European Cloud Service
Data Protection Certification

AUDITOR-Schutzklassenkonzept

-15.10.2018 -

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

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

Autoren

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

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

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

UNIKASSEL VERSITÄT

provet

KIT Karlsruher Institut für Technologie

CRITICAL INFORMATION INFRASTRUCTURES

Inhaltsverzeichnis

Abkürzungsverzeichnis

Abs.	Absatz
Art.	Artikel
DSGVO	EU-Datenschutz-Grundverordnung (Geltung ab 25.5.18)
Lit.	Litera
Nr.	Nummer
S.	Siehe
TCDP	Trusted Cloud Datenschutz-Profil
Z.B.	Zum Beispiel

Hinweis zur geschlechtsneutralen Formulierung:

Aus Gründen der leichteren Lesbarkeit wird auf eine geschlechtsspezifische Differenzierung, wie z.B. Cloud-Nutzer/innen, verzichtet. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung für alle Geschlechter.

Hinweis zu AUDITOR als Nachfolger von TCDP:

Die Zertifizierung nach dem alten Bundesdatenschutzgesetz wurde im Pilotprojekt „Datenschutz-Zertifizierung für Cloud-Dienste“ durch das im September 2016 finalisierte TCDP untersucht. TCDP stellt einen Prüfstandard für die Datenschutz-Zertifizierung von Cloud-Diensten nach dem alten Bundesdatenschutzgesetz dar und unterscheidet hierbei zwischen drei Schutzklassen, die im Schutzklassenkonzept beschrieben werden. Als Nachfolge zum TCDP entwickelt das Forschungsprojekt AUDITOR einen Standard für die Datenschutz-Zertifizierung von Cloud-Diensten nach der DSGVO. Der AUDITOR-Kriterienkatalog unterscheidet bei technischen und organisatorischen Anforderungen an Datenschutz und Datensicherheit ebenfalls drei Schutzklassen und baut maßgeblich auf dem Schutzklassenkonzept von TCDP auf.

1 Die Datenschutz-Zertifizierung

Ein zentrales Element des AUDITOR-Zertifizierungsverfahrens bildet der Kriterienkatalog, der die normativen Anforderungen der Datenschutz-Grundverordnung und des Bundesdatenschutzgesetzes an Cloud-Anbieter als Auftragsverarbeiter gemäß Art. 4 Nr. 8 DSGVO für die von ihnen angebotenen Cloud-Dienste in prüffähige Kriterien überführt. Der Kriterienkatalog nimmt bei einigen Kriterien eine Unterscheidung nach Schutzklassen vor und legt für diese unterschiedliche Anforderungen fest, die erfüllt werden müssen. Schutzklassen stellen bei der Datenschutz-Zertifizierung ein wichtiges Instrument dar, da mit ihnen der individuelle Schutzbedarf von Datenverarbeitungsvorgängen und dessen Erfüllung durch zertifizierte Cloud-Dienste ausgedrückt werden kann. Die Grundlagen und Ausgestaltungen der Schutzklassen werden in diesem Schutzklassenkonzept beschrieben.

Den Zertifizierungsgegenstand der AUDITOR-Zertifizierung bilden Datenverarbeitungsvorgänge im Kontext von Cloud Computing, die in Produkten oder Diensten oder mit Hilfe von (auch mehreren) Produkten oder Diensten erbracht werden. Da Datenverarbeitungsvorgänge oder Bündel von Datenverarbeitungsvorgängen regelmäßig in Form von Diensten vorliegen, wird in diesem Dokument häufig der Ausdruck „Zertifizierung von Cloud-Diensten“ verwendet. Dies ändert jedoch nichts daran, dass mit diesem Ausdruck stets die Zertifizierung von Datenverarbeitungsvorgängen im Kontext des Cloud Computing gemeint ist, da Art. 42 Abs. 1 Satz 1 DSGVO Datenverarbeitungsvorgänge als Zertifizierungsgegenstand festlegt.

Gemäß Art. 28 Abs. 1 DSGVO darf der Cloud-Nutzer als Verantwortlicher der Datenverarbeitung nur solche Cloud-Anbieter als Auftragsverarbeiter einsetzen, „die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt […]“. Art. 28 Abs. 5 DSGVO bestimmt, dass Verantwortliche erfolgreich durchlaufene genehmigte Zertifizierungsverfahren von Auftragsverarbeitern als „Faktor“ dafür heranziehen können, dass der Auftragsverarbeiter die hinreichenden Garantien gemäß Art. 28 Abs. 1 DSGVO bietet.

Hat der Cloud-Anbieter ein genehmigtes Zertifizierungsverfahren durchlaufen und die für ihn maßgeblichen Kriterien erfüllt, erhält er von der die Zertifizierung durchführenden akkreditierten Zertifizierungsstelle ein Zertifikat. Der Cloud-Nutzer darf in diesen Fall darauf vertrauen, dass der zertifizierte Cloud-Dienst datenschutzkonform angeboten wird und muss nicht selbst die technischen und organisatorischen Maßnahmen des ausgewählten Cloud-Anbieters prüfen und sich von diesen überzeugen.

2 Berücksichtigung individueller Datenschutz- und Datensicherheitsanforderungen durch Schutzklassen

2.1 Zertifizierung und risikobasierter Ansatz für technische und organisatorische Maßnahmen bei Datenschutz und Datensicherheit

Ein AUDITOR-Zertifikat informiert Cloud-Nutzer darüber, ob ein Cloud-Anbieter als Auftragsverarbeiter bei seinem angebotenen Cloud-Dienst alle normativen Anforderungen erfüllt, die die Datenschutz-Grundverordnung und das Bundesdatenschutzgesetz an diesen stellt. Ein wesentliches Element der gesetzlichen Anforderungen sind die vom Cloud-Anbieter zu erbringenden technischen und organisatorischen Maßnahmen zur Einhaltung der zentralen datenschutzrechtlichen Grundsätze aus Art. 5 Abs. 1 DSGVO.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder hat im Standard-Datenschutzmodell für Anforderungen an eine rechtskonforme Datenverarbeitung, die aus dem Datenschutzrecht resultieren und die durch technische und organisatorische Maßnahmen gewährleistet werden können und müssen, sogenannte Gewährleistungsziele formuliert. Diese sind: Datenminimierung, Verfügbarkeit, Integrität, Vertraulichkeit, Nichtverkettung, Transparenz und Intervenierbarkeit.

Die technischen und organisatorischen Maßnahmen, die im Anwendungsfall von AUDITOR von den Cloud-Anbietern zur Erfüllung der Gewährleistungsziele ergriffen werden müssen, werden durch die Datenschutz-Grundverordnung in keiner allgemeingültigen und absoluten Form vorgeschrieben. Vielmehr fordert der in den Art. 24, 25 und 32 DSGVO niedergelegte sogenannte risikobasierte Ansatz, dass die Maßnahmen immer entsprechend der konkreten Umstände der Verarbeitung und der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten der betroffenen Personen ausgewählt werden müssen. Konkret schreibt die Datenschutz-Grundverordnung beispielsweise bei der Sicherheit der Verarbeitung in Art. 32 Abs. 1 DSGVO vor, dass die Anforderungen an die technischen und organi-

satorischen Maßnahmen und damit auch der Grad der zu erreichenden Zuverlässigkeit dieser Maßnahmen unter „Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen“ zu bestimmen sind. Die Maßnahmen müssen demnach „ein dem Risiko angemessenes Schutzniveau“ gewährleisten.

Hinweis: Auch das BSI nimmt im IT-Grundschutz im Abschnitt „CON.2 Datenschutz“ in Nr. 3.1 Bezug auf das Standard-Datenschutzmodell und fordert, dass die Nichtberücksichtigung des vollständigen Schutzziele-Katalogs und eine Nichtanwendung dieser Methodik sowie der Referenzmaßnahmen begründet werden müssen. Cloud-Anbieter müssen sich daher auch mit dem Standard-Datenschutzmodell im Rahmen der ISO 27001 Zertifizierung auf Basis von IT-Grundschutz auseinandersetzen.

2.2 Das Schutzklassenkonzept

Das Schutzniveau wird im Schutzklassenkonzept durch unterschiedliche „Schutzklassen“ ausgedrückt. Der Cloud-Nutzer eines Cloud-Dienstes kann den individuellen Schutzbedarf seiner Datenverarbeitungsvorgänge in die entsprechende Schutzklasse einordnen und einen Cloud-Dienst wählen, dessen Datenschutz- und Datensicherheitsniveau der von ihm benötigten Schutzklasse entspricht. Die Schutzklasse eines Cloud-Dienstes kann der Cloud-Nutzer dem Zertifikat des Cloud-Anbieters entnehmen.

Die Schutzklasse nimmt eine Doppelfunktion ein: Zum einen beschreibt sie den Schutzbedarf der Datenverarbeitungsvorgänge. Zum anderen legt sie die Anforderungen an die technischen und organisatorischen Maßnahmen fest, die der Cloud-Anbieter erfüllen muss.

Um diese Doppelfunktion deutlich zu machen, wird bei der Schutzklasse zwischen zwei Komponenten unterschieden: den Schutzbedarfsklassen und den Schutzanforderungsklassen. Die Schutzbedarfsklasse beschreibt den Schutzbedarf des Cloud-Nutzers für seine Datenverarbeitungsvorgänge anhand genereller Merkmale. Die Schutzanforderungsklasse beschreibt in allgemeiner Form die technischen und organisatorischen Anforderungen, die für Cloud-Dienste der betreffenden Klasse maßgeblich vom Cloud-Anbieter zu erfüllen sind. Für jede Schutzbedarfsklasse wird eine korrespondierende Schutzanforderungsklasse definiert.

Es ist dabei nicht erforderlich, jede gesetzliche Anforderung (in Gestalt der Kriterien des AUDITOR-Kriterienkatalogs) einer bestimmten Schutzanforderungsklasse zuzuordnen, da die nicht technisch-organisatorischen datenschutzrechtlichen Anforderungen an die Auftragsverarbeitung vom Schutzbedarf unabhängig sind. So stellt etwa die Pflicht des Cloud-Anbieters zur Unterstützung des Cloud-Nutzers bei der Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten gemäß Art. 28 Abs. 3 lit. e DSGVO eine gesetzliche Anforderung an die Auftragsverarbeitung dar, die jedoch vom Schutzbedarf des jeweiligen Datenverarbeitungsvorgangs unabhängig ist.

Unterschiedliche normative Anforderungen müssen jedoch dort formuliert werden, wo ein unterschiedlicher Schutzbedarf zu unterschiedlichen Anforderungen an technische und organisatorische Maßnahmen führt. Im Kriterienkatalog sind von der Schutzklasse abhängige Kriterien vor allem in Kapitel 2, Nr. 2 bei der Gewährleistung der Datensicherheit formuliert worden.

Obwohl mit der Bildung von Schutzbedarfsklassen eine Generalisierung einhergeht, muss beim Schutzklassenkonzept gewährleistet werden, dass der individuelle Schutzbedarf der Datenverarbeitung durch die technischen und organisatorischen Anforderungen der betreffenden Schutzanforderungsklasse abgedeckt ist. Dies wird im Schutzklassenkonzept dadurch erreicht, dass die Schutzanforderungen so definiert werden, dass sie den höchsten individuellen Schutzbedarf in der jeweils korrespondierenden Schutzbedarfsklasse abdecken.

Damit wird gewährleistet, dass für alle individuellen Schutzbedarfe in der jeweiligen Schutzbedarfsklasse hinreichende Schutzanforderungen gelten. Zugleich hat dies zur Folge, dass vielfach in den Schutzanforderungsklassen höhere Schutzanforderungen gestellt werden als es nach dem individuellen Schutzbedarf einer Datenverarbeitung nötig wäre. Der Cloud-Anbieter eines zertifizierten Cloud-Dienstes wird daher oft ein höheres Maß an Schutzanforderungen erfüllen als dies nach dem individuellen gesetzlichen Bedarf des Datenverarbeitungsvorganges erforderlich wäre.

2.3 Abbildung individuellen Schutzbedarfs durch Schutzbedarfsklassen

2.3.1 Anforderungen an Schutzbedarfsklassen

Voraussetzung der Zertifizierung nach Schutzklassen ist es, dass jeder individuelle Schutzbedarf einer Schutzbedarfsklasse zuordenbar ist. Schutzbedarfsklassen werden daher so definiert, dass sie lückenlos jeden individuellen Schutzbedarf abdecken. Hierfür werden sie mit Merkmalen beschrieben, die den Schutzbedarf des konkreten Datenverarbeitungsvorgangs widerspiegeln. Die Beschreibung ermöglicht es dem Cloud-Nutzer, den Schutzbedarf seiner Datenverarbeitung den Merkmalen der Schutzklasse zuzuordnen.

Für den Bereich der Datensicherheit wird der Schutzbedarf gemäß Art. 32 Abs. 1 DSGVO anhand mehrerer Faktoren bestimmt: Maßgeblich sind insbesondere die allgemeine Sensitivität der Daten nach ihrer Datenart, der Umfang der Datenverarbeitung, die Umstände und Zwecke der Datenverarbeitung sowie die Eintrittswahrscheinlichkeit und Schwere des Schadens für die Rechte der betroffenen Personen. Gemäß Art. 32 Abs. 2 DSGVO sind „bei der Beurteilung des angemessenen Schutzniveaus […] insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch – ob unbeabsichtigt oder unrechtmäßig – Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden“. Bei der Bestimmung der Schutzbedarfsklasse ist daher immer die konkrete Verarbeitung zu betrachten. Da alle relevanten Umstände miteinzubeziehen sind und somit mitunter eine Vielzahl an Umständen, kann die Bestimmung des konkreten Schutzbedarfs kompliziert werden. Dies steht jedoch der Bildung von Schutzklassen nicht entgegen.

Verarbeitet ein Cloud-Nutzer beispielsweise Daten wie die PIN und TAN im Online-Banking, so muss er sich insbesondere mit Angriffen Unbefugter, dem Missbrauch dieser Daten und den Wahrscheinlichkeiten dieser Vorkommnisse auseinandersetzen, weil diese Daten Zugang zu wirtschaftlichen Vorteilen bieten und daher in besonderem Maße Begehrlichkeiten wecken.

2.3.2 Schritte zur Ermittlung des Schutzbedarfs von Datenverarbeitungsvorgängen

Da eine lediglich allgemeine Beschreibung des Schutzbedarfs die Gefahr birgt, dass die Zuordnung des individuellen Schutzbedarfs zu einer Schutzbedarfsklasse allein von den Einschätzungen des jeweiligen Cloud-Nutzers abhängig und damit sehr subjektiv ist, was zu Rechtsunsicherheit führen und den Nutzen der Zertifizierung beeinträchtigen kann, enthält das Schutzklassenkonzept eine Systematik der Ermittlung des Schutzbedarfs.

Den Ausgangspunkt und ersten Schritt bildet der abstrakte Schutzbedarf anhand der Datenart. Es ist anerkannt, dass die Art der verarbeiteten Daten einen wesentlichen Einfluss auf den Schutzbedarf der Datenverarbeitung hat, da bestimmte Datenarten wie beispielsweise gesundheitsbezogene Daten einen wesentlich höheren Einfluss auf die Persönlichkeitsrechte der betroffenen Person haben als andere Datenarten.

In einem zweiten Schritt ist zu prüfen, ob schutzbedarfserhöhende Umstände vorliegen und ob der Schutzbedarf aufgrund dieser Umstände so stark zunimmt, dass eine Höherstufung in eine höhere Schutzklasse erforderlich ist.

Die Höherstufung wird in der Regel eine Schutzbedarfsklasse betreffen. In manchen Fällen kommt aber auch eine Höherstufung um zwei Schutzbedarfsklassen in Betracht. Als Zwischenergebnis dieser Prüfung ist eine Einstufung des Datenverarbeitungsvorgangs in eine Schutzbedarfsklasse zu treffen.

Im dritten Schritt ist zu prüfen, ob schutzbedarfsmindernde Umstände vorliegen. Diese können dazu führen, dass der Datenverarbeitungsvorgang im Ergebnis einer niedrigeren Schutzbedarfsklasse zugeordnet wird, als dies nach dem Zwischenergebnis des zweiten Schritts der Fall wäre. Die Möglichkeit der Herabstufung ergibt sich aus der vom Gesetz geforderten Maßgeblichkeit aller Umstände des Einzelfalls. Ein Beispiel für einen Umstand, der den Schutzbedarf senkt, ist etwa die vorherige Verschlüsselung von Daten durch den Cloud-Nutzer, bevor diese an den Cloud-Anbieter übermittelt und etwa in einem Host-Dienst gespeichert werden. Entsprechend der Heraufstufung des Schutzbedarfs im zweiten Schritt kann hier eine Herabstufung um eine, aber auch um mehrere, Schutzbedarfsklassen notwendig sein. Mit Abschluss des dritten Schritts ist die für die jeweilige Datenverarbeitung maßgebliche Schutzbedarfsklasse bestimmt.

Wenn in einem Cloud-Dienst mehrere Datenverarbeitungsvorgänge erfolgen sollen, muss der Dienst dem Schutzbedarf aller Datenverarbeitungsvorgänge gerecht werden. Daher ist für die Auswahl des Dienstes letztlich der höchste Schutzbedarf der verschiedenen Datenverarbeitungsvorgänge maßgeblich.

In der Praxis kann die Ermittlung der für einen Datenverarbeitungsvorgang maßgeblichen Schutzbedarfsklasse unter Umständen Schwierigkeiten bereiten. In diesen Fällen kann sich der Cloud-Nutzer

dadurch absichern, dass er in Zweifelsfällen die höhere Schutzbedarfsklasse wählt, um Risiken zu vermeiden.

2.4 Schutzanforderungsklassen für technische und organisatorische Maßnahmen

Entsprechend dem Ziel des Schutzklassenkonzepts müssen für jede Schutzbedarfsklasse korrespondierende Schutzanforderungen definiert werden, die den Schutzbedarf erfüllen und in den Schutzanforderungsklassen festgelegt werden.

Die Schutzanforderungen werden anhand abstrakter Merkmale beschrieben, damit sie durch verschiedene technische und organisatorische Maßnahmen erfüllt werden können. Bei der Gestaltung seines Cloud-Dienstes kann der Cloud-Anbieter die von ihm zu treffenden Maßnahmen im Hinblick auf die verschiedenen Schutzanforderungsklassen wählen. Im Rahmen der Zertifizierung des Cloud-Dienstes wird geprüft, ob die Maßnahmen die Anforderungen einer bestimmten Schutzanforderungsklasse erfüllen. Ist dies der Fall, wird das Zertifikat für die entsprechende Schutzklasse erteilt.

Die Anforderungen an die technischen und organisatorischen Maßnahmen lassen sich nicht im Wege eines Katalogs zuordnen. So ist es beispielsweise nicht möglich, im Rahmen des Zugangsschutzes den Schutzbedarf durch Passwort pauschal einer bestimmten Schutzanforderungsklasse zuzuordnen, da die Nutzung von Passwörtern je nach Ausgestaltung und den Umständen des Einzelfalls sehr unterschiedlichen Sicherheitsanforderungen genügen muss. Insoweit besteht ein erheblicher Interpretationsbedarf, der die Würdigung aller Umstände der konkreten Ausgestaltung des Dienstes einschließt. Diese Wertung wird bei der Zertifizierung im Rahmen der Prüfung vorgenommen. Daher ist es erforderlich, dass die Prüfung und Zertifizierung von qualifizierten Prüfern und akkreditierten Zertifizierungsstellen vorgenommen wird.

Wie bei den Schutzbedarfsklassen gilt es auch bei den Schutzanforderungsklassen zu beachten, dass nicht für jede gesetzliche Anforderung an die Auftragsverarbeitung eine Differenzierung nach Schutzanforderungsklassen erforderlich ist, weil gesetzliche Anforderungen häufig vom Schutzbedarf unabhängig sind.

2.5 Anzahl der Schutzklassen

Das AUDITOR-Schutzklassenkonzept umfasst 3 Schutzklassen. Für diese werden jeweils Schutzbedarfe (Schutzbedarfsklassen) und Schutzanforderungen (Schutzanforderungsklassen) beschrieben.

Es werden drei Schutzklassen gebildet, weil sich für sie hinreichend unterschiedliche Anforderungen definieren lassen und bei stärkerer Differenzierung zu hohe Schwierigkeiten der eindeutigen Zuordnung von Maßnahmen zu Schutzanforderungsklassen entstehen würden. Die Unterscheidung von drei Schutzklassen stellt wiederum das Mindestmaß an Differenzierung dar, weil bei nur zwei Schutzklassen die Gefahr besteht, dass in vielen Fällen Anforderungen erfüllt werden müssten, die erheblich über dem individuellen Schutzbedarf liegen und damit Kosten entstehen, die in Anbetracht des tatsächlich bestehenden Schutzbedarfs nicht geboten sind. Mit drei Schutzklassen wird die Zertifizierung für Cloud-Anbieter und Cloud-Nutzer handhabbar gemacht, weil die Zuordnung eines individuellen Schutzbedarfs oder einer Schutzmaßnahme zu einer Schutzklasse einfach und eindeutig ermöglicht wird.

Datenverarbeitungsvorgänge, die keine Aussagen über persönliche oder sachliche Verhältnisse natürlicher Personen enthalten, erzeugen, unterstützen oder solche ermöglichen, weisen keinen datenschutzrechtlichen Schutzbedarf auf. Da sie keine personenbezogene Daten verarbeiten, liegen diese Datenverarbeitungsvorgänge unterhalb von Schutzklasse 1, weshalb sie aus dem Schutzklassenkonzept herausfallen.

Beispiel: Der Cloud-Nutzer möchte reine Wetterdaten, wirksam anonymisierte Daten oder synthetisch erzeugte Testdaten („Max Mustermann“) verarbeiten.

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

Beispiel: Der Cloud-Nutzer möchte die Daten von V-Leuten des Verfassungsschutzes oder Daten über Personen, die mögliche Opfer von strafbaren Handlungen sein können, speichern. Die unbefugte Offenlegung dieser Daten kann zur Gefahr für Leib und Leben der betroffenen Personen führen.

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

Weisen Datenverarbeitungsvorgänge extrem hohen Schutzbedarf oder stark divergierende Umstände auf, muss der Cloud-Nutzer, der seine Datenverarbeitung an einen Cloud-Anbieter im Rahmen einer Auftragsverarbeitung auslagern möchte, in diesen Fällen selbst eine Risikoanalyse vornehmen und aufgrund dieser Analyse insbesondere die Anforderungen an die technischen und organisatorischen Maßnahmen des Cloud-Anbieters feststellen und sich von der Erfüllung der Anforderungen beim Cloud-Anbieter überzeugen, da das AUDITOR-Zertifikat nur für die Schutzklassen 1, 2 und 3 vergeben wird.

2.6 Die Anwendung des Schutzklassenkonzepts bei der Zertifizierung und Nutzung von Cloud-Diensten

Die Anwendung des Schutzklassenkonzepts bei der Zertifizierung und Nutzung eines zertifizierten Cloud-Dienstes führt zu einer differenzierten Aufgabenverteilung zwischen dem Cloud-Anbieter und dem Cloud-Nutzer sowie der akkreditierten Zertifizierungsstelle.

Der Cloud-Nutzer ordnet den Schutzbedarf seiner konkreten Datenverarbeitungsvorgänge einer bestimmten Schutzbedarfsklasse zu. Er ermittelt den Schutzbedarf hierbei anhand der dargestellten drei Schritte und kann auf dieser Grundlage einen Cloud-Dienst wählen, der für die betreffende Schutzklasse zertifiziert ist.

Der Cloud-Anbieter gewährleistet bei der Verarbeitung von Daten eine bestimmte Schutzbedarfsklasse und beantragt eine Zertifizierung für die korrespondierende Schutzanforderungsklasse.

Die akkreditierte Zertifizierungsstelle ordnet den Cloud-Dienst – auf der Grundlage der im Rahmen des Zertifizierungsverfahrens erfolgten Prüfung – anhand der konkreten technischen und organisatorischen Maßnahmen einer bestimmten Schutzklasse zu. Im Zertifikat wird die Eignung des Cloud-Dienstes für eine konkrete Schutzanforderungsklasse zum Ausdruck gebracht.

3 Schutzklassen

Im Folgenden werden die Schutzbedarfsklassen definiert und durch Beispiele erläutert (3.1) Anschließend wird die Zuordnung des Schutzbedarfs eines Datenverarbeitungsvorgangs zu einer Schutzbedarfsklasse anhand des dreischrittigen Verfahrens dargestellt (3.2). Dabei werden zunächst die abstrakten Schutzbedarfsklassen nach der jeweiligen Datenart definiert (3.2.1) und sodann Faktoren vorgestellt, die zu einer Heraufstufung (3.2.2) oder zu einer Absenkung des Schutzbedarfs (3.2.3) führen. Abschließend werden die Schutzanforderungsklassen beschrieben (3.3).

3.1 Schutzbedarfsklassen

3.1.1 Schutzbedarfsklasse 1

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

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

Hinweis: Damit die betroffene Person gegen Datenverarbeitungen vorgehen kann, muss sie Auskunft über die Datenverarbeitung erhalten und ihre übrigen Betroffenenrechte aus den Art. 17-22 DSGVO ausüben können. Wie einfach Betroffenenrechte ausgeübt werden können, hängt in großem Maße von der konkreten Ausgestaltung des Cloud-Dienstes ab.

Beispiel: Der Cloud-Nutzer möchte die Adressdaten seiner Vertragspartner speichern und verwalten. Dieser Datenverarbeitungsvorgang enthält aufgrund der Art der Daten (Name, Anschrift) und der Verarbeitung Aussagen über die persönlichen Verhältnisse der Vertragspartner.

3.1.2 Schutzbedarfsklasse 2

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

Beispiel: Der Cloud-Nutzer (Arbeitgeber) möchte den Grad der Behinderung von betroffenen Mitarbeitern im Betrieb verarbeiten. Dieser Datenverarbeitungsvorgang enthält aufgrund der Art der Daten und der Verarbeitung Aussagen über die Gesundheit der Mitarbeiter und weist daher einen hohen Schutzbedarf auf.

3.1.3 Schutzbedarfsklasse 3

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

Beispiel: Der Cloud-Nutzer ist Rechtsanwalt und möchte Mandantendaten, die dem Mandantengeheimnis überliegen, verarbeiten.

3.2 Ermittlung des Schutzbedarfs

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

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

Im Ergebnis wird der Schutzbedarf der konkreten Datenverarbeitung nach den Schutzbedarfsklassen kategorisiert.

3.2.1 Schutzbedarfsklassen nach Datenart (Schritt 1)

Im 1. Schritt wird zunächst der abstrakte Schutzbedarf der zu verarbeitenden Daten nach der Datenart bestimmt.

3.2.1.1 Datenarten mit normalem Schutzbedarf (Schutzbedarfsklasse 1)

Personenbezogene Daten im Sinne des Art. 4 Nr. 1 DSGVO, d.h. alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen und bei denen keine besonderen Beeinträchtigungen für die Persönlichkeitsrechte der betroffenen Personen zu erwarten sind.

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

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

3.2.1.2 Datenarten mit hohem Schutzbedarfs (Schutzbedarfsklasse 2)

Daten, die eine spezifische Aussagekraft über die Persönlichkeit und/oder die Lebensumstände der betroffenen Person haben oder sonst für die Verhältnisse der betroffenen Person von Bedeutung sind. Die unbefugte Erhebung, Verarbeitung oder Nutzung solcher Daten kann zu Beeinträchtigungen der betroffenen Person in ihrer gesellschaftlichen Stellung oder ihren wirtschaftlichen Verhältnissen führen („Ansehen“) führen.

In die Schutzbedarfsklasse 2 fallen auch Datenarten, die der Gesetzgeber als besonders schutzwürdig in Art. 9 Abs. 1 DSGVO ausgewiesen hat.

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

- Name, Anschrift eines Vertragspartners;
- Geburtsdatum;
- Familienstand:
- verwandtschaftliche Beziehungen und Bekanntenkreis;
- Daten über Geschäfts- und Vertragsbeziehungen;
- Kontext zu einem Vertragspartner (z.B. Gegenstand einer vereinbarten Leistung);
- Verarbeitungen nicht veränderbarer Personendaten, die lebenslang als Anker für Profilbildungen dienen können, wie genetische Daten i.S.v. Art. 4 Nr. 13 DSGVO oder biometrische Daten i.S.v. Art. 4 Nr. 14 DSGVO;
- Daten über die rassische und ethnische Herkunft;
- Daten über politische Meinungen;
- Religiöse oder weltanschauliche Überzeugungen;
- Gewerkschaftsangehörigkeit;
- Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person;
- Verarbeitungen eindeutig identifizierender, hoch verknüpfbarer Daten wie Krankenversichertennummern oder Steuernummern;
- Daten, die mögliche Auswirkungen auf das Ansehen/die Reputation der betroffenen Person haben;
- Daten über den geschützten inneren Lebensbereich der betroffenen Person (z.B. Tagebücher);
- Gesundheitsdaten i.S.v. Art. 4 Nr. 15 DSGVO;
- Grad der Behinderung;
- Verarbeitung von Daten mit inhärenter Intransparenz für die betroffene Person (Schätzwerte beim Scoring, Anwendung von Algorithmen);
- Einkommen;
- Sozialleistungen;
- Steuern;
- Ordnungswidrigkeiten;
- Daten über Mietverhältnisse;
- Patientenverwaltungsdaten (mit Ausnahme von besonders sensiblen Diagnosedaten und dergleichen);
- Arbeitszeitzeitdaten;
- Mitgliederverzeichnisse;
- Melderegister;
- Zeugnisse und Prüfungsergebnisse;
- Versicherungsdaten;
- Personalverwaltungsdaten aus Beschäftigungsverhältnissen (mit Ausnahme von dienstlichen Beurteilungen und beruflicher Laufbahn);
- Verkehrsordnungswidrigkeiten;
- einfache Bewertungen von eher geringer Bedeutung (z.B. Ja/Nein-Entscheidung bei Einstufung im Mobilfunkvertrag etc.);
- Zugangsdaten zu einem Dienst;
- Kommunikationsinhalte einer Person (z.B. E-Mail-Inhaltsdaten, Brief, Telefonat);
- (genauer) Aufenthaltsort einer Person;
- Finanzdaten einer Person (z.B. Kontostand, Kreditkartennummer, einzelne Zahlung);
- Kreditauskünfte;
- Verkehrsdaten der Telekommunikation.

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

3.2.1.3 Datenarten mit sehr hohem Schutzbedarf (Schutzbedarfsklasse 3)

Daten, die eine erhebliche Aussagekraft über die Persönlichkeit und/oder die Lebensumstände einer betroffenen Person haben oder sonst für die Verhältnisse der betroffenen Person von erheblicher Bedeutung sind, weil sie beispielsweise von der Entscheidung oder Leistung des Datenverarbeiters unmittelbar existentiell abhängig ist. Die unbefugte Erhebung, Verarbeitung oder Nutzung solcher Daten kann zu erheblichen Nachteilen für die betroffene Person hinsichtlich ihrer gesellschaftlichen Stellung und ihren wirtschaftlichen Verhältnissen führen („Existenz“).

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

Nicht abschließende Beispiele für Daten mit sehr hohem Schutzbedarf:

- Daten, die einem Berufs-, Geschäfts-, Fernmelde- oder Mandantengeheimnis unterliegen (z.B. Patientendaten, Mandantendaten);
- Daten, deren Kenntnis eine erhebliche konkrete Schädigung der betroffenen Person oder Dritter ermöglicht (z.B. PIN, TAN im Online-Banking);
- Schulden;
- Patientendaten (besonders sensible Diagnosedaten wie Aids, Krebs, psychische Erkrankungen und dergleichen) soweit nicht Schutzbedarfsklasse 2);
- besonders sensible Sozialdaten;
- Pfändungen;
- Personalverwaltungsdaten wie dienstliche Beurteilungen, berufliche Laufbahn und dergleichen, soweit nicht Schutzbedarfsklasse 2;
- Daten über Vorstrafen und strafprozessuale Verhältnisse (z.B. Ermittlungsverfahren) einer Person und entsprechende Verdachtsmomente; Straffälligkeit;
- Besonders sensitive Gesundheitsdaten i.S.v. Art. 4 Nr. 15 DSGVO wie z.B. zu Krankheiten, deren Bekanntwerden der betroffenen Person in besonderem Maße unangenehm sind oder zu einer gesellschaftlichen der betroffenen Person führen können;
- Persönlichkeitsprofile, z.B. Bewegungsprofil, Kaufverhaltensprofil, mit erheblicher Aussagekraft über die Persönlichkeit der betroffenen Person.

3.2.2 Höherstufung (Schritt 2)

Der Schutzbedarf einer Datenverarbeitung kann sich aufgrund verschiedener Umstände erhöhen, wenn durch die Umstände eine stärkere Beeinträchtigung der Persönlichkeitsrechte der betroffenen Person zu erwarten ist. In diesem Fall ist die Einstufung in eine höhere Schutzbedarfsklasse vorzunehmen.

Weiterhin gilt zu beachten, dass in dem Fall, in dem sich aufgrund der unten aufgeführten Umstände der Schutzbedarf erhöht, sich auch regelmäßig das Missbrauchsrisiko erhöhen wird, da sich dieses nicht allein nach der Art der Daten, sondern auch nach den Umständen der Datenverarbeitung bestimmt.

Beispiel: Die Speicherung einer großen Menge an Kreditkartendaten an einer Stelle kann diese Daten zu einem lohnenden Angriffsziel für Kriminelle machen, sodass durch den Umstand, dass Daten in großer Menge verarbeitet werden, das Missbrauchsrisiko steigt. Schließlich ist der Zugriff auf eine große Menge an Kreditkartendaten für Kriminelle „lohnender“ ist als nur der Zugriff auf wenige Daten. Die Gefährdung für alle gespeicherten Kreditkartendaten steigt.

Umstände, die zur Höherstufung führen können, sind insbesondere:

- Verwendungskontext von Daten;
- Verkettung von Daten;
- Menge an Daten;

- Anzahl betroffener Personen;
- Kumulierung vieler Rechte;
- automatisierte Entscheidungsfindung;
- Einsatz von hochkomplexer und stark miteinander vernetzter Technik;
- keine Kotrollmöglichkeiten für betroffene Personen.

→ **Verwendungskontext von Daten**

Der Verwendungskontext von Daten kann zu höherem Schutzbedarf führen, soweit damit eine erheblich erhöhte Aussagekraft der Daten über die Persönlichkeit der betroffenen Person einhergeht oder die unberechtigte Verwendung konkrete Nachteile für die betroffene Person haben kann.

Beispiel: Die Verwendung des Namens in einem (allgemeinen) Telefonbuch begründet regelmäßig keine gesteigerte Aussagekraft. Die Verwendung in der Patientenliste eines Arztes durchaus, unter Umständen sogar erheblich.

Beispiele für schutzbedarfserhöhende Verwendungskontexte sind:

- Datenart: Name, Anschrift;
- Verwendungskontext: Führungszeugnis; Täterlichtbilddatei, Strafakte, Beschäftigtenscreening, Personalakte.

→ **Verkettung von Daten**

Die Verkettung von Daten bezeichnet die Verknüpfung von Daten mit anderen Daten, um dadurch neue Aussagen zu gewinnen. Die Verkettung kann zu höherem Schutzbedarf führen, soweit mit dieser eine erheblich erhöhte Aussagekraft der Daten über die Persönlichkeit der betroffenen Person einhergeht. Dies gilt auch dann, wenn ein Datum mit anderen Daten derselben oder einer niedrigeren Schutzbedarfsklasse verknüpft wird.

Beispiel: Die Verknüpfung von Daten über den Kauf von Produkten (Schutzbedarfsklasse 2) und ggf. weiterer Daten derselben oder anderer Art, etwa Aufenthaltsort (Schutzbedarfsklasse 2), kann je nach Anzahl der Daten zu einem genauen Persönlichkeitsprofil führen. Ein solches Persönlichkeitsprofil kann in Schutzbedarfsklasse 3 einzustufen sein.

Beispiele für schutzbedarfserhöhende Verkettbarkeit von Daten sind:

- Aufenthaltsortdaten, die konkret zu einem Bewegungsprofil zusammengeführt werden können (die Zusammenführung ist in der konkreten Situation möglich und naheliegend).

→ **Menge von Daten**

Schon aufgrund der schieren Menge an Daten kann ein gesteigertes Interesse an unbefugter Verarbeitung und Nutzung der Daten bestehen, sodass eine höhere Gefahr der unbefugten Verarbeitung und Nutzung auch in Bezug auf jedes einzelne Datum besteht. Der Schutzbedarf von Daten kann sich daher erhöhen, wenn sie in großer Menge verarbeitet werden.

Beispiel: Die Speicherung einer großen Menge an Kreditkartendaten an einer Stelle kann diese Daten zu einem lohnenden Angriffsziel für Kriminelle machen, so dass die Wahrscheinlichkeit eines Angriffs steigt. Damit steigt die Gefährdung für alle dort gespeicherten Kreditkartendaten.

Beispiele für schutzbedarfserhöhende Zusammenfassung von Daten sind:

- Sammlung großer Mengen Bank- und Kreditkartendaten.
- Sammlung von Daten aus Videoüberwachungsanlagen

→ **Anzahl betroffener Personen**

Häufig geht mit einer großen Menge an Daten auch eine große Anzahl an betroffenen Personen einher. Schutzerhöhend kann sich jedoch auch auswirken, wenn zwar keine großen Datenmengen verarbeitet werden, aber von der Verarbeitung eine große Anzahl Personen betroffen ist.

→ **Kumulierung vieler Rechte**

Weiterhin kann sich der Schutzbedarf von Daten erhöhen, wenn diese von Personen verarbeitet werden, die zu verschiedenen Zwecken unterschiedliche Rollen mit unterschiedlichen Rechten wahrnehmen und somit das Ausmaß der Verfügungsgewalt über die Daten bei diesen Personen steigt

Beispiel: Der Administrator eines Online-Dienstes bekommt aufgrund der Vielzahl seiner Rechte ein umfassendes Bild von der betroffenen Person, deren Daten er administriert.

→ **Automatisierte Entscheidungsfindung**

Der Schutzbedarf von Daten kann sich zudem erhöhen, wenn die Verarbeitung von Daten zu einer automatisierten Entscheidungsfindung führen soll, die gegenüber der betroffenen Person eine rechtliche Wirkung entfaltet oder die die betroffene Person in ähnlicher Weise erheblich beeinträchtigt, ohne dass die betroffene Person Einfluss auf die Entscheidung ausüben kann.

Beispiel:

Die Vorauswahl der Bewerber für die Besetzung einer ausgeschriebenen Stelle wird automatisiert durch Algorithmen vorgenommen, ohne dass ein Personalsachbearbeiter die Auswahl überprüft.

→ **Einsatz von hochkomplexer und stark miteinander vernetzter Technik**

Der Schutzbedarf von Daten kann sich zudem erhöhen, wenn bei der Verarbeitung eine hochkomplexe und stark miteinander vernetzte Technik eingesetzt werden soll, da durch die Vernetzung der einzelnen Komponenten zusätzliche Angriffsflächen für Cyber-Attacken geschaffen werden. Zudem umspannt vernetzte Technik nicht selten unterschiedliche Lebensbereiche des Nutzers und liefert daher Informationen mit sehr hoher Aussagekraft über die persönlichen und sachlichen Verhältnisse von betroffenen Personen, deren unbefugte Kenntnisnahme ernsthafte Nachteile für diese mit sich bringen kann.

Beispiel: Smarthome-Anwendungen können aus vielen datenverarbeitenden Komponenten wie bspw. smarten Bewegungsmeldern, Überwachungskameras, Heizungs- und Klimaanlagen, Zugangs- und Aufzugssteuerungselementen bestehen. Der unbefugte Zugang zu Daten aus Bewegungsmeldern gibt Aufschluss über die Anwesenheit von Bewohnern und kann als Grundlage für die Planung von Einbrüchen dienen.

→ **Keine Kontrollmöglichkeiten für betroffene Personen**

Der Schutzbedarf von Daten kann sich weiterhin erhöhen, wenn der betroffenen Person keine Möglichkeit einer unmittelbaren Kontrolle über ihre Daten ermöglicht wird, sodass die Datenverarbeitungsvorgänge keine Interventions- oder Selbstschutzmöglichkeiten für die betroffenen Personen bieten.

3.2.3 Herabstufung (Schritt 3)

Der Schutzbedarf einer Datenverarbeitung kann sich aufgrund verschiedener Umstände verringern, soweit aufgrund der Umstände oder bestimmter Maßnahmen die Gefahr eines Eingriffs oder der Aussagewert der Daten vermindert wird. Der somit verringerte Schutzbedarf kann, je nach Umfang des erreichten Schutzbedarfs, zur Einstufung in eine niedrigere Schutzbedarfsklasse führen.

Beispiel: Bei (wirksamer) Pseudonymisierung der Daten wird der Aussagewert für jeden, der die Zuordnungsregel nicht kennt, wesentlich herabgesetzt. Umstände, die zur Herabstufung führen können, sind insbesondere:

- Informationsgehalt und Verwendungskontext;
- Verschlüsselung von Daten (Art. 32 Abs. 1 lit. a DSGVO);
- Pseudonymisierung von Daten (Art. 4 Nr. 5 und Art. 32 Abs. 1 lit. a DSGVO);

Hinweis: Verschlüsselung und Pseudonymisierung von Daten sind zugleich Maßnahmen, die zum Schutz personenbezogener Daten eingesetzt werden. Sowohl Verschlüsselung als auch Pseudonymisierung haben damit eine doppelte Bedeutung: Sie beeinflussen aus Sicht des Cloud-Anbieters den Schutzbedarf von Daten. So haben Daten einen geringeren Schutzbedarf, wenn sie dem Cloud-Anbieter pseudonymisiert oder verschlüsselt zur Verfügung gestellt werden. Unabhängig davon gehören Verschlüsselung und Pseudonymisierung zu den Maßnahmen, die vom Cloud-Anbieter zum Schutz der Daten gegen Zugriffe Unbefugter eingesetzt werden können.

→ **Informationsgehalt und Verwendungskontext**

Daten können aufgrund ihres Informationsgehaltes und ihres Verwendungskontextes eine geringere Aussagekraft über die persönlichen und sachlichen Verhältnisse der betroffenen Person haben, als sie der abstrakten Einstufung der Datenart nach entspricht.

Beispiel: Die Terminvereinbarung eines Patienten beim Hausarzt oder Zahnarzt ist in die Datenart Gesundheitsdatum einzustufen. Da die bloße Termininformation keine erhebliche Aussagekraft über die Persönlichkeit und/oder Lebensumstände der betroffenen Person hat, entspricht der Schutzbedarf anderen Aufenthaltsdaten. Dies ist jedoch nicht der Fall bei einer Terminvereinbarung bei einem Facharzt (z.B. Onkologe), weil diese erhebliche Rückschlüsse auf mögliche Krankheiten der betroffenen Person ermöglicht.

→ **Verschlüsselung von Daten**

Verschlüsselung von Daten ist das Verändern personenbezogener Daten derart, dass ohne Entschlüsselung die Kenntnisnahme des Inhalts der Daten nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist.

Hinweis: Die Verschlüsselung von Daten wirkt sich nur dann schutzbedarfsmindernd aus, wenn sie durch den Cloud-Nutzer vor der Übergabe der Daten an den Cloud-Anbieter vorgenommen wird. Diese Verschlüsselung ist daher von der Verschlüsselung gespeicherter Daten als Schutzanforderung nach Nr. 2.9 des AUDITOR-Kriterienkatalogs zu unterscheiden

→ **Pseudonymisierung von Daten**

Pseudonymisierung bezeichnet „die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden“ (Art. 4 Nr. 5 DSGVO).

Hinweis: Die Pseudonymisierung von Daten wirkt sich nur dann schutzbedarfsmindernd aus, wenn sie durch den Cloud-Nutzer vor der Übergabe der Daten an den Cloud-Anbieter vorgenommen wird. Diese Pseudonymisierung ist daher von der Pseudonymisierung als Schutzanforderung nach Nr. 2.7 des AUDITOR-Kriterienkatalogs zu unterscheiden

3.3 Schutzanforderungsklassen

Die Schutzanforderungsklassen dienen dazu, die technischen und organisatorischen Maßnahmen festzulegen, die dazu geeignet sind, die Gewährleistungsziele für die jeweilige Schutzklasse zu erreichen und damit die Rechte und Freiheiten der betroffenen Personen in Bezug auf die jeweiligen Risiken des Dienstes angemessen zu schützen. Je größer die Risiken, desto höher ist der Gewährleistungsbedarf.

Wichtig ist, dass bei der Festlegung der Maßnahmen neben der Art der Daten, die verarbeitet werden, auch die beteiligten technischen Systeme (Hardware, Software und Infrastruktur) sowie ihre Schnittstellen und die technischen und organisatorischen (inklusive der personellen) Prozesse der Verarbeitung von Daten mit den Systemen berücksichtigt werden, da die Systeme und Prozesse, die mit der konkreten Datenverarbeitung verknüpft sind, den Schutzbedarf der Daten erben.

Wichtig ist zudem, dass die festgelegten Maßnahmen selbst die Gewährleistungsziele einhalten müssen.

Beispiel: Bei der Speicherung von Protokollierungsdaten müssen die Protokolle verfügbar, integritätsgeschützt, vor unbefugtem Zugriff gesichert sein und einer gesonderten Zweckbindung unterliegen.

3.3.1 Schutzanforderungsklasse 1

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

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

Hinweis: Im Anhang des Standard-Datenschutzmodells[1] soll künftig ein Katalog von Maßnahmen für normalen Schutzbedarf bereitgestellt werden. Die Maßnahmen sollen als Referenzen genutzt werden können, um Risiken einzudämmen und die Gewährleistungsziele zu erreichen. Der Maßnahmenkatalog befindet sich derzeit in der Erarbeitungsphase. Die ersten Bausteine des Katalogs sind inzwischen veröffentlicht.[2] Sie sind jedoch noch nicht in der Datenschutzkonferenz abgestimmt worden, sondern befinden sich in der Erprobungsphase.

3.3.2 Schutzanforderungsklasse 2

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

Ein hoher Schutzbedarf erfordert nicht immer die Implementierung einer Vielzahl von zusätzlichen Maßnahmen. In vielen Fällen genügt es, die Wirkung einer Maßnahme zu erhöhen, soweit diese einen Ansatzpunkt für eine solche Skalierung bietet. Die Verwendung längerer kryptographischer Schlüssel oder der Einsatz einer Zwei-Faktor-Authentifizierung oder von Hardware-Token dienen hier als Beispiele. Weiterhin kann eine Anpassung dadurch erfolgen, dass mit größerer Zuverlässigkeit eine spezifikationsgerechte Ausführung der Maßnahme sichergestellt wird. Dazu müssen mögliche Störeinflüsse bestimmt und die Robustheit der Maßnahmen durch zusätzliche Vorkehrungen – oft organisatorischer Natur – erhöht werden.

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

Hinweis: Im Anhang des Standard-Datenschutzmodells[3] soll künftig ein Katalog von Maßnahmen für hohen Schutzbedarf bereitgestellt werden. Die Maßnahmen sollen als Referenzen genutzt werden können, um Risiken einzudämmen und die Gewährleistungsziele zu erreichen. Der Maßnahmenkatalog befindet sich derzeit in der Erarbeitungsphase. Die ersten Bausteine des Katalogs sind inzwischen veröffentlicht.[4] Sie sind jedoch noch nicht in der Datenschutzkonferenz abgestimmt worden, sondern befinden sich in der Erprobungsphase.

3.3.3 Schutzanforderungsklasse 3

Der Cloud-Anbieter muss über die technischen und organisatorischen Maßnahmen der Schutzanforderungsklassen 1 und 2 hinaus risikoangemessene technische und organisatorische Maßnahmen erreichen, um die Daten, insbesondere gegen Vernichtung, Verlust, Veränderung, unbefugten Zugang und unbefugte Offenlegung zu schützen.

Die Maßnahmen müssen geeignet sein, um solche Vorgänge aufgrund technischer oder organisatorischer Fehler, einschließlich Bedienfehler, oder fahrlässiger oder vorsätzlicher Handlungen hinreichend

[1] Das Standard-Datenschutzmodell, V. 1.1 – Erprobungsfassung, abrufbar unter: https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methode_V1.1.pdf.
[2] Die Bausteine sind abrufbar unter: https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/.
[3] Das Standard-Datenschutzmodell, V. 1.1 – Erprobungsfassung, abrufbar unter: https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methode_V1.1.pdf.
[4] Die Bausteine sind abrufbar unter: https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/.

sicher auszuschließen. Dazu gehört insbesondere ein hinreichender Schutz gegen bekannte Angriffsszenarien sowie Verfahren zur Erkennung von Missbräuchen. Jeder Eingriff muss nachträglich festgestellt werden können.