhält, in Bezug auf das Recht und Praxis des Drittlandes, um überprüfen zu können, ob die vom Auftragsverarbeiter getroffenen zusätzlichen Maßnahmen tatsächlich ein angemessenes Schutzniveau für die in das Drittland übermittelten personenbezogenen Daten gewährleisten.

(4) Der Cloud-Anbieter überwacht fortlaufend die Angemessenheit des Datenschutzniveaus und stellt sicher, dass Datenübermittlungen umgehend ausgesetzt oder beendet werden, wenn im Fall des Abs. 2 oder 3 der Empfänger die Pflichten, die er nach den geeigneten Garantien des Art. 46 Abs. 2 oder 3 DSGVO eingegangen ist, verletzt hat oder ihre Erfüllung unmöglich ist und im Fall von Abs. 3 die zusätzlichen Maßnahmen nicht mehr eingehalten werden können oder unwirksam sind.[35]

(5) Cloud-Anbieter, die personenbezogene Daten verarbeiten und nicht nur dem Recht der Datenschutz-Grundverordnung unterliegen, sondern zugleich dem Recht eines Drittlands, das sie zu einer Offenlegung dieser personenbezogenen Daten gegenüber staatlichen Stellen des Drittlands verpflichtet, ergreifen zusätzliche Maßnahmen, um die personenbezogenen Daten vor einer Offenlegung an staatliche Stellen des Drittlands wirksam zu schützen. Der Cloud-Anbieter stellt sicher, dass personenbezogene Daten staatlichen Stellen von Drittländern nur offengelegt werden, wenn die Offenlegung auf eine in Kraft befindliche internationale Übereinkunft zwischen dem ersuchenden Drittland und der Union oder Deutschland gestützt ist. Der Cloud-Anbieter muss den Cloud-Nutzer über diese rechtliche Verpflichtung vor einer Offenlegung informieren, sofern die Information nicht aus anerkannten wichtigen Gründen des öffentlichen Interesses im EU- oder deutschem Recht verboten ist.

(6) Wenn der Cloud-Anbieter Daten an einen außerhalb der EU oder des EWR ansässigen Auftragsverarbeiter übermittelt (im Sinne von Art. 44 DSGVO), muss er die in Kapitel V der DSGVO festgelegten Verpflichtungen in vollem Umfang erfüllen.

---

[33] Die Übermittlung bezieht sich auf die Bewegung personenbezogener Daten, wenn diese aus der EU/dem EWR in ein Land oder mehrere Länder außerhalb der EU/des EWR übermittelt werden sowie auch die Fälle, in denen Daten durch Fernzugriff zugänglich gemacht oder dem Datenimporteur mitgeteilt werden. Siehe EDSA-Leitlinien 05/2021 zum Zusammenspiel zwischen Art. 3 und Kapitel V der Datenschutz-Grundverordnung.

[34] Es versteht sich von selbst, dass der Auftragsverarbeiter bei Datenübermittlungen weiterhin an die Weisungen des Verantwortlichen gebunden ist, wie sie in der rechtsverbindlichen Vereinbarung zur Auftragsdatenverarbeitung festgelegt sind, siehe Kriterium Nr. 1.4(1).

[35] Es versteht sich von selbst, dass der Auftragsverarbeiter bei Datenübermittlungen weiterhin an die Weisungen des Verantwortlichen gebunden ist, wie sie in der rechtsverbindlichen Vereinbarung zur Auftragsdatenverarbeitung festgelegt sind, siehe Kriterium Nr. 1.4(1).

Ermittlungsmethoden

- Dokumentprüfung, insbesondere Rechtsanalyse
- Inspektion
- Prüfung
- Audit

Ermittlung

Ein Evaluator führt eine Dokumentprüfung durch. Dabei prüft er das Verzeichnis eingesetzter Subauftragsverarbeiter in Drittländern oder die Liste an Ländern, in die Daten übermittelt werden, sowie weitere Dokumente (bspw. eine Vertragsvorlage zur Empfängerverpflichtung). Ein Evaluator prüft, ob für den Empfängerstaat oder die internationale Organisation ein Beschluss der Europäischen Kommission nach Art. 45 Abs. 3 DSGVO vorliegt oder der Cloud-Anbieter Dokumente über die vereinbarten geeigneten Garantien nach Art. 46 Abs. 2 oder 3 DSGVO oder vorhandene Zertifizierungen nach Art. 42 Abs. 2 DSGVO und die ergänzenden rechtsverbindlichen und durchsetzbaren Verpflichtungen zur Anwendung der geeigneten Garantien nachweisen kann. Basiert die Drittlandsübermittlung auf vereinbarten geeigneten Garantien nach Art. 46 Abs. 2 oder 3 DSGVO, sind im Rahmen einer Dokumentenprüfung die Dokumentationen des Cloud-Anbieters zur Beurteilung von Rechtslage und Rechtspraxis im Rahmen des sechsschrittigen Fahrplans des Europäischen Datenschutzausschusses im betreffenden Drittland zu überprüfen. Ein Evaluator sollte hierbei die Dokumentationen zu allen sechs Schritten des Fahrplans prüfen. Der Evaluator prüft, ob die in die Beurteilung einbezogenen Quellen wie z.B. Rechtsvorschriften, Rechtsprechung des EuGH oder nationaler Gerichte, Berichte zwischenstaatlicher Organisationen, Berichte über Erfahrungen zur Rechtspraxis usw. hinreichend sind, um die Einhaltung der wesentlichen europäischen Garantien und somit die Angemessenheit des Datenschutzniveaus im Drittland für die konkreten Datenübermittlungen beurteilen zu können. Hierfür sollte sich der Evaluator die konkreten Ausführungen des Cloud-Anbieters zur Einhaltung der wesentlichen europäischen Garantien im jeweiligen Drittland vorlegen lassen. Wo dem Evaluator über das gebotene Prüfprogramm hinaus aufgrund seiner Zertifizierungserfahrung für den Cloud-Dienst einschlägige, aus europäischer Sicht problematische Regelungen des Drittlands zum Zugang staatlicher Stellen zu personenbezogenen Daten bekannt sind, prüft der Evaluator zusätzlich, ob diese Regelungen auch in den Dokumentationen des Cloud-Anbieters aufgeführt und behandelt werden. Befragungen im Rahmen eines Audits mit den für die Beurteilung des Datenschutzniveaus befassten Mitarbeitern können ebenfalls durchgeführt werden (bspw. Kenntnis der Verfahrensschritte zur Prüfung des angemessenen Schutzniveaus und der relevanten Quellen, die für die Beurteilung einbezogen werden sollten, Kenntnis der wesentlichen europäischen Garantien und wie ihre Einhaltung bzw. Nichteinhaltung zu prüfen ist).

Kommen die Ausführungen des Cloud-Anbieters zu dem Schluss, dass Rechtslage und Rechtspraxis im Drittland den wesentlichen europäischen Garantien nicht genügen, prüft der Evaluator im Rahmen einer Dokumentenprüfung die Dokumentationen des Cloud-Anbieters zu den zusätzlichen Maßnahmen, die nach dem 4. Schritt des Fahrplans ergriffen worden sind, um ein angemessenes Datenschutzniveau im Drittland zu gewährleisten. Hierbei sollte ein Evaluator insbesondere prüfen, ob die zusätzlichen Maßnahmen hinreichend sind, um die Schutzlücken, die im Drittland bestehen und zu einer Unangemessenheit des Datenschutzniveaus führen, zu beseitigen.

Die Ermittlungsmethoden, die der Evaluator anwendet, hängen von der Art der zusätzlichen Maßnahmen ab: Verpflichtet sich der Cloud-Anbieter z.B. vertraglich dazu, keine Hintertüren oder ähnliche technischen Maßnahmen im Cloud-Dienst eingebaut zu haben, die staatlichen Stellen von Drittländern den Zugang zum Cloud-Dienst und zu den personenbezogenen Daten verschaffen oder diesen erleichtern, prüft der Evaluator die entsprechenden Klauseln im Vertrag im Rahmen einer Dokumentenprüfung. Ergänzend soll der Cloud-Dienst vom Evaluator im Rahmen einer Inspektion stichprobenartig auf verdächtige Datenabflüsse geprüft werden.

Vereinbarte organisatorische Maßnahmen sollten im Rahmen einer Dokumentenprüfung durch die Vorlage von z.B. erhaltenen Transparenzberichten oder „Warrant Canary“-Erklärungen des Empfängers überprüft werden.

Auch können vom Evaluator weitere Dokumentationen zu Maßnahmen überprüft werden, die der Cloud-Anbieter durchführt, um die Angemessenheit des Datenschutzniveaus im Drittland regelmäßig zu überprüfen, z.B. proaktive Abfragen bei Empfängern nach Rechtsänderungen im betreffenden Drittland, Bearbeitung der regelmäßigen Meldungen, die der Empfänger aufgrund vertraglicher Pflichten zu geänderten Rechtsvorschriften oder Anfragen von staatlichen Stellen an den Cloud-Anbieter macht. Weiterhin sollen Dokumentationen zu Maßnahmen, Verfahren und Zuständigkeiten überprüft werden, die vom Cloud-Anbieter ergriffen werden, wenn das Datenschutzniveau im Drittland nicht mehr angemessen ist und die Datenübermittlung daher eingestellt wird. Auch kann hier eine Befragung im Rahmen eines Audits mit den zuständigen Mitarbeitern, z.B. im Hinblick auf die Kenntnis des relevanten Vorgehens in diesem Fall, durchgeführt werden.

Die Vorlage einer aktuell gültigen Zertifizierung nach Art. 42 Abs. 2 DSGVO, die bereits für Datenverarbeitungsvorgänge des zu zertifizierenden Zertifizierungsgegenstands erlangt worden ist, kann ebenfalls von einem Evaluator überprüft werden. In diesem Fall erstreckt sich die Prüfung des Evaluators auch auf die Verbindlichkeit und Durchsetzbarkeit der eingegangenen Verpflichtung zur Anwendung der geeigneten Garantien.

Wird Verschlüsselung eingesetzt, sollten zunächst im Rahmen einer Dokumentenprüfung die Dokumentationen zum jeweiligen Verfahren überprüft werden. Anhand der aktuellen technischen Anforderungen und Richtlinien, z.B.

vom BSI, sollte der Evaluator prüfen, ob eine starke Verschlüsselung gewählt wurde, die auch den Zeitraum berücksichtigt, für den die Vertraulichkeit der verschlüsselten Daten sicherzustellen ist-, der Verschlüsselungsalgorithmus hinsichtlich seiner Schlüssellänge und sonstiger Parametrisierung dem Stand der Technik entspricht und wie die Schlüsselverwaltung organisiert ist. Hierfür kann der Evaluator Einsicht nehmen in Dokumentationen zum Verschlüsselungsverfahren, Richtlinien, Protokoll- und Logdaten, Ergebnisprotokolle interner/externer Audits und Risikoanalysen. Die Implementierung des Verschlüsselungsverfahrens wird im Rahmen einer Inspektion und/oder Prüfung durch repräsentative Stichproben festgestellt und auf Angemessenheit überprüft. Geprüft werden sollte auch, wie Schlüssel erzeugt werden und die Schlüsselverwaltung aufgebaut ist und ob die Schlüssel allein beim Exporteur oder bei anderen mit dieser Aufgabe betrauten Stellen im EWR oder in einem Drittland mit Angemessenheitsbeschluss liegen. Auch die Software für die Verschlüsselung und ihre Konfiguration sollte im Rahmen einer Assetprüfung überprüft und auf das Vorhandensein von Auffälligkeiten geprüft werden. Ebenso wird die korrekte Speicherung der verschlüsselten Daten durch eine Prüfung festgestellt. Die Implementierung und Sicherheit der Verschlüsselungsverfahren wird durch repräsentative technische Tests (z.B. Penetrationstests) festgestellt und auf Angemessenheit überprüft.

Wird Pseudonymisierung eingesetzt, sollten zunächst im Rahmen einer Dokumentenprüfung die Dokumentationen zum jeweiligen Verfahren überprüft werden. Der Evaluator prüft, wie die Pseudonymisierung vorgenommen wird, damit eine Personenbeziehbarkeit ohne Hinzuziehung der zusätzlichen Information nicht mehr gegeben ist, und wie die Identifizierungsdateien beim Exporteur aufbewahrt und geschützt werden. Hierfür können z.B. Dokumentationen der TOM, Richtlinien, Protokoll- und Logdaten, Ergebnisprotokolle interner/externer Audits oder Risikoanalysen geprüft werden. Durch eine Befragung der Mitarbeiter sollte ebenfalls überprüft werden, ob diese die aktuellen Empfehlungen zur Pseudonymisierung kennen und umsetzen.

Die Implementierung des Pseudonymisierungsverfahren sollte zusätzlich im Rahmen einer Inspektion und/oder Prüfung durch repräsentative Stichproben festgestellt und auf Angemessenheit überprüft werden. Ebenso wird die korrekte Verarbeitung der pseudonymen Daten durch eine Prüfung festgestellt. Dazu sollten die Art der eingesetzten Programme, die Programmierungen zur Pseudonymisierung und deren Konfiguration im Rahmen einer Assetprüfung überprüft und eine stichprobenartige Prüfung von Datensätzen durchgeführt werden.

Eine Überprüfung der Wirksamkeit der ergriffenen TOM zum Schutz der zusätzlichen Informationen zur Identifizierbarkeit ist ebenfalls erforderlich, damit festgestellt werden kann, dass die Kontrolle über den Pseudonymisierungsalgorithmus oder den Datenspeicher, der die Re-Identifizierung anhand der zusätzlichen Informationen ermöglicht, allein beim Exporteur liegt und zwar ausschließlich in einem Mitgliedstaat oder in einem Drittland bei einer vom Exporteur betrauten Stelle im EWR oder in einer Rechtsordnung, die ein dem EWR im Wesentlichen gleichwertiges Schutzniveau bietet und daher weder der Pseudonymisierungsalgorithmus noch der Datenspeicher, der die Re-Identifizierung anhand der zusätzlichen Informationen ermöglicht, einem Herausgabeanspruch aus dem Drittland unterliegt.

Wenn der Cloud-Anbieter personenbezogene Daten verarbeitet und nicht nur dem Recht der Datenschutz-Grundverordnung unterliegt, sondern zugleich dem Recht eines Drittlands, das ihn zu einer Offenlegung dieser personenbezogenen Daten gegenüber staatlichen Stellen des betreffenden Drittlands verpflichtet, bedarf es einer ebenso umfassenden, wie bedarfsgerechten Prüfung durch den Evaluator, mit der die Wirksamkeit der zusätzlich zu ergreifenden Maßnahmen durch den Cloud-Anbieter sichergestellt wird.

Im Rahmen einer Dokumentenprüfung sind die Dokumentationen zu den zusätzlichen Maßnahmen zu überprüfen, die der Cloud-Anbieter ergriffen hat, um die personenbezogenen Daten vor einer Offenlegung gegenüber den staatlichen Stellen des Drittlands wirksam zu schützen. Wird oder werden beispielsweise Verschlüsselungs- und/oder Pseudonymisierungsverfahren eingesetzt, ist im Rahmen der Dokumentenprüfung die Dokumentationen zu den/dem jeweiligen Verfahren zu überprüfen. Bezüglich der Vorgehensweise im Einzelnen gelten die vorstehenden, für die zusätzlichen Maßnahmen zu Verschlüsselung und Pseudonymisierung im Kontext der Drittlandsübermittlungen aufgeführten Maßstäbe hinsichtlich der Dokumentenprüfung entsprechend.

Bei technischen Maßnahmen sind die Maßnahmen auch im Rahmen von Tests und Inspektionen auf ihre Wirksamkeit zu prüfen. Wird oder werden beispielsweise Verschlüsselungs- und/oder Pseudonymisierungsverfahren eingesetzt, soll die wirksame Implementierung im Rahmen einer Inspektion und/oder Prüfung durch repräsentative Stichproben festgestellt und auf Angemessenheit überprüft werden. Bezüglich der Vorgehensweise im Einzelnen gelten die vorstehenden, für die zusätzlichen Maßnahmen zu Verschlüsselung und Pseudonymisierung im Kontext der Drittlandsübermittlungen aufgeführten Maßstäbe hinsichtlich der Implementierung entsprechend.

Sollten Pseudonymisierungsverfahren eingesetzt werden, ist eine Überprüfung der Wirksamkeit der ergriffenen TOM zum Schutz der zusätzlichen Informationen zur Identifizierbarkeit ebenfalls erforderlich, damit festgestellt werden kann, dass die Kontrolle über den Pseudonymisierungsalgorithmus oder den Datenspeicher, der die Re-Identifizierung anhand der zusätzlichen Informationen ermöglicht, bei einer vom Cloud-Anbieter betrauten vertrauenswürdigen und auf die Vertraulichkeit verpflichteten Stelle (z.B. Treuhänder) liegt und zwar ausschließlich in einem Mitgliedstaat oder in einem Drittland im EWR oder in einer Rechtsordnung, die ein dem EWR im Wesentlichen gleichwertiges Schutzniveau bietet und daher weder der Pseudonymisierungsalgorithmus noch der Datenspeicher, der die Re-Identifizierung anhand der zusätzlichen Informationen ermöglicht, einem Herausgabeanspruch aus dem Drittland unterliegt. Entsprechendes gilt bei der Anwendung von Verschlüsselungsverfahren für die Aufbewahrung kryptographischen Schlüsselmaterials.

Darüber hinaus können auch Mitarbeiterbefragungen zur bisherigen Handhabung entsprechender Herausgabeverlangen aus Drittländern (z.B. im Hinblick auf die Kenntnis des festgelegten Vorgehens) durchgeführt werden.

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

Kriterium

(1) Cloud-Anbieter ohne Niederlassung in der EU oder im EWR, für die dennoch gemäß Art. 3 Abs. 2 DSGVO die Datenschutz-Grundverordnung gilt, benennen schriftlich einen Vertreter in der EU oder im EWR. 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.

(2) Der Cloud-Anbieter beauftragt den Vertreter als Ansprechpartner für sämtliche Fragen im Zusammenhang mit der Datenverarbeitung zur Gewährleistung der Einhaltung der Datenschutz-Grundverordnung und erteilt dem Vertreter die notwendigen Vollmachten, damit dieser im Namen des Cloud-Anbieters und an dessen Stelle tätig werden kann, um die Pflichten der Datenschutz-Grundverordnung zu erfüllen.

Ermittlungsmethoden

- Dokumentprüfung

Ermittlung

Ein Evaluator führt eine Dokumentprüfung durch, dabei prüft er bspw. Verträge mit Vertretern, Benennungsurkunden, Richtlinien, öffentliche Informationen für Cloud-Nutzer (bspw. Kontaktinformationen des Vertreters auf der Website), Verantwortlichkeiten und deren Rollenbeschreibungen. Ein Evaluator führt ein Abgleich mit der Zuständigkeit der Vertreter (zugeordnete Mitgliedstaaten) und den Staaten in denen sich Cloud-Nutzer befinden durch. Hierzu können rechtsverbindliche Vereinbarungen mit dem Cloud-Nutzer und Dokumente über die Staaten, in denen der Cloud-Dienst genutzt werden kann, herangezogen werden. Abhängig von der Anzahl der Vertreter kann eine stichprobenartige Prüfung durchgeführt werden.

C. Kriterien und Ermittlungsmethoden für Verarbeitung als Verantwortlicher

Kapitel VII: Der Cloud-Anbieter als Verantwortlicher

Nr. 12 – Sicherstellung der Datenschutzgrundsätze (Art. 5 Abs. 1 und 2 i.V.m. Art. 24 DSGVO)

Kriterium

(1) Der Cloud-Anbieter stellt bei der Verarbeitung von personenbezogenen Daten, die für die Durchführung des Auftrags über die Erbringung des Cloud-Dienstes oder zur Erfüllung rechtlicher Verpflichtungen erforderlich sind, der betroffenen Person alle Informationen zur Verfügung, die diese benötigt, um die Rechtmäßigkeit der Verarbeitung überprüfen zu können (Grundsatz der Transparenz und Rechtmäßigkeit). Der Cloud-Anbieter darf die Daten der betroffenen Person nur nach Treu und Glauben verarbeiten (Grundsatz von Treu und Glauben[36]).

(2) Der Cloud-Anbieter legt für die Verarbeitung der Daten zur Durchführung des Auftrags über die Erbringung des Cloud-Dienstes und zur Erfüllung rechtlicher Verpflichtungen die Zwecke der jeweiligen Datenverarbeitungen eindeutig und präzise fest (Grundsätze der Zweckfestlegung und Zweckbindung).

(3) Der Cloud-Anbieter legt einen Prozess fest und verfügt über TOM, die gewährleisten, dass nur personenbezogene Daten verarbeitet werden, soweit diese zur Erreichung der festgelegten Verarbeitungszwecke erforderlich (d.h. angemessen, erheblich und auf das notwenige Maß beschränkt) sind (Grundsatz der Datenminimierung).

(4) Der Cloud-Anbieter legt einen Prozess fest und verfügt über TOM zur Prüfung der sachlichen Richtigkeit, Korrektur und Löschung unzutreffender oder unvollständiger personenbezogener Daten, die er für die Durchführung des Auftrags über die Erbringung des Cloud-Dienstes und zur Erfüllung rechtlicher Verpflichtungen verarbeitet (Grundsatz der Datenrichtigkeit).

(5) Der Cloud-Anbieter legt einen Prozess fest und stellt durch TOM sicher, dass bei der Datenverarbeitung der Personenbezug nur solange hergestellt wird, wie dies für die Erreichung der festgelegten Zwecke zur Durchführung des Auftrags über die Erbringung des Cloud-Dienstes oder zur Erfüllung rechtlicher Verpflichtungen unverzichtbar ist und löscht nicht erforderliche Daten frühestmöglich. Dazu legt er Kriterien fest, nach denen ein Personenbezug ermittelt, für den konkreten Verarbeitungszweck erhalten und für die geeignete Speicherung im erforderlichen Maß (Umfang und Dauer) vorgehalten wird (Grundsatz der Speicherbegrenzung).

Ermittlungsmethoden

- Dokumentprüfung, insbesondere Rechtsanalyse
- Inspektion
- Prüfung
- Audit
- Entwicklungs- und Designprüfung

[36] "Treu und Glauben [Fairness]" kann als eine Art Auffangklausel gesehen werden, "um eine unzulässige Datenverarbeitung auch in Ermangelung einer entsprechenden Regelung als rechtswidrig qualifizieren zu können". Dieser Rechtsbegriff ist bereits im deutschen Zivilrecht belegt und bezieht sich dort auf "Treu und Glauben" und das Element des Vertrauens in die Pflichterfüllung durch den Verpflichteten aufgrund einer berechtigten Erwartung. In Bezug auf die Verarbeitung personenbezogener Daten kann die Verarbeitung als unlauter verstanden werden, wenn sie das Vertrauen missbraucht. Gerechtfertigtes Vertrauen kann explizit durch Vereinbarungen oder früheres Verhalten oder implizit durch die berechtigte Erwartung der Einhaltung von Verkehrs-, Handels- oder Berufsregeln begründet werden. Vertrauensmissbrauch liegt auch vor, wenn eine Einwilligung verlangt wird, obwohl die Datenverarbeitung gesetzlich erlaubt ist. Der Grundsatz der Fairness ist z.B. "bei der Abwägung der widerstreitenden Interessen zwischen dem Verantwortlichen und der betroffenen Person gemäß Art. 6 Abs.1 UAbs. 1 lit. f, bei der Bestimmung der Freiwilligkeit der Einwilligung und des Koppelungsverbots nach Art. 7 Abs. 4 und bei der Festlegung von Verhaltensregeln nach Art. 40 Abs. 2." zu berücksichtigen, vgl. Simitis/Hornung/Spiecker gen. Döhmann, 2019, Art. 5, Rn. 47.

Ermittlung

Die Erfüllung des Transparenzgrundsatzes und Rechtmäßigkeit wird in den Kriterien zu den Informations- und Auskunftspflichten über die Datenverarbeitung (Nr. 15.1 und Nr. 15.2) und der datenschutzgerechten Systemgestaltung und den datenschutzfreundlichen Voreinstellungen (Nr. 19.1 und Nr. 19.2) ermittelt.

Grundsätzlich kann ein Evaluator zur Ermittlung und Sicherstellung der Datenschutzgrundsätze Einblick in TOMs, die Dokumentation der Datenflüsse, das Verzeichnis von Verarbeitungstätigkeiten und das Datensicherheitskonzept erhalten.

Zur Ermittlung der Einhaltung der Grundsätze der Zweckfestlegung und Zweckbindung sollte ein Evaluator eine Dokumentprüfung durchführen, darunter bspw. die Datenschutzerklärung oder Dokumentationen zu TOM, die eine logische oder physische Datentrennung sicherstellen.

Für die Einhaltung des Grundsatzes der Datenminimierung kann basierend auf der Analyse der Zweckbindung im Rahmen einer Dokumentenprüfung überprüft werden, ob alle erhobenen und verarbeiteten Daten für die Verarbeitung zwingend erforderlich sind. Hierbei prüft ein Evaluator die Prozessdokumentation des Cloud-Anbieters und die eingesetzten TOM (z.B. Berechtigungskonzepte zum Zugriff auf personenbezogene Daten). Auch müssen mittels einer Inspektion die Datenbestände, die zur Durchführung des Auftrags über die Erbringung des Cloud-Dienstes und zur Erfüllung rechtlicher Verpflichtungen gehalten werden, stichprobenartig daraufhin überprüft werden, ob diese nur Daten enthalten, die zwingend für die Zweckerreichung erforderlich sind.

Eine Befragung der Mitarbeiter und des DSB in Hinblick auf Verfahrensschritte, Prozesse und Richtlinien zur Datenminimierung kann darüber hinaus durchgeführt werden.

Unterstützend kann im Rahmen einer Entwicklungs- und Designprüfung festgestellt werden, ob während der Anwendung von Entwicklungs- oder Designmethoden bereits die Grundsätze der Datenminimierung, Zweckfestlegung und Zweckbindung einbezogen werden, sodass nur für die Verarbeitung erforderliche Daten verarbeitet werden, und bspw. entsprechende Datenfelder in Datenbanken und Benutzeroberflächen datenminimierend designed werden.

Ein Evaluator führt eine Dokumentprüfung durch, um die Einhaltung des Grundsatzes der Datenrichtigkeit festzustellen. Hierzu zählen insbesondere die Prozessdokumentation zur Prüfung der sachlichen Richtigkeit, Korrektur und Löschung unzutreffender oder unvollständiger personenbezogener Daten sowie Dokumentationen über entsprechende (technische) Verfahren (bspw. Einstellungen von Datenbanksystemen) und TOM zur Berichtigung und Löschung von personenbezogenen Daten, wobei hier auch auf die Berichtigungs- und Löschpflichten (Kriterien Nr. 15.4 und 15.4) verwiesen wird. Unterstützend kann im Rahmen einer Inspektion eine testweise Korrektur oder Löschung der Daten durchgeführt werden. Eine Befragung oder Beobachtung von Mitarbeitern in Bezug auf die Prüfung, Korrektur und Löschung unzutreffender oder unvollständiger personenbezogener Daten sollte durchgeführt werden (bspw. Bekanntheit der Verfahrensschritte und Richtlinien, klare Verteilung der Verantwortlichkeiten).

Zur Ermittlung des Grundsatzes der Speicherbegrenzung führt ein Evaluator eine Dokumentprüfung durch. Dabei prüft er bspw. Löschkonzepte (bspw. Fristen und Art der Löschung), Dokumentation von ergriffenen Maßnahmen wie Pseudonymisierungs- oder Anonymisierungsverfahren zur Umsetzung des Speicherbegrenzungsgrundsatzes, oder Protokolle über durchgeführte Löschungen oder Pseudonymisierungen. Im Rahmen eines Audits sollte eine Befragung der Mitarbeiter zur Speicherbegrenzung durchgeführt werden (bspw. Kenntnis über Speicherfristen, Richtlinien, Verfahrensschritte).

Nr. 13 – Rechtsgrundlage für die Datenverarbeitung (Art. 6 Abs. 1 UAbs. 1 lit. b, c oder f i.V.m. Abs. 2 DSGVO)

Kriterium

(1) Der Cloud-Anbieter verarbeitet personenbezogene Daten und führt Verarbeitungsvorgänge nur durch, die für die Erfüllung eines Vertrags zur Datenverarbeitung im Auftrag des Cloud-Nutzers[37] oder zur Durchführung vorvertraglicher Maßnahmen, die auf Anfrage des Cloud-Nutzers erfolgen, erforderlich sind. In Bezug auf Letzteres darf der Cloud-Anbieter nur Daten des Cloud-Nutzers verarbeiten, die es ihm ermöglichen, ein Angebot auf der Grundlage der geografischen, technischen und individuellen Bedürfnisse des Cloud-Nutzers zu erstellen, bevor er eine rechtsverbindliche Vereinbarung zur Auftragsdatenverarbeitung abschließt. Der Cloud-Anbieter dokumentiert Strukturen und Abläufen, die zu einem Vertragsschluss oder zu einem vorvertraglichen Verhältnis führen.

[37] Da der Cloud-Nutzer auch eine natürliche Person sein kann, ist es auch möglich, dass er die „betroffene Person“ (wie indirekt über Art. 4 Nr. 1 DSGVO definiert) ist.

(2) Der Cloud-Anbieter verarbeitet personenbezogene Daten und führt Verarbeitungsvorgänge nur durch, die zur Erfüllung einer rechtlichen Verpflichtung nach deutschem oder EU-Recht erforderlich sind, der er unterliegt. Der Cloud-Anbieter dokumentiert die rechtlichen Verpflichtungen, einschließlich der Bedingungen ihres Eintritts, ihres Umfangs und der Umstände ihres Wegfalls.

(3) Der Cloud-Anbieter verarbeitet personenbezogene Daten und führt Verarbeitungsvorgänge durch, die zur Wahrung seiner berechtigten Interessen oder solcher eines Dritten erforderlich sind, es sei denn, diese Interessen werden durch die Interessen oder Grundrechte und -freiheiten des Cloud-Nutzers, die den Schutz personenbezogener Daten erfordern, überwogen. Der Cloud-Anbieter dokumentiert den Prozess der Interessenabwägung, inklusive der Beteiligten, deren Interessen abgewogen werden, der konkreten Interessen, Grundrechte und Grundfreiheiten und der personenbezogenen Daten und Verarbeitungsvorgänge, den einbezogenen Abwägungskriterien und dem Ergebnis der Abwägung und, falls erforderlich, die Ausgleichs- oder zusätzlichen Maßnahmen die vorgesehen werden müssen, um die Auswirkung der Verarbeitung auf betroffene Personen zu begrenzen und auf diese Weise einen Ausgleich zwischen den involvierten Rechten und Interessen zu schaffen.

(4) Der Cloud-Anbieter prüft, bestimmt und dokumentiert die Rechtsgrundlagen für die Verarbeitungsvorgänge nach Abs. 1 bis 3.

(5) Der Cloud-Anbieter verfügt über Anweisungen an Mitarbeiter, anhand derer das Vorhandensein einer ausreichenden Rechtsgrundlage zu prüfen ist und legt entsprechende Zuständigkeiten für Prüfungen fest.

Ermittlungsmethoden

- Dokumentprüfung, insbesondere Rechtsanalyse
- Inspektion
- Prüfung

Ermittlung

Der Evaluator prüft den Abschluss von standardisierten Vereinbarungen zur Bereitstellung des Dienstes anhand eines Auszuges von Vereinbarungen aus der Datenbank (oder einem anderen Speicherort der Vereinbarungen). Auch sollte ein stichprobenartiger Abgleich des Vertragsabschlussdatums mit dem Zeitstempel der initialen Nutzerdatensatzerzeugung durchgeführt werden. Sollten keine standardisierten Vereinbarungen geschlossen worden sein, prüft ein Evaluator im Rahmen der Dokumentprüfung alle oder eine repräsentative Stichprobe von rechtsverbindlichen Vereinbarungen, die ein Cloud-Anbieter mit den Cloud-Nutzern zur Diensterbringung geschlossen hat.

Eine repräsentative Stichprobe sollte mindestens so umfassend gewählt werden, dass durch eine vergleichende Begutachtung einer Auswahl an Vereinbarungen mit hoher Wahrscheinlichkeit ausgeschlossen werden kann, dass eine weitere Vereinbarung wesentlich abweicht. Der Stichprobenumfang ist somit auch abhängig von der Gesamtanzahl an geschlossenen Vereinbarungen. Die individuellen Vereinbarungen können zu Gruppen zusammengefasst werden, wobei aus jeder Gruppe von Vereinbarungen eine ausreichende Anzahl an Vereinbarungen geprüft werden muss. Vereinbarungen können unter anderem hinsichtlich des Gegenstands, der Dauer, der Art und den Zweck der Verarbeitung in Gruppen eingeteilt werden.

Bei der Datenverarbeitung auf Grundlage des Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO prüft der Evaluator im Rahmen einer stichprobenartigen Dokumentenprüfung das Vorhandensein von geschlossenen Vereinbarungen zur Auftragsverarbeitung, Mustern hiervon oder Vermerken zu eingegangenen vorvertraglichen Verhältnissen, aufgrund derer die Datenverarbeitung durchgeführt wird. Weiterhin prüft der Evaluator stichprobenartig, ob die durch den Cloud-Anbieter verarbeiteten Daten und Verarbeitungsvorgänge zur Erfüllung eines Vertrags zur Datenverarbeitung im Auftrag des Cloud-Nutzers oder zur Durchführung vorvertraglicher Maßnahmen erforderlich sind. Die Ermittlungsmethoden zum Grundsatz der Datenminimierung aus Nr. 12 finden analog Anwendung.

Außerdem muss der Evaluator anhand einer geeigneten Dokumentation (z.B. Prozessdokumentation, Funktionsdokumentation, Protokolldateien oder Logs) prüfen, ob der Cloud-Anbieter technische oder organisatorische Vorkehrungen getroffen hat, die einen Vereinbarungsschluss vor der eigentlichen Dienstnutzung sicherstellen (bspw. in Bezug auf einen Vereinbarungs- bzw. Registrierungsprozesses mit potenziellen Cloud-Nutzern). Anhand dieser Funktionsdokumentation muss für einen Evaluator ersichtlich werden, dass ein Cloud-Dienst nur dann erbracht werden kann, wenn eine rechtsverbindliche Vereinbarung gemäß den Vorgaben des Kriterienkatalogs geschlossen wird.

Unterstützend kann ein Evaluator eine Inspektion in Form einer testweisen Durchführung eines entsprechenden Vereinbarungs- bzw. Registrierungsprozesses vornehmen, um sicherzustellen, dass die in der Dokumentation angegebenen Strukturen, Abläufe und Konzepte auch in dem Cloud-Dienst realisiert wurden. Im Rahmen der testweisen Durchführung sollte ein Evaluator auch überprüfen, ob durch Vorsatz oder Fehlverhalten das Abschließen einer Vereinbarung umgangen werden kann.

Im Rahmen einer Dokumentenprüfung mit repräsentativen Stichproben prüft der Evaluator, ob die Rechtsgrundlagen für die Verarbeitung niedergelegt sind und den betroffenen Personen kommuniziert werden. Hierfür sollte der Evaluator die Datenschutzerklärung des Cloud-Anbieters, Informationserteilungen an betroffene Personen nach Art. 13 und 14 DSGVO (s. Nr. 15.1 und 15.2), das Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 Abs. 1

DSGVO (s. Nr. 18) und interne Vermerke des Cloud-Anbieters prüfen, aus denen sich die Festlegung einer Rechtsgrundlage ergibt.

Im Rahmen einer Dokumentenprüfung prüft der Evaluator die Anweisungen, Richtlinien, Dienstanweisungen oder ähnlichen Dokumente an die Mitarbeiter des Cloud-Anbieters, in denen das Vorgehen zur Prüfung des Vorhandenseins einer Rechtsgrundlage für die Datenverarbeitung durch die Mitarbeiter niedergelegt ist, sowie die Strukturen und Zuständigkeiten für solche Prüfungen.

Bei der Datenverarbeitung auf Grundlage des Art. 6 Abs. 1 UAbs. 1 lit. c DSGVO prüft der Evaluator im Rahmen einer stichprobenartigen Dokumentenprüfung, ob die durch den Cloud-Anbieter verarbeiteten Daten und Verarbeitungsvorgänge zur Erfüllung einer rechtlichen Verpflichtung, der der Cloud-Anbieter unterliegt, erforderlich sind. Zur Prüfung der Erforderlichkeit werden die Dokumentationen des Cloud-Anbieters zu den rechtlichen Verpflichtungen, denen er unterliegt, inklusive der Darstellung der Bedingungen ihres Eintritts, ihres Umfangs und der Umstände ihres Wegfalls genutzt. Im Übrigen finden die Ermittlungsmethoden zum Grundsatz der Datenminimierung aus Nr. 12 analog Anwendung.

Bei der Datenverarbeitung auf Grundlage des Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO prüft der Evaluator im Rahmen einer stichprobenartigen Dokumentenprüfung den festgelegten Prozess zur Interessenabwägung. Stichprobenartig können zudem Dokumente über bereits erfolgte Interessenabwägungen geprüft werden, um festzustellen, dass diese korrekt durchgeführt wurden. Unterstützend kann ein Evaluator eine Prüfung und Inspektion des Prozesses der Interessenabwägung vornehmen, um sicherzustellen, dass dieser entsprechend der Prozessbeschreibung erfolgt.

Nr. 14 – Gewährleistung der Datensicherheit durch geeignete TOM nach dem Stand der Technik

Nr. 14.1 – Datensicherheitskonzept (Art. 24, 25, 32 i.V.m. Art. 5 Abs. 1 lit. f und Abs. 2 DSGVO)

Kriterium

(1) Der Cloud-Anbieter führt eine Risikoanalyse nach dem Stand der Technik in Bezug auf die Datensicherheit durch und verfügt über ein Datensicherheitskonzept entsprechend seiner Schutzklasse, das den spezifischen Risiken seiner Datenverarbeitungsvorgänge zur Durchführung des Auftrags über die Erbringung des Cloud-Dienstes und zur Erfüllung rechtlicher Verpflichtungen, die sich insbesondere durch Vernichtung, Verlust, Veränderung, unbefugte Offenlegung von und unbefugten Zugang zu personenbezogenen Daten ergeben können, angemessen ist.

(2) Der Cloud-Anbieter unterhält eine Beschreibung aller personenbezogenen Daten oder Datenkategorien, die er als Verantwortlicher zur Durchführung des Auftrags über die Erbringung des Cloud-Dienstes und zur Erfüllung rechtlicher Verpflichtungen verarbeitet.

(3) Die in Nr. 14 geforderten Angaben können außer im Datensicherheitskonzept auch in sonstigen Dokumenten getroffen werden, solange diese als rechtsverbindlich für die Auftragsverarbeitung zwischen Cloud-Anbieter und Cloud-Nutzer vereinbart worden sind. Die Anforderungen an das Datensicherheitskonzept gelten auch für diese sonstigen Dokumente.

(4) Im Datensicherheitskonzept stellt der Cloud-Anbieter dar, welche Datensicherheitsmaßnahmen er ergriffen hat, um die bestehenden Risiken abzustellen oder einzudämmen. Der Cloud-Anbieter schildert auch die Abwägungen, die er vorgenommen hat, um zu diesen Maßnahmen zu gelangen.

(5) Das Datensicherheitskonzept ist schriftlich oder in einem elektronischen Format zu dokumentieren.

(6) Das Datensicherheitskonzept ist in regelmäßigen Abständen (mindestens jährlich und nach jeder wesentlichen Veränderung) auf Aktualität und Angemessenheit zu überprüfen und bei Bedarf zu aktualisieren.

(7) Sofern der Cloud-Anbieter Auftragsverarbeiter zur Durchführung des Auftrags mit dem Cloud-Nutzer einsetzt, beschreibt das Datensicherheitskonzept welche Datenverarbeitungsvorgänge ausgelagert sind und daher den TOM des Auftragsverarbeiters unterliegen.

(8) Soweit das Datensicherheitskonzept Sicherheitsmaßnahmen des Cloud-Nutzers verlangt, sind diese dem Cloud-Nutzer in Schriftform oder in einem elektronischen Format mitzuteilen.

Ermittlungsmethoden

- Dokumentprüfung, insbesondere Rechtsanalyse
- Inspektion
- Audit

Ermittlung

Für die Prüfung eines angemessenen Datensicherheitskonzepts gelten die Ausführungen in Nr. 2.1 analog.

Nr. 14.2 – Sicherheitsbereich und Zutrittskontrolle (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 sichert Räume und Anlagen gegen Schädigung durch höhere Gewalt[38] und verwehrt Unbefugten den Zutritt zu Räumen und Datenverarbeitungsanlagen, um unbefugte Kenntnisnahmen personenbezogener Daten und Einwirkungsmöglichkeiten auf die Datenverarbeitungsanlagen auszuschließen. Die TOM müssen geeignet sein, um im Regelfall den Zutritt Unbefugter aufgrund technischer oder organisatorischer Fehler, einschließlich Bedienfehler, des Cloud-Anbieters oder fahrlässiger Handlungen Dritter auszuschließen. Der Cloud-Anbieter muss wenigstens eine Reihe von Sicherheitsanforderungen für jede Sicherheitszone festlegen, dokumentieren und umsetzen.

(2) Der Cloud-Anbieter überprüft die Erforderlichkeit der Berechtigungen für den Zutritt zu Räumen und Anlagen in regelmäßigen Abständen (mindestens jährlich oder bei wesentlichen Veränderungen) auf Aktualität und Angemessenheit und aktualisiert sie bei Bedarf.

(3) Jeder befugte Zutritt ist zu protokollieren.

Schutzklasse 2 und 3

(4) Die Kriterien von Schutzklasse 1 sind erfüllt.

(5) Zusätzlich ergreift der Cloud-Anbieter geeignete Maßnahmen, um Schädigungen nicht nur durch höhere Gewalt, sondern auch durch fahrlässige Handlungen Befugter ausschließen. Der Zutritt ist vor vorsätzlichen Handlungen Unbefugter hinreichend sicher geschützt, was Schutz gegen Zutrittsversuche durch bekannte Angriffsszenarien, Täuschung und Gewalt einschließt.

(6) Alle unbefugten Zutritte und Zutrittsversuche sind nachträglich feststellbar.

Ermittlungsmethoden

- Dokumentprüfung
- Inspektion
- Prüfung
- Audit

Ermittlung

Für den Zutrittsschutz zu Räumlichkeiten und Anlagen gelten die Ausführungen in Nr. 2.2 analog.

Nr. 14.3 – Zugangskontrolle (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 sicher, dass Unbefugte keinen Zugang zu Datenverarbeitungssystemen erhalten und auf diese einwirken können. Dies gilt auch für Sicherungskopien, soweit diese personenbezogene Daten enthalten.

(2) Der Cloud-Anbieter überprüft die Erforderlichkeit der Berechtigungen für den Zugang zu Datenverarbeitungssystemen in regelmäßigen Abständen (mindestens jährlich oder bei wesentlichen Veränderungen) auf Aktualität und Angemessenheit und aktualisiert sie bei Bedarf.

[38] Nach einer auf verschiedenen Gebieten des Unionsrechts entwickelten ständigen Rechtsprechung sind unter „höherer Gewalt“ ungewöhnliche und unvorhersehbare Ereignisse zu verstehen, auf die derjenige, der sich darauf beruft, keinen Einfluss hat und deren Folgen trotz Anwendung der gebotenen Sorgfalt nicht hätten vermieden werden können, vgl. ECLI:EU:C:2017:39, Rn. 53.

(3) Der Cloud-Anbieter schützt Zugänge von Befugten über das Internet mit einer Zwei-Faktor-Authentifizierung. Der Zugang über das Internet hat über eine Transportverschlüsselung nach dem Stand der Technik zu erfolgen.

(4) Der Cloud-Anbieter implementiert die Maßnahmen zur Zugangskontrolle derart, um im Regelfall den Zugang zu Datenverarbeitungssystemen durch Unbefugte aufgrund technischer oder organisatorischer Fehler, einschließlich Bedienfehler, des Cloud-Anbieters oder fahrlässiger Handlungen des Cloud-Nutzers oder Dritter auszuschließen.

Schutzklasse 2

(5) Die Kriterien von Schutzklasse 1 sind erfüllt.

(6) Gegen zu erwartenden vorsätzlichen unbefugten Zugang ist ein Schutz vorzusehen, der zu erwartende Zugangsversuche ausschließt. Das umfasst einen hinreichenden Schutz gegen bekannte Angriffsszenarien und stellen einen unbefugten Zugang im Regelfall nachträglich fest.

Schutzklasse 3

(7) Die Kriterien von Schutzklasse 1 und 2 sind erfüllt.

(8) Der Cloud-Anbieter muss unbefugten Zugang zu Datenverarbeitungssystemen ausschließen. Dies umfasst regelmäßige Maßnahmen zur aktiven Detektion von und Reaktion auf Angriffe. Jeder unbefugte Zugang und Zugangsversuch sind nachträglich feststellbar.

Ermittlungsmethoden

- Dokumentprüfung
- Inspektion
- Prüfung
- Audit

Ermittlung

Für die Prüfung der Zugangskontrolle gelten die Ausführungen in Nr. 2.3 analog.

Nr. 14.4 – 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 auf personenbezogene Daten zugreifen können und schließt unbefugte Einwirkungen auf personenbezogene Daten aus. Dies gilt auch für Sicherungskopien, soweit sie personenbezogene Daten enthalten.

(2) Der Cloud-Anbieter überprüft die Erforderlichkeit der Berechtigungen für den Zugriff auf personenbezogene Daten in regelmäßigen Abständen (mindestens jährlich oder bei wesentlichen Veränderungen) auf Aktualität und Angemessenheit und aktualisiert sie bei Bedarf.

(3) Zugriffe auf personenbezogene Daten sind zu kontrollieren (d.h. zu überwachen und zu bewerten) und müssen protokolliert werden.

(4) Der Cloud-Anbieter implementiert Maßnahmen, die im Regelfall den Zugriff auf personenbezogene Daten durch Unbefugte aufgrund technischer oder organisatorischer Fehler, einschließlich Bedienfehler, des Cloud-Anbieters oder fahrlässiger Handlungen des Cloud-Nutzers oder Dritter ausschließen.

(5) Der Cloud-Anbieter schützt Zugriffe von Befugten über das Internet durch eine Zwei Faktor-Authentifizierung.

Schutzklasse 2

(6) Die Kriterien von Schutzklasse 1 sind erfüllt.

(7) Zu erwartender vorsätzlicher, unbefugter Zugriff muss ausgeschlossen werden. Dies umfasst insbesondere einen angemessenen Schutz gegen bekannte Angriffsszenarien sowie Maßnahmen, mit denen ein unbefugter Zugriff in der Regel nachträglich erkannt werden kann.

Schutzklasse 3

(8) Die Kriterien von Schutzklasse 1 und 2 sind erfüllt.

(9) Unbefugter Datenzugriff muss unter Berücksichtigung der Ergebnisse der Risikoanalyse ausgeschlossen sein. Dazu gehören regelmäßig manipulationssichere technische Maßnahmen zur Verhinderung und aktiven Erkennung von Angriffen. Unbefugte Zugriffe und damit verbundene Versuche können nachträglich erkannt werden.

Ermittlungsmethoden

- Dokumentprüfung
- Inspektion
- Prüfung
- Audit

Ermittlung

Für die Prüfung der Zugriffskontrolle gelten die Ausführungen in Nr. 2.4 analog.

Nr. 14.5 – Übermittlung von Daten und Transportverschlüsselung (Art. 32 Abs. 1 lit. b und Abs. 2 i.V.m. Art. 5 Abs. 1 lit. f und Abs. 2 DSGVO)

Kriterium

Schutzklasse 1

(1) Der Cloud-Anbieter setzt bei Datenübermittlungsvorgängen eine Transportverschlüsselung nach dem Stand der Technik ein oder fordert dies durch entsprechende Konfiguration von Schnittstellen. Die eingesetzte Transportverschlüsselung gewährleistet, dass personenbezogene Daten bei der elektronischen Übermittlung nicht unbefugt gelesen werden können. Bei verschlüsselter Übermittlung sind die Schlüssel sicher aufzubewahren.

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

(3) Der Cloud-Anbieter protokolliert automatisiert die Metadaten aller Datenüberübermittlungsvorgänge, einschließlich der Empfänger, auch solche vom und an den Cloud-Nutzer oder an Subauftragsverarbeiter. Nr. 14.6 (1) gilt entsprechend.

(4) Die Kriterien gelten auch für die Übermittlungen von Daten im eigenen Netzwerk des Cloud-Anbieters und seiner Auftragsverarbeiter und zwischen diesen.

(5) Der Cloud-Anbieter schützt den Transport von Datenträgern durch TOM, so dass personenbezogene Daten während des Transports von Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Der Cloud-Anbieter führt ein Verzeichnis der Transporte.

Schutzklasse 2

(6) Die Kriterien von Schutzklasse 1 sind erfüllt.

(7) Der Cloud-Anbieter schützt personenbezogene Daten gegen vorsätzliches unbefugtes Lesen, Kopieren, Verändern oder Entfernen und schließt zu erwartende Versuche aus. Er schützt gegen bekannte Angriffsszenarien und stellt ein unbefugtes Lesen, Kopieren, Verändern oder Entfernen im Regelfall (nachträglich) fest.

Schutzklasse 3

(8) Die Kriterien von Schutzklasse 1 und 2 sind erfüllt.

(9) Der Cloud-Anbieter verhindert unbefugtes Lesen, Kopieren, Verändern oder Löschen von Daten. Er unternimmt regelmäßig Maßnahmen, um Angriffe aktiv zu erkennen und abzuwehren, und um jedes unbefugte Lesen, Kopieren, Ändern oder Löschen von Daten sowie jeden diesbezüglichen Versuch.

Ermittlungsmethoden

- Dokumentprüfung
- Prüfung
- Audit

Ermittlung

Der Evaluator kann den Schutz von Daten bei der Übertragung analog wie in Nr. 2.5 angegeben nachprüfen.

Nr. 14.6 – Nachvollziehbarkeit der Datenverarbeitung (Art. 32 Abs. 1 lit. b und Abs. 2 i.V.m. Art. 5 Abs. 1 lit. c, e, f und Abs. 2 DSGVO)

Kriterium

Schutzklasse 1

(1) Der Cloud-Anbieter protokolliert Eingaben, Veränderungen und Löschungen an Daten, die zur Durchführung des Auftrags über die Erbringung des Cloud-Dienstes und zur Erfüllung rechtlicher Verpflichtungen erforderlich sind, um eine nachträgliche Prüfbarkeit und Nachvollziehbarkeit der Datenverarbeitung sicherzustellen. Der Cloud-Anbieter beachtet die Grundsätze der Erforderlichkeit, Zweckbindung, Speicherbegrenzung und Datenminimierung. Der Cloud-Anbieter bewahrt die Protokolldaten sicher auf.

(2) Der Cloud-Anbieter kann Dateneingaben, -veränderungen oder -löschungen, die bei der bestimmungsgemäßen Nutzung des Cloud-Dienstes durch den Cloud-Nutzer wie auch bei administrativen Maßnahmen des Cloud-Anbieters erfolgen, jederzeit nachvollziehen.

(3) Der Cloud-Anbieter verhindert vorsätzliche Manipulation durch Gestaltung der Protokollierung der administrativen Aktivitäten und der Nutzer-Aktivitäten dergestalt, 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 fahrlässiger Handlungen des Cloud-Nutzers oder Dritter gewahrt bleibt.

Schutzklasse 2

(4) Die Kriterien von Schutzklasse 1 sind erfüllt.

(5) Der Cloud-Anbieter sieht gegen zu erwartende vorsätzliche Manipulationen der Protokollierungsinstanzen und gegen vorsätzlichen Zugriff auf oder Manipulationen von Protokollierungsdateien (Logs) durch Unbefugte einen Schutz vor, der zu erwartende Manipulationsversuche ausschließt. Zu diesen Schutzmaßnahmen gehören insbesondere ein hinreichender Schutz gegen bekannte Angriffsszenarien sowie Maßnahmen, durch die eine Manipulation im Regelfall (nachträglich) festgestellt werden kann.

Schutzklasse 3

(6) Die Kriterien von Schutzklasse 1 und 2 sind erfüllt.

(7) Der Cloud-Anbieter verhindert Manipulationen der Protokollinstanzen und Protokolldateien (Logs). Er unternimmt regelmäßig Maßnahmen, um Manipulationen aktiv zu erkennen und deckt jede Manipulation und, wenn möglich, jeden damit verbundenen Versuch nachträglich auf.

Ermittlungsmethoden

- Dokumentprüfung, insbesondere Rechtsanalyse
- Inspektion
- Prüfung
- Audit

Ermittlung

Die Nachvollziehbarkeit der Datenverarbeitung kann der Evaluator analog wie in Nr. 2.6 angegeben prüfen.

Nr. 14.7 – Verschlüsselung gespeicherter Daten (Art. 32 Abs. 1 lit. a DSGVO)

Kriterium

Schutzklasse 1,2 und 3

(1) Der Cloud-Anbieter stellt sicher, dass Anmeldedaten zur Nutzung des Cloud-Dienstes verschlüsselt gespeichert werden.

(2) Personenbezogene Daten, die zur Durchführung des Auftrags über die Erbringung des Cloud-Dienstes und zur Erfüllung rechtlicher Verpflichtungen gespeichert werden müssen, werden verschlüsselt gespeichert.

(3) Der Cloud-Anbieter verfolgt laufend die technische Entwicklung im Bereich der Verschlüsselung. Die Maßnahmen des Cloud-Anbieters, insbesondere die sichere Schlüsselverwaltung, entsprechen dem Stand der Technik[39] (wie in den Umsetzungshinweisen beschrieben).

(4) Eingesetzte Verschlüsselungsverfahren sind durch andere Verschlüsselungsverfahren zu ersetzen, wenn sie nicht mehr den aktuellen technischen Empfehlungen (best practices) entsprechen.

(5) Unbefugter Zugang zu Verschlüsselungsschlüsseln ist durch geeignete Maßnahmen zu verhindern.

Ermittlungsmethoden

- Dokumentprüfung
- Inspektion
- Prüfung
- Audit

Ermittlung

Für die Prüfung der verschlüsselten Speicherung gelten die Ausführungen unter Nr. 2.9 analog.

Nr. 14.8 – Getrennte Verarbeitung
(Art. 5 Abs. 1 lit. b i.V.m. Art. 24, 25, 32 Abs. 1 lit. b und Abs. 2 DSGVO)

Kriterium

Schutzklasse 1

(1) Der Cloud-Anbieter verarbeitet personenbezogene Daten, die zur Durchführung des Auftrags über die Erbringung des Cloud-Dienstes und zur Erfüllung rechtlicher Pflichten verarbeitet werden, logisch oder physisch getrennt nach den jeweiligen Verarbeitungszwecken.

(2) Der Cloud-Anbieter verhindert vorsätzliche Verletzungen bezüglich der Datentrennung bei technischen oder organisatorischen Fehlern, einschließlich Bedienfehlern, des Cloud-Anbieters oder seiner Mitarbeiter.

Schutzklasse 2

(3) Die Kriterien von Schutzklasse 1 sind erfüllt.

(4) Der Cloud-Anbieter schließt zu erwartende vorsätzliche Verstöße aus. Dies umfasst Schutz gegen bekannte Angriffsszenarien in Bezug auf das Trennungsprinzip. Zu den dafür erforderlichen TOM gehört im Rahmen der Datenspeicherung die Verschlüsselung mit individuellen Schlüsseln. Er stellt vorsätzliche Verstöße gegen das Trennungsgebot im Regelfall (nachträglich) fest.

Schutzklasse 3

(5) Die Kriterien von Schutzklasse 1 und 2 sind erfüllt.

(6) Der Cloud-Anbieter schließt Verletzungen der Datentrennung aus. Der Cloud-Anbieter erkennt vorsätzliche Verletzungen der getrennten Verarbeitung.

Ermittlungsmethoden

- Dokumentprüfung
- Inspektion
- Prüfung
- Audit

Ermittlung

Die Datentrennung und deren Angemessenheit kann der Evaluator analog wie in Nr. 2.10 angegeben prüfen.

[39] Der Stand der Technik umfasst das, was derzeit als beste Praktiken, Technologien, Methoden und Strategien zum Schutz von Informationssystemen allgemein anerkannt ist. Der Stand der Technik bedeutet nicht notwendigerweise die technologisch fortschrittlichste Lösung, sondern umfasst robuste Technologien und Prozesse sowie qualifiziertes Personal, um wirksam gegen die sich fortentwickelnden Datenschutzbedrohungen zu schützen.

Nr. 15 – Wahrung von Betroffenenrechten

Erläuterungen Ermittlung

Die Kriterien unter Nr. 15 als Verantwortlicher decken sich (in Teilen) mit den Kriterien zu Nr. 6 als Auftragsverarbeiter. Kann ein Cloud-Anbieter dem Evaluator nachweisen, dass die Wahrung von Betroffenenrechten bei der Durchführung des Auftrags mit dem Cloud-Nutzer durch die gleichen TOM wie zur Wahrung von Betroffenenrechten zur Durchführung der Auftragsdatenverarbeitung eingesetzt werden, so kann die Überprüfung der Kriterien unter Nr. 15 und Nr. 6 gemeinsam durchgeführt werden. Spezifische Anforderungen, die sich aus der Rolle als Verantwortlicher gemäß den folgenden Kriterien ergeben, sind dabei zu berücksichtigen (insb. Nr. 15.1).

Nr. 15.1 – Informationspflicht bei Direkterhebung (Art. 13 i.V.m. Art. 12 Abs. 1 und Art. 5 Abs. 1 lit. a DSGVO)

Kriterium

Der Cloud-Anbieter stellt durch TOM sicher, dass die betroffene Person zum Zeitpunkt der Erhebung ihrer personenbezogenen Daten zur Durchführung des Auftrags über die Erbringung des Cloud-Dienstes und zur Erfüllung rechtlicher Verpflichtungen über die Umstände der Verarbeitung und über ihre Betroffenenrechte verständlich und in klarer und einfacher Sprache informiert wird. Die Information an die betroffene Person umfasst alle in Art. 13 Abs. 1 und 2 DSGVO geforderten Angaben.

Ermittlungsmethoden

- Dokumentprüfung
- Inspektion

Ermittlung

Der Evaluator prüft das Muster der Datenschutzerklärung mit den Informationen nach Art. 13 Abs. 1 und 2 DSGVO, das der Cloud-Nutzer bei Vertragsschluss über die Erbringung des Cloud-Dienstes erhält. Findet der Vertragsschluss online statt, kann im Rahmen eines (Test-)Vertragsabschlusses nachgeprüft werden, ob der Cloud-Anbieter alle Informationen nach Art. 13 Abs. 1 und 2 DSGVO bereitstellt. Zur Prüfung der Informationspflicht gegenüber anderen betroffenen Personen wie z.B. den Mitarbeitern des Cloud-Nutzers prüft der Evaluator ebenfalls das Muster der Datenschutzerklärung, dass der Cloud-Anbieter dem Mitarbeiter z.B. über E-Mail bei Erhebung der Daten übermittelt.

Nr. 15.2 – Informationspflicht bei Dritterhebung (Art. 14 i.V.m. Art. 12 Abs. 1 und Art. 5 Abs. 1 lit. a DSGVO)

Kriterium

Sofern die personenbezogenen Daten der betroffenen Person zur Durchführung des Auftrags über die Erbringung des Cloud-Dienstes und zur Erfüllung rechtlicher Verpflichtungen nicht direkt bei der betroffenen Person erhoben werden (Dritterhebung), stellt der Cloud-Anbieter durch TOM sicher, dass die betroffene Person innerhalb einer angemessenen Frist über die Umstände der Verarbeitung und über ihre Betroffenenrechte verständlich und in klarer und einfacher Sprache informiert wird, sofern die Informationserteilung nicht unmöglich ist oder einen unverhältnismäßigen Aufwand erfordert. Die Information an die betroffene Person umfassen alle in Art. 14 Abs. 1 und 2 DSGVO geforderten Angaben.

Ermittlungsmethoden

- Dokumentprüfung

Ermittlung

Der Evaluator prüft das Muster der Datenschutzerklärung mit den Informationen nach Art. 14 Abs. 1 und 2 DSGVO, dass der Cloud-Anbieter der betroffenen Person zur Verfügung stellt. Darüber hinaus prüft er Dokumentationen zum Meldeverfahren, bspw. Verfahrensschritte, Meldewege oder Protokolle über durchgeführte Meldungen.

Nr. 15.3 – Auskunftserteilung (Art. 15 i.V.m. Art. 5 Abs. 1 lit. a 3. Alt. DSGVO)

Kriterium

Der Cloud-Anbieter stellt durch TOM sicher, dass er der betroffenen Person auf Antrag Auskunft über die Datenverarbeitung erteilt, die er als Verantwortlicher über sie zur Durchführung des Auftrags über die Erbringung des Cloud-Dienstes und zur Erfüllung rechtlicher Verpflichtungen durchführt. Er stellt der betroffenen Person eine Kopie dieser Daten zur Verfügung.

Ermittlungsmethoden

- Dokumentprüfung
- Inspektion
- Audit

Ermittlung

Der Evaluator prüft Dokumentationen über Maßnahmen zur Auskunftserteilung gegenüber einem Cloud-Nutzer. Insb. sollte der Evaluator Einsicht in die Dokumentation der relevanten Mechanismen und Meldewege, Dienstbeschreibungen erhalten. Ein Evaluator sollte exemplarische Datensätze und Protokolle zu getätigten Weisungen und darauffolgenden Auskünften sichten.

Im Rahmen einer Inspektion kann eine repräsentative Probeauskunft durchgeführt werden, um zu prüfen, ob eine Auskunftserteilung und Bereitstellung der Daten möglich ist (bspw. durch eine technische Funktion innerhalb des Cloud-Dienstes oder durch manuelle Anfragen beim Cloud-Dienst-Support). Im Rahmen eines Audits kann auch anhand von Befragungen (z.B. zur Kenntnis über Verfahrensschritte etc.) und Beobachtungen geprüft werden, ob bei einem Antrag Auskunft erteilt werden kann.

Nr. 15.4 – Berichtigung und Vervollständigung (Art. 16 i.V.m. Art. 5 Abs. 1 lit. d DSGVO)

Kriterium

Der Cloud-Anbieter stellt durch TOM sicher, dass er der natürlichen Person die Möglichkeit einräumt, ihre in Zusammenhang mit der Durchführung des Auftrags über die Erbringung des Cloud-Dienstes stehenden unvollständigen oder unrichtigen personenbezogenen Daten selbst zu korrigieren oder zu löschen. Alternativ führt der Cloud-Anbieter die (berechtigte) Korrektur oder Löschung durch.

Ermittlungsmethoden

- Dokumentprüfung
- Inspektion
- Audit

Ermittlung

Der Evaluator prüft Dokumentationen über Maßnahmen zur Berichtigung und Vervollständigung von Daten (z.B. Dokumentation der relevanten Mechanismen und Meldewege, Dienstbeschreibungen). Ein Evaluator sollte exemplarische Datensätze und Protokolle zu getätigten Weisungen und darauffolgende Berichtigungen oder Vervollständigungen sichten.

Im Rahmen einer Inspektion kann eine repräsentative Probeberichtigung und -vervollständigung durchgeführt werden, um zu prüfen, ob eine Berichtigung und Vervollständigung von Daten möglich ist (bspw. durch eine technische Funktion innerhalb des Cloud-Dienstes oder durch manuelle Anfragen beim Cloud-Dienst-Support). Im Rahmen eines Audits kann auch anhand von Befragungen (z.B. zur Kenntnis über Verfahrensschritte etc.) und Beobachtungen geprüft werden, ob eine Berichtigung oder Vervollständigung durchgeführt werden kann.

Nr. 15.5 – Löschung (Art. 17 Abs. 1 DSGVO)

Kriterium

(1) Der Cloud-Anbieter stellt durch TOM sicher, dass er personenbezogene Daten, die er zur Erfüllung des Auftrags über die Erbringung des Cloud-Dienstes verarbeitet, auf Antrag der betroffenen Person hin und von sich aus unverzüglich löscht, wenn die Voraussetzungen von Art. 17 Abs. 1 lit. a, d oder e DSGVO vorliegen. Die Löschung hat irreversibel zu erfolgen, sodass keine Informationen über die betroffene Person gewonnen werden können. Der Cloud-Anbieter stellt sicher, dass die Löschung durch die Nutzung von Maßnahmen nach dem Stand der Technik unwiderruflich ist.

(2) Der Cloud-Anbieter stellt sicher, dass die Löschung von personenbezogenen Daten, die er zur Erfüllung des Auftrags über die Erbringung des Cloud-Dienstes verarbeitet werden, nicht nur im aktiven Datenbestand vorgenommen wird, sondern auch in Kopien und Datensicherungen.

(3) Der Cloud-Anbieter hat sicherzustellen, dass nach einer Wiederherstellung von personenbezogenen Daten, die bereits im aktiven Datenbestand, aber noch nicht in der Datensicherung gelöscht waren, eine erneute Löschung der betroffenen Daten erfolgt.

Ermittlungsmethoden

- Dokumentprüfung
- Inspektion
- Prüfung
- Audit

Ermittlung

Der Evaluator prüft Dokumentationen über Maßnahmen zur Löschung von Daten (z.B. Dokumentation der relevanten Mechanismen und Meldewege, Löschkonzepte, Voraussetzungen und Fristen für Löschung, Dienstbeschreibungen). Auch kann ein Evaluator die (automatisierte) Benachrichtigung über tatsächliche Löschungen der für die Diensterbringung nicht mehr benötigten personenbezogenen Daten prüfen.

Im Rahmen einer Inspektion kann eine repräsentative Probelöschung durchgeführt werden, um zu prüfen, ob eine (vollständige) Löschung von Daten möglich ist (bspw. durch eine technische Funktion innerhalb des Cloud-Dienstes oder durch manuelle Anfragen beim Cloud-Dienst-Support). Im Rahmen eines Audits kann auch anhand von Befragungen (z.B. zur Kenntnis über Verfahrensschritte etc.) und Beobachtungen geprüft werden, ob eine Löschung durchgeführt werden kann.

Unterstützend können Sicherheitstests durchgeführt werden um zu prüfen, dass Daten hinreichend sicher gelöscht wurden.

Die Möglichkeiten zur Ermittlung unter Nr. 6.4 sind anwendbar.

Nr. 15.6 – Einschränkung der Verarbeitung (Art. 18 Abs. 1 und 3 DSGVO)

Kriterium

(1) Der Cloud-Anbieter stellt durch TOM sicher, dass er die Verarbeitung von personenbezogenen Daten, die er durchführt, um den Auftrag mit dem Cloud-Nutzer über die Erbringung des Cloud-Dienstes zu erbringen oder eine rechtliche Verpflichtung zu erfüllen, auf Antrag der betroffenen Person einschränken kann.

(2) Der Cloud-Anbieter stellt durch TOM sicher, dass er die betroffene Person informiert, bevor er eine Einschränkung aufhebt.

Ermittlungsmethoden

- Dokumentprüfung
- Inspektion
- Audit

Ermittlung

Der Evaluator prüft Dokumentationen über Maßnahmen zur Einschränkung der Verarbeitung von Daten (z.B. Dokumentation der relevanten Mechanismen und Meldewege, Dienstbeschreibungen, Maßnahmen zur Information des Cloud-Nutzers). Ein Evaluator sollte exemplarische Datensätze und Protokolle zu getätigten Weisungen und darauffolgender Einschränkung sichten. Auch können Nachrichten oder Protokolle über die Aufhebung von Einschränkungen an Cloud-Nutzer geprüft werden.

Im Rahmen einer Inspektion kann eine repräsentative Einschränkung durchgeführt werden, um zu prüfen, ob eine Einschränkung von der Datenverarbeitung und Aufhebung dieser (inkl. Mitteilung an den Cloud-Nutzern) möglich ist (bspw. durch eine technische Funktion innerhalb des Cloud-Dienstes oder durch manuelle Anfragen beim Cloud-Dienst-Support). Im Rahmen eines Audits kann auch anhand von Befragungen (z.B. zur Kenntnis über Verfahrensschritte etc.) und Beobachtungen geprüft werden, ob eine Einschränkung oder Information des Cloud-Nutzers über eine Aufhebung der Einschränkung durchgeführt werden kann.

Nr. 15.7 – Mitteilungspflicht bei Berichtung, Löschung oder Einschränkung der Verarbeitung (Art. 19 i.V.m. Art. 5 Abs. 1 lit. a 3. Alt. DSGVO)

Kriterium

Soweit der Cloud-Anbieter Empfängern personenbezogene Daten zur Durchführung des Auftrags mit dem Cloud-Nutzer über die Erbringung des Cloud-Dienstes oder aufgrund einer rechtlichen Verpflichtung offengelegt hat, stellt er durch TOM sicher, dass er diesen Empfängern, jede Berichtigung, Löschung oder Einschränkung der Verarbeitung mitteilt und die betroffene Person auf Verlangen über die Empfänger unterrichtet.

Ermittlungsmethoden

- Dokumentprüfung
- Inspektion
- Audit

Ermittlung

Der Evaluator prüft Dokumentationen über Maßnahmen zur Mitteilung (z.B. Dokumentation der relevanten Mechanismen und Meldewege, Dienstbeschreibungen). Ein Evaluator sollte exemplarische Datensätze und Protokolle zu getätigten Weisungen und darauffolgender Mitteilung sichten. Auch kann ein Evaluator prüfen, ob Cloud-Nutzer bereits eine Unterrichtung der Empfänger verlangt haben, und falls ja, wie ein Cloud-Anbieter dieses Verlangen bearbeitet hat.

Im Rahmen einer Inspektion können testweise Einschränkungen (inkl. Mitteilung an die betroffene Person) und die Aufhebung dieser durchgeführt werden. Die Einschränkung kann bspw. durch eine technische Funktion innerhalb des Cloud-Dienstes oder durch manuelle Anfragen beim Cloud-Dienst-Support erfolgen. Im Rahmen eines Audits kann auch anhand von Befragungen (z.B. zur Kenntnis über Verfahrensschritte etc.) und Beobachtungen nachgewiesen werden, wie Einschränkungen und ihre Aufhebungen durchgeführt werden und wie die betroffene Person benachrichtigt wird.

Nr. 15.8 – Generelle Informationspflicht, Informationspflicht bei Untätigkeit oder verzögerter Antragsbearbeitung (Art. 12 Abs. 3 und 4, Art. 15 bis 19 DSGVO)

Kriterium

(1) Der Cloud-Anbieter stellt durch TOM sicher, dass er die betroffene Person über die auf Antrag gemäß den Art. 15 bis 19 DSGVO ergriffenen Maßnahmen in Bezug auf die Datenverarbeitung, die er als Verantwortlicher über sie zur Durchführung des Auftrags über die Erbringung des Cloud-Dienstes und zur Erfüllung rechtlicher Verpflichtungen durchführt, unverzüglich, spätestens innerhalb eines Monats nach Antragseingang, informiert.

(2) Der Cloud-Anbieter stellt durch TOM sicher, dass er die betroffene Person informiert, falls er ihren Antrag nach Art. 15 bis 19 DSGVO in Bezug auf die Datenverarbeitung, die er als Verantwortlicher über sie zur Durchführung des Auftrags über die Erbringung des Cloud-Dienstes und zur Erfüllung rechtlicher Verpflichtungen durchführt, nicht unverzüglich, spätestens innerhalb eines Monats beantwortet. Die Information bezieht sich auf die Fristverlängerung und die Gründe hierfür.

(3) Der Cloud-Anbieter stellt durch TOM sicher, dass er die betroffene Person, spätestens innerhalb eines Monats darüber informiert, falls er keine Maßnahmen ergreift, um ihren Antrag nach Art. 15 bis 19 DSGVO in Bezug auf die Datenverarbeitung, die er als Verantwortlicher über sie zur Durchführung des Auftrags über die Erbringung des Cloud-Dienstes und zur Erfüllung rechtlicher Verpflichtungen durchführt, zu beantworten. Die Information der betroffenen Person bezieht sich auf die Gründe der Untätigkeit und die Möglichkeit bei der Aufsichtsbehörde Beschwerde oder einen gerichtlichen Rechtsbehelf einzulegen.

Ermittlungsmethoden

- Dokumentprüfung
- Inspektion
- Audit

Ermittlung

Der Evaluator prüft Dokumente zu Maßnahmen, die ein Cloud-Anbieter ergriffen hat, um einer betroffenen Person die erforderlichen Informationen zu erteilen. Anhand von Prozessdokumentationen und Protokollen können die durchgeführten Informationserteilungen an die betroffenen Personen überprüft werden, auch auf Vollständigkeit der erteilten Informationen und ihre rechtzeitige Erteilung.

Im Rahmen einer Inspektion kann der Evaluator eine Probeinformationserteilung durchführen, um zu prüfen, dass diese möglich ist und alle erforderlichen Informationen liefert.

Im Rahmen eines Audits kann auch eine Befragung relevanter Mitarbeiter (z.B. zur Kenntnis des festgelegten Prozesses zur Beantwortung von Anträgen von betroffenen Personen oder der Gründe, Anträgen von betroffenen Personen nicht zu entsprechen) durchgeführt werden.

Nr. 16 – Meldung von Datenschutzverletzungen (Art. 33 Abs. 1, 3 bis 5 DSGVO)

Kriterium

(1) Der Cloud-Anbieter verfügt über einen Prozess zur Meldung von Datenschutzverletzungen aus der Verarbeitung von Daten, die zur Durchführung des Auftrags über die Erbringung des Cloud-Dienstes und zur Erfüllung rechtlicher Verpflichtungen vorgenommen werden, inklusive der Festlegung von Verfahrensschritten, Fristen und Maßnahmen zur Identifikation, Analyse und Bewertung der Datenschutzverletzung und ihrer Meldung, der Verantwortlichkeiten und der Sensibilisierung der beteiligten Mitarbeiter.

(2) Der Cloud-Anbieter meldet der Aufsichtsbehörde Datenschutzverletzungen[40] aus der Verarbeitung von Daten, die zur Durchführung des Auftrags über die Erbringung des Cloud-Dienstes und zur Erfüllung rechtlicher Verpflichtungen vorgenommen werden, unverzüglich nach Bekanntwerden, sofern sie voraussichtlich zu einem Risiko für die Rechte und Freiheiten der betroffenen Personen führen.

(3) Bei der Bewertung der Risiken für die Rechte und Freiheiten des Cloud-Nutzers, muss der Cloud-Anbieter den Typus der Sicherheitsverletzung, die Art, die Sensibilität und das Volumen der personenbezogenen Daten, die leichte Identifizierbarkeit der Personen, die Schwere der Folgen für die Personen, die besonderen Merkmale des Cloud-Nutzers, die besonderen Merkmale des Cloud-Anbieters und die Zahl der betroffenen Personen berücksichtigen.

(4) Der Cloud-Anbieter verfügt über einen Prozess und Maßnahmen zur Identifikation, Analyse und Bewertung des Risikos für die Rechte und Freiheiten der betroffenen Personen.

(5) Der Cloud-Anbieter dokumentiert die Datenschutzverletzungen samt aller mit ihnen in Zusammenhang stehenden Fakten, Auswirkungen und ergriffenen Maßnahmen.

(6) Die Meldung an die zuständige Aufsichtsbehörde enthält mindestens die Vorgaben aus Art. 33 Abs. 3 lit. a bis d DSGVO.

(7) Der Cloud-Anbieter bestimmt, welche Faktoren erfüllt sein müssen, damit von einem voraussichtlichen Risiko für die Rechte und Freiheiten von betroffenen Personenausgegangen werden muss und wer für die Meldung zuständig ist. Die zuständigen Mitarbeiter sind ausreichend geschult, um Verstöße beurteilen zu können.

Ermittlungsmethoden

- Dokumentprüfung
- Audit

Ermittlung

Ein Evaluator prüft das Datensicherheitskonzept und darin beschriebene TOMs zur Meldung von Datenschutzverletzungen. Er kann zudem weitere Dokumentation prüfen, darunter bspw. Prozessdokumentation mit den Verfahrensschritten und Fristen zur Meldung der Datenschutzverletzung, Verfahrensverzeichnisse, Verfahrensanweisungen, Richtlinien, Muster und Vorlagen zur Meldung von Datenschutzverletzungen, Entscheidungsregeln zur Beurteilung von Datenschutzverletzungen, Verfahren zur Risikobeurteilung und Faktoren die bei der Risikoanalyse einbezogen werden, Meldewege und Verantwortlichkeiten / Zuständigkeiten.

Im Rahmen einer Dokumentenprüfung können auch bereits getätigte Meldungen von Datenschutzverletzungen an die Aufsichtsbehörde auf Vollständigkeit nach Art. 33 Abs. 3 DSGVO geprüft werden, sofern solche vorhanden sind. Bei gemeldeten Datenschutzverletzungen sollten insbesondere auch die Dokumentationen der TOM zur Behebung der Datenschutzverletzung hinsichtlich ihrer Geeignetheit und Schutzwirkung zur Behebung der Datenschutzverletzung oder zur Abmilderung der nachteiligen Auswirkungen geprüft werden, sowie ob die 72 Stunden-Frist eingehalten wurde und wenn nicht, wie die Fristverlängerung begründet wurde.

Die Implementierung dieser Konzepte kann durch eine Befragung von Mitarbeitern oder Beobachtung einer Probemeldung geprüft werden. Im Rahmen einer Vor-Ort-Auditierung sollte geprüft werden, ob ausreichend Ressourcen vorliegen, um eine rasche Bearbeitung von Meldungen sicher zu stellen.

[40] Wenn möglich, spätestens 72 Stunden, nach Kenntniserlangung.

Auch sollte ein Evaluator Unterlagen zur Schulung zuständiger Mitarbeiter prüfen (bspw. Zeugnisse, Nachweise von Workshops) und eine Befragung dieser (bspw. in Hinblick auf die Bekanntheit von Richtlinien und Verfahrensschritten) im Rahmen eines Audits durchführen. Auch kann der Evaluator das Organigramm bzw. einer Übersicht zur Personalsituation in verantwortlichen Bereichen mit entsprechender dokumentierter Qualifikation des Personals prüfen. Dabei muss der Evaluator auch durch Befragungen prüfen, ob Verantwortlichkeiten klar kommuniziert und geregelt sind (bspw. wer ist verantwortlich über die Mitteilung an die Aufsichtsbehörde zu entscheiden und diese vorzunehmen?).

Nr. 17 – Benachrichtigung der betroffenen Person bei Datenschutzverletzungen (Art. 34 Abs. 1 bis 3 DSGVO)

Kriterium

(1) Der Cloud-Anbieter unterrichtet die betroffene Person über Datenschutzverletzungen aus der Verarbeitung von Daten zur Durchführung des Auftrags über die Erbringung des Cloud-Dienstes und zur Erfüllung rechtlicher Verpflichtungen unverzüglich, wenn die Datenschutzverletzung voraussichtlich ein hohes Risiko für ihre Rechte und Freiheiten hat.

(2) Die Benachrichtigung enthält mindestens die Informationen nach Art. 33 Abs. 3 lit. b, c und d DSGVO und erfolgt in klarer und einfacher Sprache.

(3) Der Cloud-Anbieter verfügt über ein Verfahren zur Identifikation, Analyse und Bewertung von Datenschutzverletzungen aus der Verarbeitung von Daten zur Durchführung des Auftrags über die Erbringung des Cloud-Dienstes und zur Erfüllung rechtlicher Verpflichtungen, anhand dessen bestimmt wird, wann, von einem voraussichtlich hohen Risiko für die Rechte und Freiheiten von betroffenen Personen ausgegangen werden muss, welche Fristen einzuhalten sind und wer für die Benachrichtigung zuständig ist. Die zuständigen Mitarbeiter sind ausreichend geschult, um Verstöße beurteilen zu können.

(4) Die Benachrichtigung nach Abs. 1 und 2 darf unter Einhaltung der Voraussetzungen des Art. 34 Abs. 3 DSGVO unterbleiben.

(5) Der Cloud-Anbieter dokumentiert die Benachrichtigungen von betroffenen Personen über Datenschutzverletzungen aus der Verarbeitung von Daten zur Durchführung des Auftrags über die Erbringung des Cloud-Dienstes und zur Erfüllung rechtlicher Verpflichtungen sowie die Umstände, Gründe und Maßnahmen, wenn die Benachrichtigung der betroffenen Personen gemäß Abs. 4 unterbleibt.

Ermittlungsmethoden

- Dokumentprüfung
- Audit
- Inspektion

Ermittlung

Ein Evaluator prüft das Datensicherheitskonzept und die darin beschriebenen TOM zur Meldung von Datenschutzverletzungen. Er kann zudem weitere Dokumentation prüfen, darunter bspw. die Prozessdokumentation mit den Verfahrensschritten und Fristen zur Benachrichtigung der betroffenen Personen über Datenschutzverletzungen, Verfahrensverzeichnisse, Verfahrensanweisungen, Richtlinien, Muster und Vorlagen zur Benachrichtigung über Datenschutzverletzungen, Entscheidungsregeln zur Beurteilung von Datenschutzverletzungen, Verfahren zur Risikobeurteilung und Faktoren die bei der Risikoanalyse einzubeziehen sind, sowie Meldewege und Verantwortlichkeiten / Zuständigkeiten.

Im Rahmen einer Dokumentenprüfung können auch bereits erfolgte Benachrichtigungen über Datenschutzverletzungen an betroffene Personen auf Vollständigkeit des Mindestinhalts nach Art. 33 Abs. 3 lit. b, c und d DSGVO und Verständlichkeit für die betroffenen Personen geprüft werden, sofern solche vorhanden sind.

Sofern der Cloud-Anbieter in der Vergangenheit von Benachrichtigungen betroffener Personen über Datenschutzverletzungen abgesehen hat, prüft der Cloud-Anbieter das Vorliegen der Voraussetzungen nach Art. 34 Abs. 3 DSGVO. Im Rahmen einer Dokumentenprüfung (z.B. der Dokumentation im Datensicherheitskonzepts) muss der Evaluator prüfen, welche TOM der Cloud-Anbieter ergriffen hat und ob diese geeignet sind, damit wahrscheinlich keine hohen Risiken für die Rechte und Freiheiten der betroffenen Personen in der Zukunft mehr bestehen. Aus der Dokumentation sollte ebenfalls hervorgehen, welche Risiken durch die Maßnahmen adressiert werden. Im Rahmen einer Inspektion können technische Maßnahmen vom Evaluator geprüft werden. Bei Art. 34 Abs. 3 lit. c DSGVO prüft der Evaluator im Rahmen einer Dokumentenprüfung die Dokumentation der erfolgten öffentlichen Bekanntmachung, z.B. in einer Tageszeitung, die anstelle einer individuellen Benachrichtigung der betroffenen Personen erfolgt ist und die Darlegung des unverhältnismäßigen Aufwands der individuellen Benachrichtigung.

Ob das festgelegte Verfahren zur Identifikation, Analyse und Bewertung von Datenschutzverletzungen beim Cloud-Anbieter gelebt wird, kann auch durch eine Befragung von Mitarbeitern (bspw. im Hinblick auf die Bekanntheit von

Richtlinien und Verfahrensschritten) durchgeführt werden. Dabei muss der Evaluator auch durch Befragungen prüfen, ob Verantwortlichkeiten klar kommuniziert und geregelt sind (bspw. wer ist verantwortlich über die Benachrichtigung der betroffenen Personen zu entscheiden und diese vorzunehmen?). Es kann auch eine Beobachtung einer Probebenachrichtigung durchgeführt werden.

Die Kompetenz der Mitarbeiter sollte durch eine Prüfung der Dokumentation von Fähigkeiten (bspw. Zeugnissen) oder erfolgter Schulungen und durch Mitarbeiterbefragungen nachgewiesen werden. Auch kann der Evaluator das Organigramm bzw. eine Übersicht zur Personalsituation in verantwortlichen Bereichen mit entsprechender dokumentierter Qualifikation des Personals prüfen.

Nr. 18 – Führen eines Verarbeitungsverzeichnisses (Art. 30 Abs. 1, 3 bis 5 DSGVO)

Kriterium

(1) Ist der Cloud-Anbieter zur Führung eines Verarbeitungsverzeichnisses verpflichtet, bezieht sich dieses auf die Verarbeitungstätigkeiten, die er durchführt, um den Auftrag über die Erbringung des Cloud-Dienstes zu erfüllen und auf Verarbeitungstätigkeiten zur Erfüllung rechtlicher Verpflichtungen. Das Verzeichnis enthält die in Art. 30 Abs. 1 lit. a bis g DSGVO aufgelisteten Inhalte.

(2) Der Cloud-Anbieter verfügt über Prozesse zur Aktualisierung des Verarbeitungsverzeichnisses, wenn Verarbeitungstätigkeiten eingeführt werden oder wegfallen, oder sich die Angaben nach Art. 30 Abs. 1 lit. a bis g DSGVO bei aufgeführten Verarbeitungstätigkeiten ändern.

(3) Zum Zweck der Aktualisierung des Verarbeitungsverzeichnisses verfügt der Cloud-Anbieter über Prozesse zur Zusammenarbeit zwischen den an den Verarbeitungstätigkeiten beteiligten Fachabteilungen, seinem Vertreter sowie ggf. dem DSB und regelt hierfür die internen Zuständigkeiten.

(4) Das Verarbeitungsverzeichnis ist schriftlich oder in einem elektronischen Format zu führen und die Aufbewahrungs- oder Speicherorte sind bekannt.

(5) Das Verarbeitungsverzeichnis ist der Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen. Der Cloud-Anbieter verfügt über Prozesse zur Entgegennahme, Bearbeitung und Beantwortung von Anfragen von Aufsichtsbehörden und regelt hierfür die internen Zuständigkeiten.

(6) Ist der Cloud-Anbieter zur Benennung eines Vertreters und zur Führung eines Verarbeitungsverzeichnisses verpflichtet, stellt er sicher, dass auch der Vertreter ein Verarbeitungsverzeichnis führt und die Kriterien nach Abs. 1 bis 5 einhält.

Ermittlungsmethoden

- Dokumentprüfung
- Audit

Ermittlung

Das Führen eines Verarbeitungsverzeichnisses kann der Evaluator analog wie in Nr. 8.3 angegeben prüfen.

Nr. 19 – Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

Nr. 19.1 – Datenschutz durch Systemgestaltung (Art. 25 Abs. 1 i.V.m. Art. 5 Abs. 1 und 2 DSGVO)

Kriterium

Der Cloud-Anbieter führte eine Risikoanalyse durch und stellt durch TOM im Rahmen der Dienstgestaltung sicher, dass im Cloud-Dienst nur personenbezogene Daten verarbeitet werden, die zur Erfüllung des Auftrags über die Erbringung des Cloud-Dienstes erforderlich sind und dass die übrigen Grundsätze des Art. 5 DSGVO im Cloud-Dienst umgesetzt werden.

Ermittlungsmethoden

- Dokumentprüfung
- Inspektion
- Prüfung
- Audit
- Entwicklungs- und Designprüfung

Ermittlung

Für die Prüfung auf Datenschutz durch Systemgestaltung gelten die Ausführung in Nr. 9.1 analog.

Nr. 19.2 – Datenschutz durch datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 i.V.m. Art. 5 Abs. 1 und 2 DSGVO)

Kriterium

(1) Der Cloud-Anbieter stellt durch Voreinstellungen sicher, dass er bei der Inbetriebnahme und Nutzung des Cloud-Dienstes nur personenbezogene Daten verarbeitet, die erforderlich sind, um den Cloud-Dienst erbringen zu können im Hinblick auf die Menge der erhobenen Daten, den Umfang ihrer Verarbeitung und die Dauer ihrer Speicherung sowie dass der Zugang zu den personenbezogenen Daten auf das erforderliche Maß[41] beschränkt wird.

(2) Der Cloud-Anbieter stellt durch Voreinstellungen sicher, dass personenbezogene Daten nicht ohne Eingreifen der betroffenen Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden und dass keine unangemessenen Risiken[42] für die betroffene Person durch das Zugänglichmachen in einem zu großen Umfang[43] zu den verfügbaren personenbezogenen Daten entstehen.

Ermittlungsmethoden

- Dokumentprüfung
- Inspektion
- Prüfung
- Audit
- Entwicklungs- und Designprüfung

Ermittlung

Für die Prüfung auf Datenschutz durch datenschutzfreundliche Voreinstellungen gelten die Ausführung in Nr. 9.2 analog.

Zur Prüfung der Erforderlichkeit der Datenverarbeitung gelten die Ausführungen in Nr. 12 zum Grundsatz der Datenminimierung analog.

Nr. 20 – Auftragsverarbeitung des Cloud-Anbieters

Nr. 20.1 – Dienstleistung aufgrund einer rechtsverbindlichen Vereinbarung (Art. 28 Abs. 3 UAbs. 1 Satz 2 DSGVO)

Kriterium

(1) Lagert der Cloud-Anbieter die Verarbeitung von Daten zur Erfüllung des Auftrags über die Erbringung des Cloud-Dienstes an einen Auftragsverarbeiter aus, schließt er mit diesem eine rechtsverbindliche Vereinbarung zur Auftragsverarbeitung ab.

(2) Der Cloud-Anbieter stellt durch geeignete TOM sicher, dass der Auftrag erst nach dem Abschluss einer rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung mit dem Auftragsverarbeiter erbracht wird.

(3) Die rechtsverbindliche Vereinbarung zur Auftragsverarbeitung ist schriftlich oder in einem elektronischen Format abzufassen.

(4) Die rechtsverbindliche Vereinbarung zur Auftragsvereinbarung muss die nachfolgenden Anforderungen dieses Kriteriums erfüllen, wobei die geforderten Festlegungen auch in sonstigen Dokumenten getroffen werden können, wenn diese als Bestandteile der rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung einbezogen worden sind.

---

[41] In Bezug auf Letzteres muss der Cloud-Anbieter sicherstellen, dass Personen, die unter seiner Aufsicht handeln, nur dann auf die personenbezogenen Daten zugreifen, wenn sie diese kennen müssen („need to know“).

[42] Unangemessene Risiken ergeben sich aus der Nichtberücksichtigung des Stands der Technik, der Kosten der Umsetzung und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Risiken unterschiedlicher Wahrscheinlichkeit und Schwere für die Rechte und Freiheiten natürlicher Personen, die von der Verarbeitung ausgehen.

[43] Ein „zu großer Umfang“ ist gegeben, wenn ein technischer oder persönlicher Zugang mehr Informationen gewährt, als für den jeweiligen Zweck der Verarbeitung erforderlich sind.

(5) Der Cloud-Anbieter stellt sicher, dass in der rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung Gegenstand und Dauer der Verarbeitung so konkret wir möglich festgelegt werden.

(6) Der Cloud-Anbieter stellt sicher, dass in der rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung, Art und Zweck der vorgesehenen Verarbeitung, Art der verarbeiteten Daten sowie die Kategorien betroffener Personen festgelegt werden.

(7) Der Cloud-Anbieter stellt sicher, dass in der rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung festgelegt ist, dass personenbezogene Daten nur auf seine dokumentierte Weisung hin vom Auftragsverarbeiter verarbeitet werden, auch in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation, sofern er nicht durch das Recht der Union oder des Mitgliedstaats, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist. Für diesen Fall enthält die rechtsverbindliche Vereinbarung zur Auftragsverarbeitung die Verpflichtung, dass der Auftragsverarbeiter dem Cloud-Anbieter diese rechtlichen Anforderungen vor der Verarbeitung mitzuteilen hat, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(8) Für den Fall, dass die Auftragsverarbeitung weisungsgebundene Übermittlungen personenbezogener Daten an Drittländer oder internationale Organisationen vorsieht, stellt der Cloud-Anbieter sicher, dass die rechtsverbindliche Vereinbarung über die Auftragsverarbeitung die Instrumente nach Art. 45 DSGVO oder Art. 46 Abs. 2 und 3 DSGVO festlegt, die für die Übermittlungen genutzt werden sollen und ggf. auch die weiteren zusätzlich zu ergreifenden Maßnahmen, um ein angemessenes Schutzniveau sicherzustellen.

(9) Der Cloud-Anbieter stellt sicher, dass in der rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung festgelegt ist, dass sich der Auftragsverarbeiter zur Information des Cloud-Anbieters verpflichtet, wenn er der Ansicht ist, dass eine Weisung des Cloud-Anbieters gegen datenschutzrechtliche Vorschriften verstößt.

(10) Der Cloud-Anbieter stellt sicher, dass in der rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung der Ort der Datenverarbeitung festgelegt wird. Erfolgt die Datenverarbeitung außerhalb der EU oder des EWR, ist das konkrete Drittland zu benennen.

(11) Der Cloud-Anbieter stellt sicher, dass sich der Auftragsverarbeiter in der rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung darauf verpflichtet, ihm Änderungen des Datenverarbeitungsortes unverzüglich mitzuteilen.

(12) Der Cloud-Anbieter stellt sicher, dass in der rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung festgelegt wird, dass der Auftragsverarbeiter die zur Verarbeitung von personenbezogenen Daten befugten Personen vor Aufnahme der datenverarbeitenden Tätigkeit zur Vertraulichkeit über das Ende ihres Beschäftigungsverhältnisses hinaus verpflichtet, sofern sie nicht bereits einer angemessenen vergleichbaren gesetzlichen Verschwiegenheitspflicht unterliegen.

(13) Der Cloud-Anbieter stellt sicher, dass gemäß Art. 32 DSGVO die dem Schutzniveau der ausgelagerten Datenverarbeitung angemessenen TOM in der rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung festgelegt werden.

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

(15) Die Pflichten des Auftragsverarbeiters zur Rückgabe von Datenträgern, Rückführung von Daten und irreversiblen Löschung von Daten nach Ende der Auftragsverarbeitung sind in der rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung festzulegen.

(16) Die rechtsverbindliche Vereinbarung über die Auftragsverarbeitung enthält Angaben zur Unterstützung des Cloud-Anbieters bei der Erfüllung der Betroffenenrechte und der Meldepflicht bei Datenschutzverletzungen.

Ermittlungsmethoden

- Dokumentprüfung, insbesondere Rechtsanalyse

Ermittlung

Der Evaluator sollte eine Einsichtnahme in das Verzeichnis eingesetzter Subauftragsverarbeiter bekommen, und eine stichprobenartige Prüfung geschlossener Vereinbarungen durchführen. Ein Evaluator prüft die Vereinbarungen zu den weiteren Subauftragsverarbeitern mitsamt der für die Konformitätsprüfung erforderlichen Angaben. Für die jeweiligen Subauftragsverarbeiter sollten vorliegende Dokumente der TOM, das Datensicherheitskonzept oder Zertifikate stichprobenartig geprüft werden. Weitere relevante Dokumente können bei der Prüfung einbezogen werden, darunter der Mustervertrag zur Auftragsverarbeitung mit Subauftragsverarbeiter, Richtlinien und Anweisungen, weitere Garantien der Subauftragsverarbeiter, interne Kontrollbereiche des Cloud-Anbieters über Subauftragsverarbeiterkontrollen, das Datenschutzkonzept, oder die Risikoabschätzung bei der Unterbeauftragung.

Nr. 20.2 – Sicherstellung ordnungsgemäßer Auftragsverarbeitung

Kriterium

(1) Der Cloud-Anbieter stellt sicher, dass der Auftragsverarbeiter personenbezogene Daten nur auf seine dokumentierte Weisung hin verarbeitet (Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. a und h, 29; 32 Abs. 4 DSGVO).

(2) Der Cloud-Anbieter stellt sicher, dass der Auftragsverarbeiter ihn informiert, wenn er der Ansicht ist, dass seine Weisungen gegen datenschutzrechtliche Vorschriften verstoßen (Art. 28 Abs. 3 UAbs.1 Satz 2 lit. h i.V.m. Art. 29 DSGVO).

(3) Der Cloud-Anbieter stellt sicher, dass der Auftragsverarbeiter bei der ausgelagerten Verarbeitung Vertraulichkeit, Integrität und Verfügbarkeit der Daten und Systeme, die Belastbarkeit der Systeme sowie die Verfügbarkeit der Daten und den Zugang zu ihnen nach einem physischen oder technischen Zwischenfall gewährleistet. Die implementierten TOM müssen vom Auftragsverarbeiter regelmäßig (mindestens jährlich und nach jeder wesentlichen Änderung) überprüft und gegebenenfalls angepasst werden (Art. 24, 25, 28, 32, 35 i.V.m. Art. 5 Abs. 1 lit. f und Abs. 2 DSGVO).

(4) Der Cloud-Anbieter stellt sicher, dass der Auftragsverarbeiter seine Mitarbeiter vor Beginn der Datenverarbeitung zur Vertraulichkeit über das Ende ihres Beschäftigungsverhältnisses hinaus verpflichtet, sofern sie nicht einer gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. b und h DSGVO).

(5) Der Cloud-Anbieter stellt sicher, dass der Auftragsverarbeiter nur Mitarbeiter mit der Durchführung von Verarbeitungsvorgängen betraut, die die dafür erforderliche Fachkunde aufweisen und die im Datenschutz und der Datensicherheit geschult sind (Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. e und f DSGVO).

(6) Der Cloud-Anbieter stellt sicher, dass der Auftragsverarbeiter den Cloud-Anbieter in jenen Fällen informiert, in denen sich der Datenverarbeitungsort ändert (Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. a und h DSGVO).

(7) Der Cloud-Anbieter stellt sicher, dass der Auftragsverarbeiter nach Abschluss der Auftragsverarbeitung oder auf Weisung des Cloud-Anbieters überlassene Datenträger zurückgibt, Daten zurückführt und beim ihm gespeicherte Daten irreversibel löscht (Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. g und h DSGVO).

(8) Der Cloud-Anbieter stellt sicher, dass der Auftragsverarbeiter dem Cloud-Anbieter die Erfüllung der Betroffenenrechte ermöglicht und alle Weisungen zur Umsetzung der Betroffenenrechte dokumentiert (Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. e und h i.V.m. Kapitel III DSGVO).

(9) Der Cloud-Anbieter stellt sicher, dass der Auftragsverarbeiter einen DSB benennt, sofern er hierzu gesetzlich verpflichtet ist (Art. 37-39 DSGVO, § 38 Abs. 1; Abs. 2 i.V.m. § 6 Abs. 5 Satz 2 BDSG).

(10) Der Cloud-Anbieter verpflichtet den Auftragsverarbeiter darauf, ein Verarbeitungsverzeichnis zu führen, wenn er gesetzlich dazu verpflichtet ist (Art. 30 Abs. 2 - 5 DSGVO).

(11) Der Cloud-Anbieter stellt sicher, dass ihm der Auftragsverarbeiter Datenschutzverletzungen und deren Ausmaß unverzüglich meldet (Art. 33 Abs. 2 und Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. f).

(12) Der Cloud-Anbieter stellt sicher, dass der Auftragsverarbeiter allen Anforderungen aus der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung nach Nr. 20.1 nachkommt und alle Anforderungen nach diesem Kriterium erfüllt (Art. 24 Abs. 1 DSGVO).

(13) Der Cloud-Anbieter stellt sicher, dass der Auftragsverarbeiter, wenn er seinerseits Subauftragsverarbeiter einsetzt, gewährleistet, dass diese die Anforderungen nach den Kriterien Nr. 10.1-10.5 aus Kapitel V einhalten.

(14) Sieht die Auftragsverarbeitung die weisungsgebundene Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen vor oder unterliegt der Auftragsverarbeiter dem Recht eines Drittlands, das ihn zur Offenlegung von personenbezogenen Daten an staatliche Stellen des Drittlands verpflichtet, obwohl die Datenverarbeitung ausschließlich in der EU oder im EWR stattfindet, stellt der Cloud-Anbieter sicher, dass der Auftragsverarbeiter das Kriterium Nr. 11.1 aus Kapitel VI einhält (Art. 46 i.V.m. Art. 42 Abs. 1 und 2; Art. 48 DSGVO).

(15) Der Cloud-Anbieter verpflichtet den Auftragsverarbeiter zur Benennung eines Vertreters nach Kriterium Nr. 11.2 aus Kapitel VI, wenn dieser gesetzlich dazu verpflichtet ist (Art. 27 i.V.m. Art. 3 Abs. 2 DSGVO).

Ermittlungsmethoden

- Dokumentprüfung
- Audit

Ermittlung

Ein Evaluator prüft vorhandene Dokumente der Subauftragsverarbeiter (bspw. befolgte Verhaltensregeln, Zertifikate, rechtsverbindliche Vereinbarungen (insb. in Hinblick auf Weisungen durch den Cloud-Anbieter und Pflichten des Subauftragsverarbeiters), Dienstbeschreibungen, Datensicherheitskonzepte, sonstige Garantien), aus denen sich die Gewähr zur Einhaltung der Datenschutz-Grundverordnung ergibt. Darüber hinaus prüft er Dokumente über die Auswahl (bspw. Protokolle über Auswahlüberlegungen und -entscheidungen) und der Durchführung von eigenen Kontrollen (bspw. Protokolle der Subauftragsverarbeiterkontrollen). Protokolle zur Pflichterfüllung infolge der Einschaltung von weiteren Auftragsverarbeitern sollten geprüft werden.

Unterstützend kann im Rahmen eines Audits eine Befragung der Mitarbeiter zur Durchführung der Kontrolle von Subauftragsverarbeitern durchgeführt werden (bspw. Bekanntheit von Verfahrensschritten und Garantien der Subauftragsverarbeiter). Auch kann im Rahmen eines Audits eine Befragung der Mitarbeiter zur Einbindung von Subauftragsverarbeitern bei den Unterstützungsfunktionen und Pflichten als Hauptauftragsverarbeiter durchgeführt werden (bspw. Bekanntheit von Verfahrensschritten und Ansprechpartner der Subauftragsverarbeiter).

Nr. 21 – Datenübermittlung[44]

Nr. 21.1 – Geeignete Garantien für die Datenübermittlung; Maßnahmen zum Schutz vor der Offenlegung gegenüber staatlichen Stellen von Drittländern (Art. 45, 46 und Art. 48 DSGVO)

Vorbemerkung

Es ist möglich, dass der Cloud-Anbieter in seiner Rolle als für die Verarbeitung Verantwortlicher Daten des Cloud-Nutzers oder von Personen, die für ihn arbeiten, im Rahmen seines Geschäfts/Unternehmens übermittelt. Dies kann z.B. aus technischen, rechtlichen oder anderen Gründen geschehen. Zum Beispiel könnte ein technisches Update/Support aus dem Ausland seines Server-Lieferanten im laufenden Geschäftsbetrieb dazu führen, dass ein Cloud-Nutzer den Cloud-Dienst nutzt, obwohl die Systeme gerade vom technischen Support bearbeitet werden. Ein anderes Beispiel könnte sein, dass der Cloud-Anbieter als Verantwortlicher für seine Systeme und deren Verarbeitung durch EU- oder mitgliedstaatliches Recht gesetzlich dazu verpflichtet ist. Daher müssen entsprechende Kriterien eingeführt werden, die sicherstellen, dass Übermittlungen in dieser Hinsicht auch dem Regime der Datenschutz-Grundverordnung unterliegen. In dieser Hinsicht ist es der für seine Geschäftslösung und die Verarbeitung Verantwortliche, der personenbezogener Daten verarbeitet. Er übermittelt Daten unter seiner eigenen Verantwortung und gegebenenfalls unter seiner eigenen rechtlichen Verpflichtung.

Kriterium

(1) Der Cloud-Anbieter kann personenbezogene Daten in Drittländer oder an internationale Organisationen übermitteln, sofern er überprüft hat, dass für den Empfängerstaat oder die internationale Organisation, in der der Datenimporteur ansässig ist, ein Beschluss der Europäischen Kommission nach Art. 45 Abs. 3 DSGVO vorliegt, dass dort ein angemessenes Datenschutzniveau gilt und der Cloud-Anbieter regelmäßig (mindestens jährlich) prüft, ob der Angemessenheitsbeschluss fort gilt und die in Frage stehende Übermittlung über den benannten Beschluss erfasst wird.

(2) Alternativ kann die Datenübermittlung stattfinden, wenn der Cloud-Anbieter nach Überprüfung von Rechtslage und Praxis im Drittland sicherstellt, dass geeignete Garantien im Sinne des Art. 46 Abs. 2 oder 3 DSGVO verwendet werden und diese geeigneten Garantien ein angemessenes Datenschutzniveau sicherstellen, das dem der Datenschutz-Grundverordnung gleichwertig ist.

(3) Reichen nach Überprüfung von Rechtslage und Praxis im Drittland die geeigneten Garantien im Sinne des Art. 46 Abs. 2 oder 3 DSGVO nicht aus, um ein angemessenes Datenschutzniveau sicherzustellen, das dem der Datenschutz-Grundverordnung gleichwertig ist, ergreift der Cloud-Anbieter zusätzliche Maßnahmen[45], um dieses angemessene Datenschutzniveau sicherzustellen. Andernfalls darf keine Datenübermittlung stattfinden.

(4) Der Cloud-Anbieter überwacht fortlaufend die Angemessenheit des Datenschutzniveaus und stellt sicher, dass Datenübermittlungen umgehend ausgesetzt oder beendet werden, wenn im Fall des Abs. 2 oder 3 der Empfänger die Pflichten, die er nach den geeigneten Garantien des Art. 46 Abs. 2 oder 3 DSGVO

[44] Die Übermittlung bezieht sich auf die Bewegung personenbezogener Daten, wenn diese aus der EU/dem EWR in ein Land oder mehrere Länder außerhalb der EU/des EWR übermittelt werden.
[45] Z.B. TOMs in Übereinstimmung mit den Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten.

eingegangen ist, verletzt hat oder ihre Erfüllung unmöglich ist und im Fall von Abs. 3 die zusätzlichen Maßnahmen nicht mehr eingehalten werden können oder unwirksam sind.

(5) Cloud-Anbieter, die personenbezogene Daten verarbeiten und nicht nur dem Recht der Datenschutz-Grundverordnung unterliegen, sondern zugleich dem Recht eines Drittlands, das sie zu einer Offenlegung dieser personenbezogenen Daten gegenüber staatlichen Stellen des Drittlands verpflichtet, ergreifen zusätzliche Maßnahmen, um die personenbezogenen Daten vor einer Offenlegung an staatliche Stellen des Drittlands wirksam zu schützen. Der Cloud-Anbieter stellt sicher, dass personenbezogene Daten staatlichen Stellen von Drittländern nur offengelegt werden, wenn die Offenlegung auf eine in Kraft befindliche internationale Übereinkunft zwischen dem ersuchenden Drittland und der Union oder Deutschland gestützt ist.

Ermittlungsmethoden

- Dokumentprüfung, insbesondere Rechtsanalyse
- Inspektion
- Prüfung
- Audit

Ermittlung

Auf die Ermittlung in Nr. 11.1 wird verwiesen.

D. Referenzen

Arbeitspapier „Anforderungen an den datenschutzkonformen Einsatz von Pseudonymisierungslösungen“	Schwartmann/Weiß (Hrsg.), Anforderungen an den datenschutzkonformen Einsatz von Pseudonymisierungslösungen, Ein Arbeitspapier der Fokusgruppe Datenschutz der Plattform Sicherheit, Schutz und Vertrauen für Gesellschaft und Wirtschaft im Rahmen des Digital-Gipfels 2018, https://www.gdd.de/downloads/anforderungen-an-datenschutzkonforme-pseudonymisierung
BSI C5	Cloud Computing Compliance Controls Catalogue (BSI C5), Version 2020, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2020/C5_2020.html, Englische Fassung
BSI TR-02102-1	Kryptographische Verfahren: Empfehlungen und Schlüssellängen, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.html, Stand 22.02.2019
BSI TR-02102-2	Kryptographische Verfahren: Empfehlungen und Schlüssellängen. Teil 2 – Verwendung von Transport Layer Security (TLS), https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.html, Stand 22.02.2019
BSI TR-02102-3	Kryptographische Verfahren: Verwendung von Internet Protocol Security (IPSec) und Internet Key Exchange (IKEv2), https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-3.html, Stand 25.01.2018
BSI TR-02102-4	Kryptographische Verfahren: Verwendung von Secure Shell (SSH), https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-4.html, Stand 25.01.2018
DIN EN 1627	Türen, Fenster, Vorhangfassaden, Gitterelemente und Abschlüsse - Einbruchhemmung - Anforderungen und Klassifizierung. Stand 2011
DIN 66398	Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten. Stand 2016
DIN 66399	Vernichtung von Datenträgern. Stand 2012
EU-SVK	Europäische Kommission, Durchführungsbeschluss vom 4.6.2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der DSGVO, https://ec.europa.eu/info/sites/default/files/1_de_act_part1_v3_1.pdf.
DSFA-Liste Verarbeitungsvorgänge	Datenschutzkonferenz, Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist, Version 1.1 vom 17.10.2018, https://www.datenschutzkonferenz-online.de/media/ah/20181017_ah_DSK_DSFA_Muss-Liste_Version_1.1_Deutsch.pdf.
Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Datenschutzniveaus für personenbezogene Daten	Europäischer Datenschutzausschuss, Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Datenschutzniveaus für personenbezogene Daten vom 10. November 2020, https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_de.pdf
Empfehlungen 02/2020 zu den wesentlichen europäischen Garantien in Bezug auf Überwachungsmaßnahmen“ erfolgen	Europäischer Datenschutzausschuss, Empfehlungen 02/2020 zu den wesentlichen europäischen Garantien in Bezug auf Überwachungsmaßnahmen vom 10. November 2020, https://edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_de.pdf
Factsheet – Mass Surveillance	European Court of Human Rights, Factsheet – mass surveillance, May 2021, https://www.echr.coe.int/documents/fs_mass_surveillance_eng.pdf.
https://gdprhub.eu/Article_2_GDPR#(c)_Processing_by_a_natural_person_in_the_course_of_purely_personal_or_household_activity	Verweis auf NOYB – European Center for Digital Rights. Abgerufen am 05.06.2024.
Guidelines 4/2019	European Data Protection Board, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default,Version 2.0, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf, Stand 20.10.2020

Handreichung zum Stand der Technik	Teletrust, IT-Sicherheitsgesetz und Datenschutz-Grundverordnung: Handreichung zum „Stand der Technik“. Technische und organisatorische Maßnahmen, https://www.teletrust.de/fileadmin/user_upload/2021-02_TeleTrusT-Handreichung_Stand_der_Technik_in_der_IT-Sicherheit_DE.pdf, Stand: 2021
IAF MD 4:2018	IAF MANDATORY DOCUMENT FOR THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) FOR AUDITING/ASSESSMENT PURPOSES Issue 2. Stand 2018
ISO 10911:2018	Leitfaden zur Auditierung von Managementsystemen (ISO 19011:2018). Stand 2018
ISO/IEC 11770-2	IT Security techniques — Key management — Part 2: Mechanisms using symmetric techniques. Stand 2018
ISO/IEC 15408:2009	Information technology -- Security techniques -- Evaluation criteria for IT security. Stand 2009
ISO/IEC 17021-1:2015	Anforderungen an Stellen, die Managementsysteme auditieren und zertifizieren – Teil 1: Anforderungen. Stand 2015
ISO/IEC 17025:2017	Allgemeine Anforderungen an die Kompetenz von Prüf- und Kalibrierlaboratorien. Stand 2017
ISO/IEC 17065:2012	Anforderungen an Stellen, die Produkte, Prozesse und Dienstleistungen zertifizieren. Stand 2012
ISO/IEC 17067:2013	Grundlagen der Produktzertifizierung und Leitlinien für Produktzertifizierungsprogramme. Stand 2013
ISO/IEC 18045:2008-018	Information technology -- Security techniques -- Methodology for IT security evaluation. Stand 2008
ISO/IEC 19941	Information technology — Cloud computing — Interoperability and portability. Stand 2017
ISO/IEC 21964-1	Information technology — Destruction of data carriers — Part 1: Principles and definitions. Stand 2018
ISO/IEC 24760-1	IT Security and Privacy — A framework for identity management — Part 1: Terminology and concepts. Stand 2019
ISO/IEC 24760-2	Information technology — Security techniques — A framework for identity management — Part 2: Reference architecture and requirements. Stand 2015
ISO/IEC 24760-3	Information technology — Security techniques — A framework for identity management — Part 3: Practice. Stand 2016
ISO 25237	Health informatics — Pseudonymization. Stand 2017
ISO/IEC 27002	Information technology — Security techniques — Code of practice for information security controls. Stand 2013
ISO/IEC 27018	Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors. Stand 2019
ISO/IEC 27040	Information technology — Security techniques — Storage security. Stand 2015
ISO/IEC 27701	Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines. Stand 2019
ISO/IEC 29101	Information technology — Security techniques — Privacy architecture framework. Stand 2018
ISO/IEC 29134	Information technology — Security techniques — Guidelines for privacy impact assessment. Stand 2017
ISO/IEC 29146	Information technology — Security techniques — A framework for access management. Stand 2016
ISO 31000	Risk management – Guidelines. Stand 2018
IEC 31010	Risk management — Risk assessment techniques. Stand 2019
Länderberichte	Inter-American Commission on Human Rights, Country Reports, https://www.oas.org/en/IACHR/jsForm/?File=/en/iachr/reports/country.asp.
SDM	Standard-Datenschutzmodell, Version 2.0, https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methode.pdf, Stand November 2019
SDM-Bausteine	Maßnahmenkatalog des SDM, https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/, Stand Juni 2024