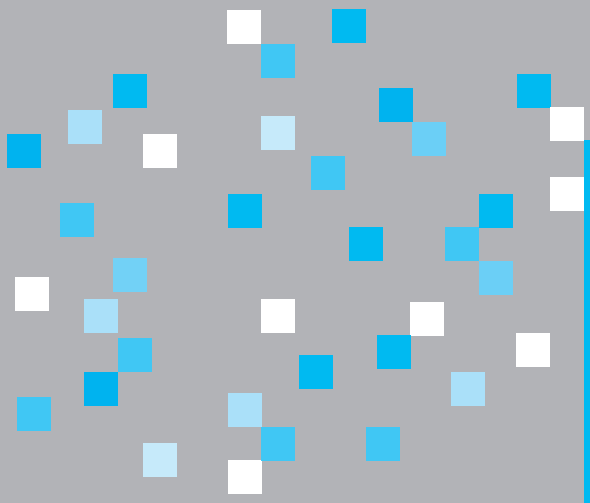
Trusted Cloud



Pilotprojekt Datenschutz-Zertifizierung für Cloud-Dienste

Schutzklassenkonzept für die Datenschutz-Zertifizierung nach TCDP Version 1.0

Pilotprojekt „Datenschutz-Zertifizierung für Cloud-Dienste“

Das Pilotprojekt „Datenschutz-Zertifizierung für Cloud-Dienste“ wurde von November 2013 bis April 2015 (Phase 1) und von September 2015 bis September 2016 (Phase 2) im Auftrag des Bundesministeriums für Wirtschaft und Energie (BMWi) durchgeführt.[1]

Am Pilotprojekt sind alle maßgeblichen Interessenvertreter beteiligt. Dazu gehören insbesondere Datenschutzbehörden und Privatwirtschaft, insbesondere Anbieter und Nutzer von Cloud-Diensten und Verbände, sowie Stellen mit Erfahrung in der Normung und Zertifizierung von IT-Diensten.

1 Informationen zum Pilotprojekt sind abrufbar unter www.tcdp.de.

Inhalt

1 Die datenschutzrechtliche Compliance-Zertifizierung

Im Rahmen der Datenschutz-Zertifizierung sind Schutzklassen ein wichtiges Instrument, um individuellen Schutzbedarf und dessen Erfüllung durch zertifizierte Dienste praxisgerecht auszudrücken.

Die datenschutzrechtliche Zertifizierung von Datenverarbeitungsdiensten soll dem Nutzer eines solchen Dienstes Rechtssicherheit verschaffen. Der Nutzer eines Datenverarbeitungsdienstes, etwa eines Cloud-Dienstes, der diese Dienstleistung auf der Grundlage einer Auftragsdatenverarbeitung in Anspruch nimmt, ist datenschutzrechtlich die verantwortliche Stelle und muss den Anbieter des Dienstes sorgfältig auswählen und sich vergewissern, dass der Anbieter die gesetzlichen Anforderungen, insbesondere an die technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit, erfüllt.

Die damit verbundene Kontrolle des Auftragnehmers wird erheblich erleichtert, wenn der betreffende Dienst über ein datenschutzrechtliches Compliance-Zertifikat (Testat) einer geeigneten Zertifizierungsstelle verfügt, welches die vom Nutzer betriebene Datenverarbeitung abdeckt. Im Folgenden wird für dieses Zertifikat bzw. Testat der Begriff „Datenschutz-Zertifikat“ verwendet.

In diesem Fall darf der Nutzer auf das Zertifikat vertrauen und muss insbesondere nicht selbst die Eignung der technischen und organisatorischen Maßnahmen überprüfen. Die „AG Rechtsrahmen des Cloud Computing“ hat in ihrem Thesenpapier die Elemente einer solchen datenschutzrechtlichen Compliance-Zertifizierung für Cloud-Dienste beschrieben.[2] Das Pilotprojekt „Datenschutz-Zertifizierung für Cloud-Dienste“[3] erarbeitet zentrale Grundlagen der Zertifizierung, insbesondere das „Trusted Cloud-Datenschutzprotokoll für Cloud-Dienste (TCDP)“ sowie eine Verfahrensordnung für TCDP-Zertifizierungen.

Das TCDP, das im September 2016 in der Version 1.0[4] veröffentlicht wird, setzt die Anforderungen des BDSG in prüffähige Normen um. Das TCDP setzt dabei auf die Konkretisierung von Anforderungen nach Schutzklassen. Grundlage und Ausgestaltung der Schutzklassen sind in diesem Schutzklassenkonzept beschrieben.

Die Datenschutz-Grundverordnung (DSGVO) enthält eine Regelung zur Zertifizierung. Die Zertifizierung nach TCDP entspricht den Prinzipien, die der Regelung der DSGVO zugrundeliegen. Es wird daher angestrebt, die TCDP-Zertifizierung zu einer Datenschutz-Zertifizierung auf der Grundlage der DSGVO weiterzuentwickeln. Dabei sollen TCDP-Zertifikate in einem vereinfachten Verfahren in Zertifikate nach DSGVO überführt werden können.

Das TCDP-Schutzklassenkonzept kann als Grundlage für ein Schutzklassenkonzept einer künftigen Zertifizierung nach DSGVO dienen.

Nachfolgend wird die Bedeutung von Schutzklassen im Rahmen einer Datenschutz-Zertifizierung dargestellt (2) und sodann die im Rahmen des Schutzklassenkonzepts verwendeten Schutzklassen beschrieben (3).

2 AG Rechtsrahmen des Cloud Computing, „Datenschutzrechtliche Lösungen für Cloud Computing. Ein rechtspolitisches Thesenpapier“, 2012, abrufbar unter www.tcdp.de.
3 Siehe zum Pilotprojekt unter www.tcdp.de.
4 Trusted Cloud-Datenschutzprofil für Cloud-Dienste (TCDP) 1.0, abrufbar unter www.tcdp.de.

2 Berücksichtigung individueller Datenschutz- und Sicherheitsanforderungen durch Schutzklassen

2.1 Zertifizierung und individueller Maßstab für Datenschutz und Sicherheit

Im Zentrum der Datenschutz-Zertifizierung steht das Zertifikat, das von einer Zertifizierungsstelle für einen bestimmten Datenverarbeitungsdienst, etwa einem Cloud-Dienst, ausgestellt wird.

Das Zertifikat soll Nutzer des Dienstes darüber informieren, ob ein bestimmter Dienst die für die von ihm gewünschte Datenverarbeitung maßgeblichen Anforderungen an die technischen und organisatorischen Maßnahmen erfüllt.

Entsprechend enthält das Zertifikat die Erklärung der Zertifizierungsstelle, dass ein bestimmter Dienst, etwa ein Cloud-Dienst, den datenschutzrechtlichen Anforderungen auf Seiten des Auftragnehmers einer Auftragsdatenverarbeitung entspricht. Ein wesentliches Element der gesetzlichen Anforderungen sind die vom Auftragnehmer zu erbringenden technischen und organisatorischen Maßnahmen zur Gewährleistung der IT-Sicherheit.

Eine wesentliche Herausforderung der Zertifizierung liegt in dem Umstand, dass die gesetzlichen Anforderungen (§ 9 BDSG) an die technischen und organisatorischen Maßnahmen ein individueller Maßstab sind: Die Anforderungen an die technischen und organisatorischen Maßnahmen richten sich nach dem Schutzbedarf der jeweiligen Datenverarbeitung. Die jeweilige Datenverarbeitung und der daraus folgende individuelle Schutzbedarf aber, werden nicht vom Diensteanbieter, etwa dem Cloud-Anbieter, sondern vom Nutzer des Dienstes, etwa dem Cloud-Nutzer, festgelegt.

Da die Zertifizierung vor der Inanspruchnahme des Dienstes vom Diensteanbieter und nicht für einen spezifischen Nutzer, sondern für die Gesamtheit der künftigen Nutzer des Dienstes betrieben werden soll, kann sich die Zertifizierung nicht auf einen konkreten Datenverarbeitungsvorgang eines bestimmten Nutzers beziehen.

2.2 Das Schutzklassenkonzept

Diese Schwierigkeit kann durch ein Schutzklassenkonzept gelöst werden. In einem Schutzklassenkonzept wird die Eignung eines Dienstes für ein bestimmtes Niveau von Sicherheitsanforderungen, das durch eine Schutzklasse bestimmt wird, geprüft und im Zertifikat zum Ausdruck gebracht. Der Nutzer des Dienstes kann seinen individuellen Schutzbedarf in die Schutzklassen einordnen und einen Dienst wählen, dessen Datenschutz- und Sicherheitsniveau der von ihm benötigten Schutzklasse entspricht.

Die Schutzklasse nimmt damit eine Doppelfunktion ein. Zum einen beschreibt sie den Schutzbedarf der Datenverarbeitungsvorgänge, und zum anderen bestimmt sie die Anforderungen an die technischen und organisatorischen Maßnahmen, deren Erfüllung der Diensteanbieter gewährleisten muss.

Um diese Doppelfunktion deutlich zu machen, wird hier zwischen Schutzbedarfsklassen und Schutzanforderungsklassen unterschieden.

Die **Schutzbedarfsklasse** beschreibt den Schutzbedarf für Datenverarbeitungsvorgänge anhand genereller Merkmale.

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

Es ist dabei nicht erforderlich, jede gesetzliche Anforderung einer bestimmten Schutzanforderungsklasse zuzuordnen. Eine Reihe von datenschutzrechtlichen Anforderungen an die Auftragsdatenverarbeitung ist vom Schutzbedarf unabhängig. So ist etwa die Bindung des Auftragnehmers an die Weisungen des Auftraggebers eine allgemeine gesetzliche Anforderung an die Auftragsdatenverarbeitung, die vom Schutzbedarf des jeweiligen Datenverarbeitungsvorgangs weitgehend unabhängig ist.

Unterschiedliche Anforderungen sind vielmehr zu formulieren, soweit ein unterschiedlicher Schutzbedarf zu unterschiedlichen Anforderungen an technische und organisatorische Maßnahmen führt.

In einem Schutzklassenkonzept muss gewährleistet sein, dass der individuelle Schutzbedarf der Datenverarbeitung durch die technischen Anforderungen der betreffenden Schutzanforderungsklasse abgedeckt ist.

Diese Forderung wird trotz der Generalisierung, die mit einer Bildung von Schutzbedarfsklassen verbunden ist, erfüllt, wenn die Schutzanforderungen so definiert werden, dass sie den höchsten individuellen Schutzbedarf in der korrespondieren Schutzbedarfsklasse abdecken.

In diesem Fall ist gesichert, dass für alle individuellen Schutzbedarfe in der jeweiligen Schutzbedarfsklasse hinreichende Schutzanforderungen gelten. Zugleich führt diese Maßgabe dazu, dass regelmäßig höhere Schutzanforderungen gestellt werden, als es dem individuellen Schutzbedarf einer Datenverarbeitung entspricht. Der Anbieter eines zertifizierten Dienstes wird also regelmäßig ein höheres Maß an Schutzanforderungen erfüllen, als es dem individuellen gesetzlichen Bedarf des Datenverarbeitungsvorganges entspricht. Dieser Effekt wird durch die Formulierung mehrerer Schutzklassen mit unterschiedlichen Anforderungen freilich stark gemindert.

Festzuhalten ist, dass die Schutzklassenbildung sicherstellt, dass für jeden individuellen Schutzbedarf ein hinreichendes Maß an Schutz besteht, soweit der Dienst die Anforderungen der betreffenden Schutzanforderungsklasse erfüllt.

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 zugeordnet werden kann.

Dies ist grundsätzlich möglich. Erforderlich ist insoweit, dass Schutzbedarfsklassen so definiert werden, dass sie jeden individuellen Schutzbedarf abdecken und insbesondere keine Lücken entstehen. Weiterhin müssen die Schutzklassen mit Merkmalen beschrieben werden, die den Schutzbedarf des konkreten Datenverarbeitungsvorgangs widerspiegeln.

Die Beschreibung muss es ermöglichen, dass der Nutzer des Dienstes den Schutzbedarf seiner Datenverarbeitung den Merkmalen der Schutzklasse zuordnen kann.

Ausgangspunkt für die Bestimmung der Schutzbedarfsklassen ist der Schutzbedarf von Datenverarbeitungsvorgängen. Dieser bestimmt sich gemäß § 9 BDSG anhand mehrerer Faktoren. Maßgeblich sind insbesondere die allgemeine Sensitivität der Daten nach ihrer Datenart sowie Umstände, die den Schutzbedarf der Datenverarbeitung erhöhen oder absenken. Dabei ist die Gefährdung, insbesondere die Wahrscheinlichkeit von Eingriffen Unbefugter oder Missbrauch, von besonderer Bedeutung. So sind etwas Passwörter besonders gefährdet, wenn sie Zugang zu wirtschaftlichen Vorteilen sichern, wie es etwa bei PIN und TAN im Online Banking der Fall ist, die erfahrungsgemäß hoher Angriffsintensität ausgesetzt sind.

Es ist somit für jeden Datenverarbeitungsvorgang ein individueller Schutzbedarf anhand der Datenart und weiterer Umstände zu bestimmen. Dabei können durchaus eine Vielzahl an Umständen von Bedeutung sein, aufgrund derer sich eine mitunter komplexe Bestimmung des konkreten Schutzbedarfs ergeben kann.

Dies hindert jedoch die Bildung von Schutzklassen nicht. Erforderlich ist lediglich, dass sich jeder individuelle Schutzbedarf einer Schutzbedarfsklasse zuordnen lässt. Entscheidend hierfür ist, neben der Lückenlosigkeit der Schutzbedarfsklassen, dass alle für die Ermittlung des individuellen Schutzbedarfs maßgeblichen Umstände berücksichtigt werden können. Dies ist, soweit der Schutzbedarf der Schutzbedarfsklasse in allgemeiner Form beschrieben wird, stets gegeben.

Eine lediglich allgemeine Beschreibung des Schutzbedarfs führt zu der Gefahr, dass die Zuordnung des individuellen Schutzbedarfs zu einer Schutzklasse allein von den Einschätzungen des jeweiligen Nutzers des Dienstes abhängig ist und es daher zu unterschiedlichen Einschätzungen des Nutzers kommt. Dies kann zu erheblicher Rechtsunsicherheit führen und die Nutzung der Zertifizierung beeinträchtigen.

Beispiel: Der Nutzer eines Cloud-Dienstes muss bestimmen, welchen Schutzbedarf die Datenverarbeitung, die er in einem Cloud-Dienst ausführen will, aufweist.

Das Schutzklassenkonzept enthält daher auch eine Systematik der Ermittlung des Schutzbedarfs. Diese Systematik hat die Aufgabe, die theoretisch mehrdimensionale Ermittlung des individuellen Schutzbedarfs anhand der relevanten Faktoren in einem vereinfachten und damit praxisgerechten Verfahren abzubilden. Die Vereinfachung ist möglich, weil es für die Zwecke der Datenschutz-Zertifizierung nicht erforderlich ist, den individuellen Schutzbedarf genau zu bestimmen. Vielmehr ist es lediglich notwendig, die maßgebliche Schutzklasse zu ermitteln.

2.3.2 Die Schritte zur Ermittlung des Schutzbedarfs eines Datenverarbeitungsvorgangs

Ausgangspunkt der Systematik ist, wie generell bei der Ermittlung des Schutzbedarfs, 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/Daten, etwa gesundheitsbezogene Daten, einen wesentlich erhöhten Einfluss auf die Persönlichkeitsrechte des Betroffenen haben können.

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. Es kommt aber auch eine Höherstufung um zwei Schutzbedarfsklassen in Betracht. Als Zwischenergebnis dieser Prüfung ist eine Einstufung der Datenverarbeitung in eine Schutzbedarfsklasse zu treffen.

Im dritten Schritt ist zu prüfen, ob schutzbedarfsmindernde Umstände vorliegen. Diese können dazu führen, dass die Datenverarbeitung 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, die etwa in einem Host-Dienst gespeichert werden sollen.

Auch in diesem dritten Schritt ist nicht eine konkrete Bestimmung des individuellen Schutzbedarfs der Datenverarbeitung notwendig. Maßgeblich ist vielmehr, ob aufgrund der schutzbedarfsmindernden Umstände eine Herabstufung des Schutzbedarfs erfolgt. 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 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 schwierig sein. In diesen Fällen kann sich der Betreiber der Datenverarbeitung dadurch absichern, dass er in Zweifelsfällen die höhere der in Betracht kommenden Schutzbedarfsklasse wählt:

Beispiel: Ein Cloud-Nutzer ist unsicher, ob seine Datenverarbeitung in die Schutzbedarfsklasse 1 oder 2 einzuordnen ist. Um Risiken wegen einer unzutreffenden Einordnung zu vermeiden, sollte er von der höheren Schutzbedarfsklasse 2 ausgehen.

2.3.3 Zusammenfassung: Die Ermittlung der maßgeblichen Schutzbedarfsklasse

Der Schutzbedarf eines konkreten Datenverarbeitungsvorgangs wird in einem dreistufigen Verfahren ermittelt:

- Im **ersten Schritt** wird der abstrakte Schutzbedarf der zu verarbeitenden Daten nach der Datenart bestimmt.
- Im **zweiten Schritt** ist zu prüfen, ob sich der Schutzbedarf aufgrund konkreter Umstände der Datenverarbeitung erhöht.
- Im **dritten Schritt** ist zu prüfen, ob der Schutzbedarf aufgrund konkreter Umstände sinkt.
- Im Ergebnis wird der Schutzbedarf der konkreten Datenverarbeitung in eine Schutzbedarfsklasse eingeordnet.

2.4 Schutzanforderungsklassen für technische und organisatorische Maßnahmen

Entsprechend dem Ziel des Schutzklassenkonzepts müssen für jede Schutzbedarfsklasse korrespondierende Schutzanforderungen definiert werden, die in den Schutzbedarfsklassen festgelegt werden.

Daher ist es erforderlich, die Schutzanforderungen anhand abstrakter Merkmale zu beschreiben, so dass die Anforderungen durch verschiedene technische und organisatorische Maßnahmen erfüllt werden können.

Bei der Gestaltung des Dienstes, etwa eines Cloud-Dienstes, kann der Diensteanbieter die von ihm zu treffenden Maßnahmen im Hinblick auf die verschiedenen Schutzanforderungsklassen wählen. Im Rahmen der Zertifizierung des Dienstes wird geprüft, ob die Maßnahmen die Anforderungen einer bestimmten Schutzanforderungsklasse erfüllen. Die Zertifizierung wird für eine bestimmte Schutzanforderung erstellt, erklärt also, dass die Anforderungen einer bestimmten Schutzanforderungsklasse erfüllt sind.

Dies gilt grundsätzlich für jede technische und organisatorische Maßnahme. Jedoch ist nicht für jede gesetzliche Anforderung an die Auftragsdatenverarbeitung eine Differenzierung nach Schutzanforderungsklassen erforderlich. So ist etwa die Bindung des Diensteanbieters an die Weisungen des Nutzers eine gesetzliche Anforderung, die vom Schutzbedarf unabhängig ist. Entsprechend erfolgt insoweit keine Differenzierung nach Schutzklassen. Entsprechendes gilt für die gesetzlichen Anforderungen an den Vertrag über Auftragsdatenverarbeitung.

Die Anforderungen an die technischen und organisatorischen Maßnahmen lassen sich nicht im Wege eines Katalogs zuordnen. Es ist beispielsweise nicht möglich, im Rahmen des Zugangsschutzes den Schutzbedarf durch Passwort pauschal einer bestimmten Schutzanforderungsklasse zuzuordnen, da die Nutzung von Passwörtern je nach der Ausgestaltung und den Umständen des Falles sehr unterschiedlichen Sicherheitsanforderungen genügt. 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 Zertifizierungsstellen bzw. Prüfern vorgenommen wird.

Zur Sicherung einer einheitlichen Prüfung und Zertifizierung, wie sie im Konzept der „AG Rechtsrahmen des Cloud Computing“ für den gesamten EU-Binnenmarkt angestrebt wird, reicht daher ein Schutzklassenkonzept alleine nicht aus. Vielmehr ist es notwendig, einen einheitlichen Anforderungskatalog auf der Grundlage der gesetzlichen Anforderungen zu formulieren, der eine Differenzierung soweit wie möglich vornimmt.

2.5 Anzahl von Schutzklassen

Für die Bildung von Schutzklassen ist es wesentlich festzulegen, wie viele Schutzklassen definiert werden sollen. Insoweit sind mehrerer Aspekte von Bedeutung.

→ So wenig Schutzklassen wie möglich

Die Zuordnung eines individuellen Schutzbedarfs oder einer technischen Schutzmaßnahme zu einer Schutzklasse muss möglichst einfach und eindeutig sein, um die Datenschutz-Zertifizierung für Anbieter und Nutzer von Diensten handhabbar zu machen. Daher sind so wenige Schutzklassen wie möglich zu bilden.

→ So viele Schutzklassen wie für eine sinnvolle Differenzierung notwendig

Ein Mindestmaß an Differenzierung ist sowohl für Anbieter als auch für Nutzer von Diensten erforderlich, um effiziente Dienste anbieten zu können. Bei zu geringer Differenzierung besteht die Gefahr, dass unangemessen hohe Anforderungen an die technischen und organisatorischen Schutzmaßnahmen gestellt werden und dadurch Kosten verursacht werden, die angesichts des tatsächlich bestehenden Schutzbedarfs nicht geboten wären.

Daraus folgt die Anforderung, dass so viele unterschiedliche Schutzklassen gebildet werden, dass unterschiedliche Niveaus an Schutzbedarf und -anforderungen, die durch unterschiedliche Maßnahmen mit jeweils unterschiedlichen Kosten berücksichtigt werden können, in verschiedene Schutzklassen eingeordnet werden können.

→ Leitlinie: Differenzierung in Schutzklassen nach erheblich unterschiedlichen Anforderungen

Leitlinie für die Schutzklassenbildung, die sowohl dem Ziel einer einfachen und eindeutigen Zuordnung von individuellem Schutzbedarf zu einer Schutzbedarfsklasse, als auch der Möglichkeit einer hinreichenden Differenzierung von Angeboten entspricht, muss daher sein, dass die Zahl der Schutzklassen so zu wählen ist, dass deutlich divergierende technische und organisatorische Maßnahmen mit unterschiedlichen Kosten unterschiedlichen Schutzklassen zugordnet werden können.

→ Konzept: 3 + 2 Schutzklassen

Die genannten Anforderungen lassen sich durch ein Konzept erfüllen, dass „drei plus zwei“ Schutzklassen unterscheidet.

Kern der Unterscheidung sind dabei drei Schutzklassen, für die jeweils Schutzbedarfe (Schutzbedarfsklassen) und Schutzanforderungen (Schutzanforderungsklassen) beschrieben werden.

Dies beruht auf der Annahme, dass sich für drei Schutzklassen hinreichend deutlich unterschiedliche Anforderungen definieren lassen, und dass bei stärkerer Differenzierung zu hohe Schwierigkeiten der eindeutigen Zuordnung von Maßnahmen zu einer Schutzanforderungsklasse entstünden. Die Unterscheidung von drei Schutzklassen wiederum erscheint als das Mindestmaß der Differenzierung. Bei weniger, namentlich nur bei zwei Schutzklassen, bestünde die Gefahr, dass in sehr vielen Fällen Anforderungen erfüllt werden müssten, die erheblich über dem individuellen Schutzbedarf liegen und damit unnötige Kosten verursachen.

Zu den drei Schutzklassen werden zwei weitere Schutzklassen/ Schutzbedarfsklassen definiert, die jedoch eher eine Abgrenzungs- und Hilfsfunktion haben. Durch eine Schutzklasse, die in diesem Schutzklassenkonzept als Schutzklasse 0 bezeichnet wird, wird das Fehlen eines datenschutzrechtlichen Schutzbedarfs gekennzeichnet, das etwa bei Daten besteht, die keinen Personenbezug aufweisen und folglich nicht dem Datenschutzrecht unterliegen.

Auf der entgegengesetzten Seite des Spektrums wird eine Schutzklasse für Datenverarbeitungsvorgänge gebildet, deren Schutzbedarf nicht in einer Schutzklasse beschreiben werden kann und damit einer übergeordneten Zertifizierung auch nicht zugänglich ist. Dies betrifft insoweit Datenverarbeitungsvorgänge mit extrem hohem Schutzbedarf und individuell stark divergierenden Umständen. Diese Situation wird in diesem Konzept als Schutzklasse „drei plus (3+)“ bezeichnet.

In diesem Fall muss die verantwortliche Stelle, die Daten im Rahmen einer Auftragsdatenverarbeitung durch einen Dienstleister verarbeiten lassen möchte, selbst eine Risikoanalyse vornehmen und aufgrund dieser Analyse insbesondere die Anforderungen an die technischen und organisatorischen Maßnahmen des Diensteanbieters feststellen und sich von der Erfüllung der Anforderungen beim Diensteanbieter vergewissern.

In den Fällen der Schutzklassen 0 und 3+ beschränkt sich die Beschreibung der Schutzklassen auf die Schutzbedarfsklassen, da sich insoweit keine oder keine überindividuellen datenschutzrechtlichen Schutzanforderungen bestimmen lassen.

2.6 Die Anwendung des Schutzklassenkonzepts bei Zertifizierung und Nutzung von Diensten

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

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

Die Zertifizierungsstelle ordnet den 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 Dienstes für eine konkrete Schutzanforderungsklasse zum Ausdruck gebracht.

Der Nutzer des Dienstes ordnet den Schutzbedarf seiner konkreten Datenverarbeitung einer bestimmten Schutzbedarfsklasse zu. Dabei führt er die beschriebene Zuordnung in den genannten drei Schritten durch. Der Nutzer kann auf dieser Grundlage einen Dienst wählen, der für die betreffende Schutzklasse zertifiziert ist.

3 Die Schutzklassen

Nachfolgend werden die Schutzbedarfsklassen definiert und durch Beispiele erläutert (3.1). Sodann wird die Zuordnung des Schutzbedarfs eines Datenverarbeitungsvorgangs zu einer Schutzbedarfsklasse in einem dreistufigen Verfahren dargestellt (3.2). Dabei werden zunächst die abstrakten Schutzbedarfsklassen nach der jeweiligen Datenart definiert (3.2.1) und sodann die Faktoren, die zu einer Heraufstufung (3.2.2) oder zu einer Absenkung des Schutzbedarfs (3.2.3) führen, dargestellt. Sodann werden die Schutzanforderungsklassen beschrieben (3.3).

3.1 Schutzbedarfsklassen

3.1.1 Schutzbedarfsklasse 0

Datenverarbeitungsvorgänge (d.h. die im Cloud-Dienst nachgefragte Dienstleitung), die keine oder keine schutzbedürftigen Aussagen über persönliche Verhältnisse natürlicher Personen enthalten, erzeugen, unterstützen oder solche ermöglichen.

Beispiel: Der Cloud-Nutzer möchte reine Wetterdaten oder personenbezogene Daten, die vom Betroffenen für jede Erhebung, Verarbeitung oder Nutzung freigegeben sind, speichern.

Hinweis: Die Freigabe personenbezogener Daten schließt nicht aus, dass hinsichtlich der freigegeben Daten Erhebungs-, Verarbeitungs- oder Nutzungsverbote für bestimmte Stellen bestehen.

3.1.2 Schutzbedarfsklasse 1

Datenverarbeitungsvorgänge, die durch die einbezogenen Daten und die konkrete Erhebung, Verarbeitung oder Nutzung dieser Daten Aussagen über die persönlichen Verhältnisse des Betroffenen enthalten, erzeugen, unterstützen oder solche ermöglichen. Die unbefugte Verwendung dieser Daten kann vom Betroffenen leicht durch Aktivitäten verhindert oder abgestellt werden.

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

3.1.3 Schutzbedarfsklasse 2

Datenverarbeitungsvorgänge, die aufgrund der verwendeten Daten oder der konkreten Erhebung, Verarbeitung oder Nutzung dieser Daten eine Aussagekraft über die Persönlichkeit oder die Lebensumstände einer Person (Betroffener) haben, unterstützen oder zu einer solchen führen können oder sonst für die Verhältnisse des Betroffenen von Bedeutung sind. Die unbefugte Erhebung, Verarbeitung oder Nutzung dieser Daten kann zu einem Nachteil für den Betroffenen (Beeinträchtigung der Rechtsgüter) führen.

Beispiel: Der Cloud-Nutzer benötigt Speicherung und Verarbeitung von Bank- und Kreditkartendaten seiner Kunden. Dieser Datenverarbeitungsvorgang enthält aufgrund der Art der Daten und der Verarbeitung Aussagen über die finanziellen Verhältnisse der Vertragspartner.

3.1.4 Schutzbedarfsklasse 3

Datenverarbeitungsvorgänge, die aufgrund der verwendeten Daten oder der konkreten Erhebung, Verarbeitung oder Nutzung dieser Daten eine erhebliche Aussagekraft über die Persönlichkeit oder die Lebensumstände einer Person (Betroffener) haben, unterstützen oder zu einer solchen führen können oder sonst für die Verhältnisse des Betroffenen von erheblicher Bedeutung sind. Die unbefugte Erhebung, Verarbeitung oder Nutzung dieser Daten kann zu schwerwiegenden Nachteilen für den Betroffenen (Beeinträchtigung der Rechtsgüter) führen.

Beispiel: Der Cloud-Nutzer benötigt Speicherung von Diagnosen von Krebspatienten.

3.1.5 Schutzbedarfsklasse 3 plus

Datenverarbeitungsvorgänge, die aufgrund der verwendeten Daten oder der konkreten Verarbeitung oder Nutzung dieser Daten eine erhebliche Aussagekraft über die Persönlichkeit oder die Lebensumstände einer Person (Betroffener) haben, unterstützen oder zu einer solchen führen können oder sonst für die Verhältnisse des Betroffenen von erheblicher Bedeutung sind. Die unbefugte Erhebung, Verarbeitung oder Nutzung dieser Daten kann zu einer konkreten Gefahr für eine wesentliche Beeinträchtigung von Leben, Gesundheit oder Freiheit des Betroffenen führen.

Beispiel: Der Cloud-Nutzer benötigt Speicherung von Daten von V-Leuten des Verfassungsschutzes, was bei unbefugter Offenbarung zur Gefahr für Leib und Leben der Betroffenen führen kann.

3.2 Ermittlung des Schutzbedarfs eines Datenverarbeitungsvorgangs

Der Schutzbedarf wird in einem dreistufigen Verfahren ermittelt:

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

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

3.2.1 Schutzbedarfsklassen nach Datenart (Abstrakter Schutzbedarf – Schritt 1)

→ Daten ohne Schutzbedarf (Schutzbedarfsklasse 0)

Daten ohne Personenbezug einschließlich wirksam anonymisierter Daten sowie Daten, die vom Betroffenen wirksam „freigegeben", also zur uneingeschränkten Erhebung, Verarbeitung oder Nutzung veröffentlicht werden.

Beispiele:
- synthetisch erzeugte Testdaten („Markus Musterman");
- Wetterdaten;
- wirksam anonymisierte Daten;
- wirksam freigegebene Daten.

→ Datenarten mit normalen Schutzbedarf (Schutzbedarfsklasse 1)

Personenbezogene Daten (Einzelangaben über die persönlichen oder sachlichen Verhältnisse des Betroffenen, § 3 Abs. 1 BDSG).

Beispiele:
- Name, Anschrift (ohne Kontext) (soweit nicht Schutzbedarfsklasse 2 oder 3);
- Staatsangehörigkeit (ohne Kontext) (soweit nicht Schutzbedarfsklasse 2 oder 3);
- Telefonnummer einer natürlichen Person (soweit nicht Schutzbedarfsklasse 2 oder 3).

→ Datenarten mit hohem Schutzbedarf (Schutzbedarfsklasse 2)

Datenarten, die eine spezifische Aussagekraft über die Persönlichkeit und/oder Lebensumstände des Betroffenen haben oder sonst für die Verhältnisse des Betroffenen von Bedeutung sind. Die unbefugte Erhebung, Verarbeitung oder Nutzung solcher Daten kann zu einem Nachteil für den Betroffenen (Beeinträchtigung der Rechtsgüter) führen.

Beispiele:
- Name, Anschrift eines Vertragspartners (soweit nicht Schutzbedarfsklasse 3 oder 3+);
- Geburtsdatum;
- Kontext zu einem Vertragspartner (z.B. Gegenstand einer vereinbarten Leistung);
- Religionszugehörigkeit;
- einfache Bewertungen eher geringer Bedeutung (z.B. Ja/Nein-Entscheidung bei Einstufung im Mobilfunkvertrag etc.);

- Zugangsdaten zu einem Dienst (soweit nicht Schutzbedarfsklasse 3 oder 3+);
- Kommunikationsinhalte einer Person (z.B. E-Mail-Inhaltsdaten, Brief, Telefonat) (soweit nicht Schutzbedarfsklasse 3 oder 3+);
- (genauer) Aufenthaltsort einer Person (soweit nicht Schutzbedarfsklasse 3 oder 3+);
- Finanzdaten einer Person (z.B. Kontostand, Kreditkartennummer, einzelne Zahlung);
- 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 bedarf einer subjektiven Bewertung, die dem Äußernden obliegt. Der Umstand, dass eine einzelne Äußerung vom Äußernden als besonders schutzbedürftig eingestuft wird oder objektiv (aus Sicht eines Dritten) besonders schutzbedürftig ist, sollte aber nicht dazu führen, dass jeder Kommunikationsinhalt als besonders schutzbedürftig gilt. Insbesondere hat der Cloud-Nutzer nicht notwendig Kenntnis vom subjektiven Schutzbedarf des Äußernden (**Beispiel:** Ein Cloud-Nutzer bucht einen sog. Kollaborations-Service mit Datenablage, Videokonferenz und Mailfunktion). Deshalb sollte der Cloud-Nutzer, soweit nicht konkrete Informationen über den Schutzbedarf bestehen (**Beispiel:** Ein Konferenzservice wird für eine Konferenz zwischen Rechtsanwalt und Mandant gebucht, hier: Schutzklasse 3), von Schutzbedarfsklasse 2 ausgehen können.

→ Datenarten mit sehr hohem Schutzbedarf (Schutzbedarfsklasse 3)

Datenarten, die eine erhebliche Aussagekraft über die Persönlichkeit und/oder Lebensumstände des Betroffenen haben oder sonst für die Verhältnisse des Betroffenen von erheblicher Bedeutung sind. Die unbefugte Erhebung, Verarbeitung oder Nutzung solcher Daten kann zu schwerwiegenden Nachteilen für den Betroffenen (Beeinträchtigung der Rechtsgüter) führen.

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

Beispiele:

- Daten, die einem Berufsgeheimnis unterliegen (z.B. Patientendaten);
- Daten, deren Kenntnis eine erhebliche konkrete Schädigung des Betroffenen oder Dritter ermöglicht (z.B. PIN, TAN im Online-Banking);
- Daten über Vorstrafen und strafprozessuale Verhältnisse (z.B. Ermittlungsverfahren) einer Person;
- Persönlichkeitsprofile, z.B. Bewegungsprofil, Kaufverhaltensprofil, mit erheblicher Aussagekraft über die Persönlichkeit des Betroffenen.

→ Datenarten mit extrem hohem Schutzbedarf (Schutzbedarfsklasse 3 plus)

Datenarten, die eine erhebliche Aussagekraft über die Persönlichkeit und/oder Lebensumstände des Betroffenen haben oder sonst für die Verhältnisse des Betroffenen von erheblicher Bedeutung sind. Die unbefugte Erhebung, Verarbeitung oder Nutzung dieser Daten kann zu einer konkreten Gefahr für eine wesentliche Beeinträchtigung von Leben, Gesundheit oder Freiheit des Betroffenen führen.

Beispiel: Daten von V-Leuten des Verfassungsschutzes.

3.2.2 Höherstufung (Schritt 2)

→ Grundsatz

Der Schutzbedarf einer Datenverarbeitung kann sich aufgrund verschiedener Umstände erhöhen, soweit hierdurch die Gefahr einer stärkeren Beeinträchtigung der Persönlichkeitsrechte des Betroffenen eintritt. Der somit erhöhte Schutzbedarf kann, je nach Umfang des erreichten Schutzbedarfs, zur Einstufung in eine höhere Schutzbedarfsklasse führen. Umstände, die zur Höherstufung führen können, sind insbesondere:

- Verwendungskontext von Daten;
- Verkettbarkeit von Daten;
- Menge an Daten.

→ Verwendungskontext von Daten

Der Verwendungskontext von Daten kann zu höherem Schutzbedarf führen, soweit damit eine (erheblich) erhöhte Aussagekraft der Daten über die Persönlichkeit des Betroffenen einhergeht oder die unberechtigte Verwendung konkrete Nachteile für den Betroffenen 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 schutzbedarferhöhende Verwendungskontexte sind:

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

→ Verkettbarkeit von Daten

Die Verkettbarkeit von Daten, d.h. die Möglichkeit, Daten mit anderen Daten zu verknüpfen und dadurch neue Aussagen zu gewinnen, kann zu höherem Schutzbedarf führen, soweit mit der Verkettung eine (erheblich) erhöhte Aussagekraft der Daten über die Persönlichkeit des Betroffenen 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 schutzbedarferhöhende 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, so dass eine höhere Gefahr der un-

befugten Verarbeitung und Nutzung auch in Bezug auf jedes einzelne Datum besteht.

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 schutzbedarferhöhende Zusammenfassung von Daten sind:
- Sammlung großer Mengen Bank- und Kreditkartendaten.

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;
- Pseudonymisierung von Daten (§ 3 Abs. 6a BDSG);
- Freigabe von Daten.

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 verschlüsselt zur Verfügung gestellt werden. Unabhängig davon gehört die Verschlüsselung zu den Maßnahmen, die vom Cloud-Anbieter zum Schutz der Daten gegen Zugriff Unbefugter eingesetzt werden können.

→ Informationsgehalt und Verwendungskontext

Daten können aufgrund ihres Informationsgehaltes und ihres Verwendungskontextes eine geringere Aussagekraft über die Persönlichkeit des Betroffenen und seine Verhältnisse haben, als sie der abstrakten Einstufung der Datenart nach entspricht.

Beispiel: Die Terminvereinbarung eines Patienten beim Hausarzt ist in die Datenart Gesundheitsdatum einzustufen. Die bloße Termininformation enthält aber keine der Schutzbedarfsklasse 3 entsprechende Aussagekraft und entspricht eher anderen Aufenthaltsdaten, weil es sich um einen Routinebesuch handeln kann, aus dem keine gesteigerte Aussagekraft über die Verhältnisse der Person folgt.

→ **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.

→ **Freigabe von Daten**

Schutzbedürftige Daten können vom Betroffenen zur Erhebung, Verarbeitung und Nutzung freigegeben werden. In diesem Fall hat der Betroffene den Schutzbedarf herabgesetzt. Die Daten können sogar frei verfügbar werden und den Schutzbedarf auf Schutzbedarfsklasse 0 herabsetzen.

Beispiel: Der Patient veröffentlicht seine Krankenakte im Internet, um Aufmerksamkeit für eine Krankheit zu erzielen und Forschung zu erleichtern.

3.3 Schutzanforderungsklassen

Die Schutzanforderungsklassen beschreiben die Anforderungen, die für Datenverarbeitungsvorgänge der korrespondierenden Schutzbedarfsklasse zu erfüllen sind. Eine Schutzanforderungsklasse 0 ist nicht zu beschreiben, da insoweit keine datenschutzrechtlichen Anforderungen bestehen. Auf die Beschreibung einer Schutzanforderungsklasse 3 plus wird verzichtet, da sich die Anforderungen, die meist sehr einzelfallbezogen sind, nur schwerlich in allgemeiner Weise beschreiben lassen. Insoweit bleibt es beim gesetzlichen – einzelfallbezogenen – Maßstab.

3.3.1 Schutzanforderungsklasse 1

Der Cloud-Anbieter muss durch risikoangemessene technische und organisatorische Maßnahmen gewährleisten, dass die Daten nicht unbefugt verarbeitet oder genutzt werden.

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.

3.3.2 Schutzanforderungsklasse 2

Der Cloud-Anbieter muss durch risikoangemessene technische und organisatorische Maßnahmen gewährleisten, dass die Daten nicht unbefugt verarbeitet oder genutzt werden.

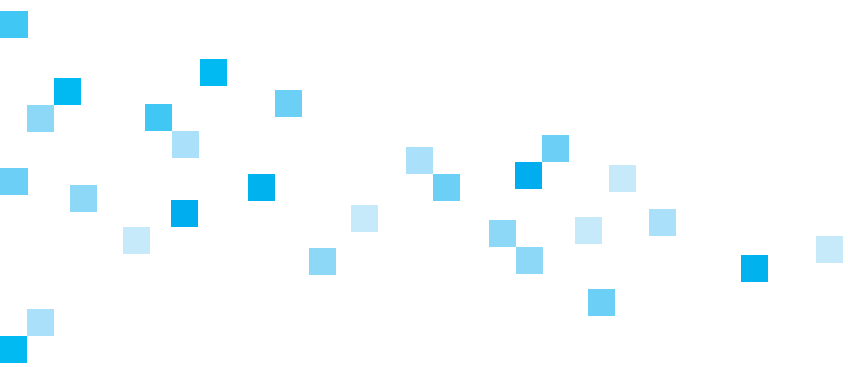
Die Maßnahmen müssen geeignet sein, um im Regelfall solche Vorgänge aufgrund technischer oder organisatorischer Fehler, einschließlich Bedienfehler, des Cloud-Anbieters oder seiner Mitarbeiter oder fahrlässiger Handlungen Dritter auszuschließen. Die Maßnahmen müssen auch geeignet sein, Schädigungen durch 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.

3.3.3 Schutzanforderungsklasse 3

Der Cloud-Anbieter muss durch risikoangemessene technische und organisatorische Maßnahmen gewährleisten, dass die Daten nicht unbefugt verarbeitet oder genutzt werden.

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



Beteiligte des Pilotprojekts

Berliner Beauftragte für Datenschutz und Informationsfreiheit

Bird & Bird LLP

Bitkom Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.

Prof. Dr. Georg Borges

Deutsche Telekom AG

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Die Landesbeauftragte für den Datenschutz und
für das Recht auf Akteneinsicht Brandenburg

DIN Deutsches Institut für Normung e. V.

ecsec GmbH

EuroCloud Deutschland_eco e.V.

Europäische EDV-Akademie des Rechts gGmbH

Landesbeauftragte für Datenschutz und
Informationsfreiheit Nordrhein-Westfalen

Landesbeauftragter für den Datenschutz Sachsen-Anhalt

PricewaterhouseCoopers AG Wirtschaftsprüfungsgesellschaft

regio iT gesellschaft für informationstechnologie mbh

SAP SE

Stiftung Datenschutz

TÜV Informationstechnik GmbH

TÜV SÜD Sec-IT GmbH

Unabhängiges Datenschutzzentrum Saarland

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Uniscon GmbH

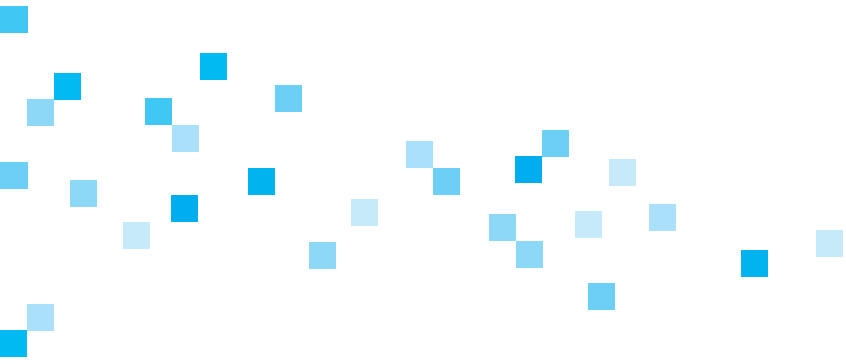
VOICE Bundesverband der IT-Anwender e.V.

Beobachtende Teilnehmer

Bayerisches Landesamt für Datenschutzaufsicht

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Bundesministerium des Innern



Impressum

Herausgeber
Pilotprojekt „Datenschutz-Zertifizierung für Cloud-Dienste“
E-Mail: info@tcdp.de
www.tcdp.de

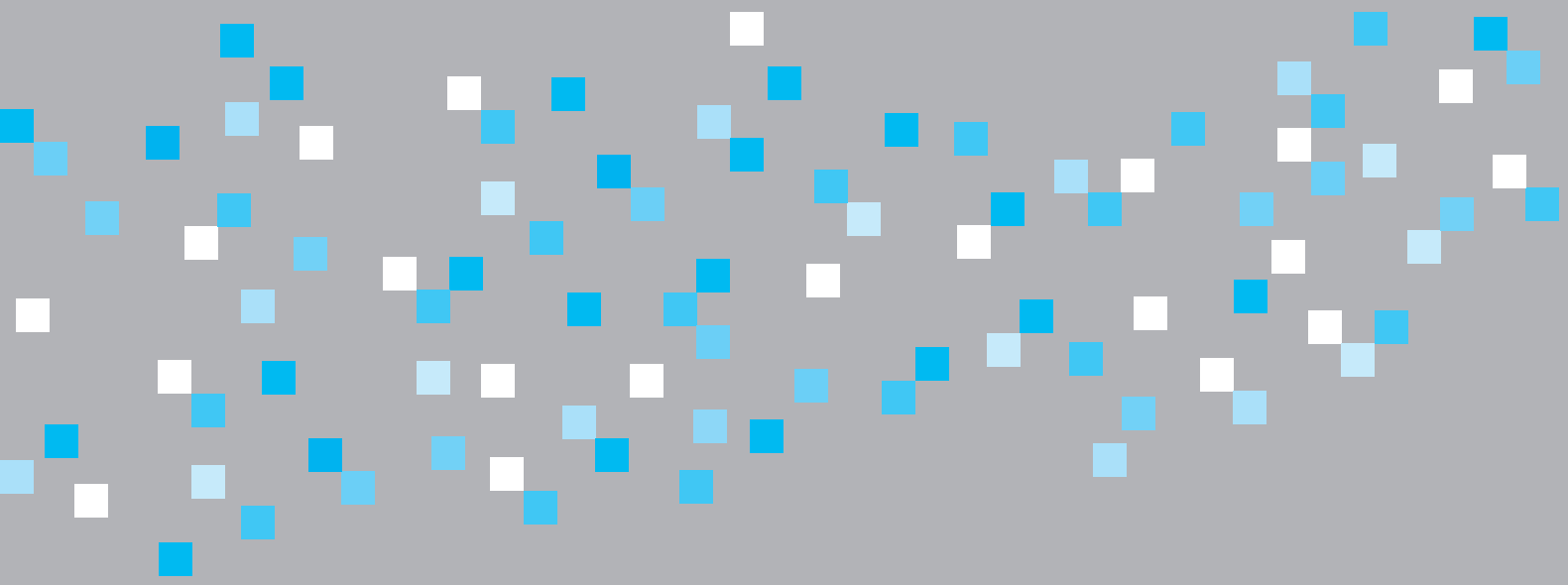
Im Auftrag des Bundesministeriums für Wirtschaft und Energie (BMWi)

Gestaltung
A&B One Kommunikationsagentur, Berlin

Satz
Christoph Engling

Druck
Ortmeier Medien GmbH, Saerbeck

Stand: September 2016



www.tcdp.de