Synopse zum Vergleich von TCDP 0.9 und TCDP 1.0

Die vorliegende Synopse soll die Orientierung zwischen TCDP 0.9 und TCDP 1.0 erleichtern. Dadurch soll des dem Cloud-Anbieter erleichtert werden, festzustellen, welche zusätzlichen Anforderungen an eine Zertifizierung nach TCDP 1.0 gegenüber TCDP 0.9 gestellt werden. Der Cloud-Nutzer wird ebenfalls in die Lage versetzt, einzuschätzen, welche zusätzlichen Maßnahmen er von einem nach TCDP 1.0 zertifiziertem Dienst gegenüber einem Dienst erwarten kann, der nach TCDP 0.9 zertifiziert wurde. Dabei ist zu beachten, dass sämtliche Dienste, die nach TCDP zertifiziert wurden – unabhängig von der jeweiligen Version – uneingeschränkt mit den Vorgaben des BDSG an die Auftragsdatenverarbeitung konform sind.

Viele Änderungen zwischen dem TCDP 0.9 und dem TCDP 1.0 ergeben sich daraus, dass das TCDP in der Version 0.9 noch einen deutlich stärkere Bezugnahme auf ISO/IEC-Normen aufwies, die nun an vielen Stellen durch eigenständige – gegebenenfalls aber an ISO/IEC-Normen angelehnte – Anforderungen ersetzt wurden.

Zusätzlich zu den Änderungen innerhalb des TCDP wurde auch die TCDP-Verfahrensordnung, die das Prüf- und Zertifizierungsverfahren standardisiert, mit der TCDP-Version 1.0 eingeführt. Die Festlegungen der TCDP-Verfahrensordnung sind daher ebenfalls zu beachten.

Zur Systematik der Synopse

Die linke Spalte der Tabelle enthält die Inhalte des TCDP 0.9. Hier sind Textstellen als gestrichen gekennzeichnet, die im TCDP 1.0 nicht mehr enthalten sind.

In der rechten Spalte ist das TCDP 1.0 so eingetragen, dass sich eine Gegenüberstellung korrespondierender Textstellen ergibt. Im Vergleich zum TCDP 0.9 neu eingefügte Teile sind gekennzeichnet.

Die wichtigsten Änderungen innerhalb des TCDP

Nachfolgend sind die wichtigsten Änderungen des TCDP 1.0 gegenüber dem TCDP 0.9 Zusammengefasst, um einen schnellen Überblick zu ermöglichen. Die hier zusammengefassten Änderungen dienen lediglich der Übersichtlichkeit und erheben keinen Anspruch auf Vollständigkeit. Maßgebend sind stets die in der jeweiligen Version des TCDP enthaltenen Anforderungen.

TCDP 1.0 Ziffer I. 4. - Datenschutz-Grundverordnung und europäische Datenschutz-Zertifizierung

Dieser Teil wurde ergänzt, um eine Anpassung des TCDP 1.0 im Hinblick auf die kommende Datenschutz-Grundverordnung zu ermöglichen. Das TCDP soll nach dem Willen der am TCDP Beteiligten in Zukunft auf Grundlage der Datenschutz-Grundverordnung weiterentwickelt werden, wobei die bereits erteilten Zertifikate nach Möglichkeit in Zertifikate nach einem DSGVO-Standard für Cloud-Dienste übergehen sollen.

TCDP 1.0 Ziffer III. - Schutzklassen

Das TCDP enthält nun detaillierte Ausführungen zum Schutzklassenkonzept. Dieses war bisher lediglich in dem Arbeitspapier „Schutzklassen in der Datenschutz-Zertifizierung“ vom April 2015 enthalten und wurde nun in aktualisierter Form in das TCDP 1.0 übernommen.

Das Schutzklassenkonzept ermöglicht es, die individuellen datenschutzrechtlichen Anforderungen des jeweiligen Cloud-Dienstes zu bestimmen und anhand der ermittelten Anforderungen die Konformität des Dienstes zu prüfen.

Das Schutzklassenkonzept unterscheidet zwischen Schutzbedarfsklassen und Schutzanforderungsklassen. Die Schutzbedarfsklassen definieren den Schutzbedarf für Datenverarbeitungsvorgänge anhand

genereller Merkmale. Dieser ergibt sich aus der Art der Daten und der Umstände der konkreten Datenverarbeitung. Die Schutzanforderungsklassen definieren in allgemeiner Form die technischen und organisatorischen Anforderungen, die für Datenverarbeitungsdienste der betreffenden Klasse maßgeblich sind. Dabei wird für jede Schutzbedarfsklasse eine korrespondierende Schutzanforderungsklasse definiert.

Der Cloud-Anbieter ist dafür verantwortlich, seinen Dienst einer Schutzanforderungsklasse zuzuordnen und sicherzustellen, dass sein Dienst die Anforderungen der Schutzanforderungsklasse stets erfüllt.

Demgegenüber kann der Cloud-Nutzer als verantwortliche Stelle den Schutzbedarf seiner Datenverarbeitung festlegen und anhand dieser Einordnung einen geeigneten Cloud-Dienst auswählen.

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

Je schwerwiegender sind die zu erwartenden Folgen einer unbefugten Verarbeitung oder Nutzung der im Cloud-Dienst verarbeiteten Daten sind, desto höher ist die Schutzbedarfsklasse zu wählen. Während bei solchen Daten der Schutzbedarfsklasse 1 meist nicht zu einem konkreten Nachteil für den Betroffenen zu rechnen ist, kann die unbefugte Erhebung, Verarbeitung oder Nutzung von Daten der Schutzbedarfsklasse 3 zu schwerwiegenden Nachteilen für den Betroffenen führen.

Spiegelbildlich hierzu verhält es sich bei den Schutzanforderungsklassen. Je höher die Schutzanforderungsklasse, desto höher sind die Anforderungen an die technischen und organisatorische Maßnahmen, insbesondere an diejenigen Maßnahmen, die eine unbefugte Verarbeitung oder vorsätzliche Eingriffe verhindern. Mit steigender Schutzanforderungsklasse ist zudem eine Protokollierung von Angriffen oder Angriffsversuchen notwendig.

TCDP 1.0 Nr. 1.5 - Technische und organisatorische Maßnahmen; Ort der Datenverarbeitung

Innerhalb des Vertrages zur Auftragsdatenverarbeitung muss nun auch der Ort der Datenverarbeitung und -speicherung festgelegt werden.

TCDP 1.0 Nr. 1.10 - Mitteilung bei Verstößen und Herausgabeverlangen

Innerhalb des Vertrages zur Auftragsdatenverarbeitung muss nun auch festgelegt werden, dass der Cloud-Anbieter den Cloud-Nutzer im Falle von Datenherausgabeverlangen unverzüglich informiert, soweit dies zulässig ist.

TCDP 1.0 Nr. 4.4 - Auswahl und Kontrolle der Unterauftragnehmer

Die Pflicht des Cloud-Anbieters zur Auswahl und Kontrolle von Unterauftragnehmern wurde auch auf Unterauftragnehmer ausgedehnt, die nun die von ihnen eingesetzten Unter-Unterauftragnehmer entsprechend auswählen und kontrollieren müssen.

TCDP 1.0 Nr. 5 - Datenschutzbeauftragter und gesetzliche Anforderungen

Ein externer Datenschutzbeauftragter muss nun auch gegenüber etwaigen weiteren Arbeit- bzw. Auftraggebern weisungsunabhängig sein.

TCDP 1.0 Nr. 6 - Berichtigung, Löschung, Sperrung von Daten

Sämtliche Anfragen auf Umsetzung von Betroffenenrechten sind nun zu dokumentieren.

TCDP 1.0 Nr. 7 - Mitteilungspflicht bei Datenschutzverstößen

Die Mitteilungspflicht bezieht sich nunmehr auch auf Verstöße von Unterauftragnehmern und Unter-Unterauftragnehmern in der gesamten „Kette“ von Unterbeauftragungen.

Es soll im Regelfall ein System zum Management von Informationssicherheitsvorfällen implementiert werden, bei dem Sicherheitsvorfälle auf etwaige Datenschutzverstöße zu überprüfen sind.

TCDP 1.0 Nr. 8 - Mitteilungs- und Dokumentationspflicht bei Datenherausgabeverlangen

Eine Regelung zum Vorgehen bei Datenherausgabeverlangen wurde komplett neu aufgenommen. Der Cloud-Anbieter ist hiernach verpflichtet, etwaige Herausgabeverlangen – soweit zulässig – dem Cloud-Nutzer unverzüglich zu melden. Hierzu kann ein Verfahren implementiert werden, nach dem bei entsprechenden Herausgabeverlangen die Zulässigkeit einer Mitteilung geprüft und ggf. die Mitteilung sofort durchgeführt wird.

TCDP 1.0 Nr. 11 - Datengeheimnis

Die Vorgaben in Bezug auf die Verpflichtung der Mitarbeiter des Cloud-Anbieter zur Einhaltung des Datengeheimnisses sind nun unabhängig von den Anforderungen gem. ISO/IEC 27018 und 27002 geregelt. Dies umfasst die Verpflichtung sämtlicher Personen, die mit der Datenverarbeitung für den Cloud-Anbieter betraut sind und die Dokumentation dieses Prozesses im Rahmen eines hierfür eingerichteten organisatorischen Verfahrens.

Es sind nun detaillierte Vorgaben zur Umsetzung der Verpflichtung auf das Datengeheimnis und der Dokumentation enthalten.

TCDP 1.0 Nr. 21 - Schutzkonzept

Der Cloud-Anbieter ist nun verpflichtet, ein Schutzkonzept zu erarbeiten, das die für seinen Dienst und seine Datenverarbeitungsanlagen spezifischen Risiken angemessen berücksichtigt. Das Schutzkonzept muss auch die vom Cloud-Nutzer einzuhaltenden Sicherheitsmaßnahmen enthalten und schriftlich dokumentiert sowie regelmäßig überprüft und aktualisiert werden.

TCDP 1.0 Nr. 22 - Sicherheitsbereich und Zutrittskontrolle

Die Umsetzungshinweise in Bezug auf Sicherheitsbereich und Zutrittskontrolle der Räume des Cloud-Anbieters sind nun unabhängig von den Anforderungen gem. ISO/IEC 27002 ausgeführt. Schutzklasse 1 erfordert risikoangemessene technische und organisatorische Maßnahmen zum Schutz vor Naturkatastrophen und unbefugten Zutritt. Schutzklasse 2 erfordert darüber hinaus einen weitergehenden Schutz gegen fahrlässige Handlungen befugter Personen und vorsätzliche Zutrittsversuche Unbefugter. Schutzklasse 3 erfordert, dass jeglicher unbefugter Zutritt hinreichend sicher ausgeschlossen ist und jeder Zutrittsversuch dokumentiert wird. Die sehr detaillierten Anforderungen des TCDP 0.9 zu Schutzklasse 3 wurden entfernt.

TCDP 1.0 Nr. 23 - Logischer Zugang zu Datenverarbeitungsanlagen und Zugriff auf Daten

Die Maßnahmen für die Zugriffskontrolle gelten nun auch für Verbindungs- und Metadaten, soweit diese personenbezogene Daten enthalten.

Die Umsetzungshinweise enthalten nun von ISO/IEC 27002 und 27018 unabhängige Angaben. Dabei umfasst Schutzklasse 1 die Verhinderung von Zugriffen Unbefugter durch geeignete technische und organisatorische Maßnahmen, wobei auch fahrlässige Handlungen durch berechtigte erfasst sind. Gegen vorsätzliche Angriffe ist ein Mindestschutz vorzusehen. In Schutzklasse 2 muss auch vorsätzlicher unbefugter Zugriff hinreichend sicher ausgeschlossen werden. Schutzklasse 3 sieht darüber hinaus den Einsatz besonders sicherer Authentifizierungssysteme vor.

TCDP 1.0 Nr. 24 - Übertragung und Speicherung von Daten

Die Umsetzungshinweise enthalten nun von ISO/IEC 27002 und 27018 unabhängige Angaben. Schutzklasse 1 erfordert, dass Unbefugte personenbezogene Daten bei der Weitergabe oder

Speicherung nicht lesen, kopieren, verändern oder entfernen können. Dabei muss verhindert werden, dass Unbefugte aufgrund technischer oder organisatorischer Fehler des Cloud-Anbieters oder aufgrund fahrlässigen Handelns von Befugten Zugriff erhalten. Jede Datenübertragung oder Transport von Datenträgern sind zu protokollieren. Gegen vorsätzliche Eingriffe ist ein Mindestschutz erforderlich. Schutzklasse 2 sieht weitergehend einen hinreichenden Schutz gegen zu erwartende vorsätzliche Zugriffsversuche Unbefugter vor, wobei ein unbefugter Zugriff im Regelfall festgestellt werden können muss. Schutzklasse 3 enthält auch einen Schutz vor unbefugtem Zugriff durch den Cloud-Anbieter, dessen Mitarbeiter und Dritte, wobei jeder unbefugte Zugriff und möglichst auch Zugriffsversuch festgestellt werden können müssen.

TCDP 1.0 Nr. 25 - Nachvollziehbarkeit der Datenverarbeitung

Die Anforderungen richten sich nun nicht mehr nach ISO/IEC 27018, sondern allein nach ISO/IEC 27002. Bei der Protokollierung sind zudem die Grundsätze der Erforderlichkeit, Zweckbindung und Datensparsamkeit zu beachten. Erforderlich ist weiterhin, dass der Cloud-Anbieter ein Protokollierungskonzept erstellt, in welchem insbesondere Gegenstand und Umfang der Protokollierung, Aufbewahrung, Integritätsschutz und Löschung von Protokollen, die Verwendung der Protokolldaten sowie die Wahrung der Datenschutzziele im Rahmen der Protokollierung dokumentiert werden.

Die Umsetzungshinweise enthalten nun von ISO/IEC 27002 und 27018 unabhängige Angaben. Schutzklasse 1 erfordert risikoangemessene technische und organisatorische Maßnahmen, durch die nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Dateneingaben, -veränderungen und -löschungen bei der bestimmungsgemäßen Nutzung des Dienstes müssen dabei nachvollziehbar sein. Die Nachweisbarkeit der Veränderungen muss auch bei technischen oder organisatorischen Fehlern gewährleistet bleiben. Gegen vorsätzliche Manipulationen der Maßnahmen zur Nachweisbarkeit ist ein Mindestschutz vorzusehen. Schutzklasse 2 erfordert, dass auch ein Schutz gegen zu erwartende vorsätzliche Manipulationen der Protokollierungsinstanzen und vorsätzlichen Zugriff auf oder Manipulationen von Protokollierungsdateien (Logs) durch Unbefugte vorgesehen ist. Schutzklasse 3 sieht vor, dass Manipulationen von Protokollierungsinstanzen und -dateien (Logs) hinreichend sicher ausgeschlossen sind und jede Manipulation sowie möglichst auch jeder entsprechende Versuch nachträglich festgestellt werden kann.

TCDP 1.0 Nr. 26 - Auftragskontrolle

Die Anforderungen an die Auftragskontrolle gelten nun losgelöst von den Anforderungen von ISO/IEC 27018. Dabei ist vom Cloud-Anbieter durch risikoangemessene Maßnahmen sicherzustellen, dass die Verarbeitung der Daten des Cloud-Nutzers nur nach Maßgabe der Weisungen des Cloud-Nutzers erfolgt.

Schutzklasse 1 sieht vor, dass die Maßnahmen geeignet sein müssen, um im Regelfall Abweichungen von den Weisungen aufgrund technischer oder organisatorischer Fehler des Cloud-Anbieters oder fahrlässiger Handlungen des Cloud-Nutzers oder Dritter auszuschließen. Gegen vorsätzliche Eingriffe ist ein Mindestschutz vorzusehen. Schutzklasse 2 sieht Maßnahmen vor, die ein Abweichen von den Weisungen durch zu erwartende vorsätzliche Eingriffe hinreichend sicher ausschließen. Zudem müssen Eingriffe im Regelfall feststellbar sein. Schutzklasse 3 erfordert, dass Abweichungen von den Weisungen des Cloud-Nutzers hinreichend sicher ausgeschlossen sind. Dazu muss eine umfassende Protokollierung von Administratorzugriffen erfolgen.

TCDP 1.0 Nr. 27 - Getrennte Verarbeitung

Die Umsetzungshinweise zu den Schutzklassen wurden präzisiert. Schutzklasse 1 sieht nun vor, dass der Cloud-Anbieter durch risikoangemessene technische und organisatorische Maßnahmen gewährleistet, dass die Daten des Cloud-Nutzers von den Datenbeständen anderer Cloud-Nutzer und von den anderen

Datenbeständen des Cloud-Anbieters getrennt verarbeitet werden und dass der Cloud-Nutzer die Datenverarbeitung nach verschiedenen Verarbeitungszwecken trennen kann. Dazu gehören etwa die anwendungsseitige Trennung verschiedener Mandanten und die Mandantenfähigkeit der Anwendungsprogramme. Die Datentrennung muss dabei im Regelfall auch bei technischen oder organisatorischen Fehlern sichergestellt bleiben. Gegen vorsätzliche Verstöße ist ein Mindestschutz vorzusehen. Schutzklasse 2 erfordert einen Schutz gegen zu erwartende vorsätzliche Verstöße, der diese hinreichend sicher ausschließt, z.B. eine Verschlüsselung der Nutzerdaten sowie die Verwendung getrennter Betriebsumgebungen für verschiedene Verarbeitungen. Verstöße müssen im Regelfall festgestellt werden können. Schutzklasse 3 erfordert darüber hinaus, dass ein Verstoß gegen die Datentrennung hinreichend sicher ausgeschlossen ist. Die Verschlüsselung und getrennte Betriebsumgebung gem. Schutzklasse 2 ist dabei zwingend erforderlich. Ebenso ist ein Verfahren zur Erkennung von Missbräuchen erforderlich.

TCDP 1.0 Nr. 28 - Kryptographie

Die Anforderungen richten sich nun ausschließlich nach den Vorgaben von ISO/IEC 27002, ohne auf ISO/IEC 27018 Bezug zu nehmen.

Die Umsetzungshinweise enthalten nun von ISO/IEC 27002 und 27018 unabhängige Angaben. Schutzklasse 1 sieht vor, dass der Cloud-Anbieter die technische Entwicklung im Bereich der Kryptographie verfolgt und dass die von ihm getroffenen Maßnahmen den aktuellen technischen Anforderungen entsprechen. Zudem muss er die angemessene Implementierung der Maßnahmen durch geeignete Tests überprüfen und dokumentieren. Schutzklasse 2 sieht weitergehend vor, dass der Cloud-Anbieter die technische Entwicklung im Bereich der Kryptographie laufend verfolgt und dass die von ihm getroffenen Maßnahmen den aktuellen technischen Empfehlungen (best practice) entsprechen. Schutzklasse 3 erfordert, dass der Cloud-Anbieter die angemessene Implementierung der kryptographischen Maßnahmen durch unabhängige, sachkundige Stellen überprüfen lässt und die Prüfung einschließlich des Ergebnisses dokumentiert wird.

TCDP 1.0 Nr. 31 - Schutz gegen zufällige Zerstörung oder Verlust (Wiederherstellbarkeit)

Gegenüber TCDP 0.9 wurden die Anforderungen an die Wiederherstellbarkeit komplett neu geschaffen. Die Anforderungen sind dabei auf Grundlage eines separaten „Wiederherstellbarkeitsniveaus“ definiert, wobei zwischen „normale Wiederherstellbarkeit“, „hohe Wiederherstellbarkeit“ und „sehr hohe Wiederherstellbarkeit“ differenziert wird. Die Wiederherstellbarkeit zielt darauf ab, die im Cloud-Dienst verarbeiteten Daten im Falle von ungewollter Zerstörung oder Verlust auf Seiten des Cloud-Anbieters zu schützen.

Der Cloud-Anbieter muss über ein Konzept zur Gewährleistung der Wiederherstellbarkeit der Daten verfügen und dieses dem Nutzer auf Anfrage zur Verfügung stellen. Im Cloud-Vertrag müssen Angaben zur maximalen Datenwiederherstellungszeit festgelegt werden. Der Cloud-Anbieter muss zudem durch risikoangemessene Maßnahmen sicherstellen, dass die Daten innerhalb der im Cloud-Vertrag angegebenen Zeit wiederhergestellt werden können, wobei die Anforderungen von ISO/IEC 27002 zu beachten sind.

Die Umsetzungshinweise sehen je nach Wiederherstellbarkeitsniveau unterschiedliche Maßnahmen vor. Normale Wiederherstellbarkeit erfordert einen Schutz gegen zu erwartende, naheliegende Ereignisse, der so zuverlässig absichert, dass diese Risiken bei normalem Verlauf nicht zu endgültigem Datenverlust führen. Hohe Wiederherstellbarkeit erfordert einen Schutz, der bei seltenen Ereignissen, die nach der Lebenserfahrung praktisch nie vorkommen, aber gleichwohl in einigen Fällen zu beobachten sind, eine Wiederherstellung ermöglicht. Sehr hohe Wiederherstellbarkeit erfordert Schutz gegen Datenverlust bei außergewöhnlichen, aber nicht als theoretisch auszuschließenden Ereignissen, die nur in extrem seltenen Einzelfällen vorkommen.