Prof. Dr. Friedrich-L. Holl
Beratung/Schulung
Datenschutzsachverständiger

Kurzgutachten

für das IT-Produkt „Zentrale Kassenprüfung“

zum Datenschutz-Gütesiegelverfahren (Rezertifizierung) beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein

im Auftrag der Lidl Stiftung & Co. KG
Oktober 2015

Inhaltsverzeichnis

1 Einleitung

Mit diesem Kurzgutachten wird die Auditierung des IT-Produkts „Zentrale Kassenprüfung“ in der Version 2015 zusammengefasst. Ziel der rechtlichen und technischen Auditierung ist die erneute Erlangung des Datenschutz-Gütesiegels gemäß der Datenschutzgütesiegelverordnung (DSGSVO)1 in Schleswig-Holstein, welches durch das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) vergeben wird.

2 Zeitpunkt der Prüfung

Juli 2013 – Mai 2015

3 Antragstellerin

Lidl Stiftung & Co. KG
Stiftsbergstr. 1
74167 Neckarsulm

4 Sachverständiget (rechtlich/technisch):

Prof. Dr. Friedrich Holl
Hektorstr. 7
10711 Berlin

5 Kurzbezeichnung des IT-Produktes:

Zentrale Kassenprüfungssoftware

6 Detaillierte Bezeichnung des IT-Produktes

Die Kassenprüfungssoftware (**Kassenkennzahlenanalyse)** der Lidl Stiftung & Co. KG dient der Analyse von Kassendaten einzelner Verkaufsstellen/Filialen, in denen Kassensysteme genutzt werden, zur Aufdeckung von Manipulationen im Kassierprozess. Der durch Manipulationen an Kassen erzeugte Verlust hat im Einzelhandel ein hohes Schädigungspotenzial, weshalb Kontrollen in diesem Bereich notwendig sind. Dabei führen einfache manuelle Stichprobenkontrollen vor Ort in der Regel nur in begrenztem Umfang zur Aufdeckung von Manipulationen, da die Vorgehensweise in vielen Fällen sehr raffiniert ist und Schäden erst durch maschinelle Auswertungen erkannt werden können, die über mehr als einen Tagesabgleich hinausgehen.

Um Kassenmanipulationen mittels des Kassenprüfungssystems der Lidl Stiftung & Co. KG aufdecken zu können, werden potenzielle Betrugsszenarien abgebildet und die Kassendaten der zu überprüfenden Kassen auf das Prüfsystem übertragen. Weitere Eingaben sind Grenzwerte, die bei den Auswertungen überschritten werden müssen. Damit wird ausgeschlossen, dass Bagatellfälle als Ergebnisse angezeigt werden. Das System überprüft dann die übertragenen Daten auf Auffälligkeiten. Danach können auf der Basis der ermittelten Daten, vor Ort die notwendigen Maßnahmen - wie beispielsweise arbeitsrechtliche Konsequenzen - ergriffen, Ermittlungsbehörden eingeschaltet werden usw.

Das Kassenprüfungssystem benötigt im Einzelnen die folgenden Elemente.

Szenarien:

Für jede spezifische Anwendung des Kassenprüfungssystems in einem Unternehmen / einer Organisation sind in einem ersten Schritt bekannte, wahrscheinliche oder mögliche Betrugsvorfälle, Manipulationen o.ä. als Szenarien im System abzubilden. Das System kann jedoch nur überprüfen, was dem jeweiligen Nutzer oder in der betroffenen Branche bereits bekannt ist; das System ist nicht in der Lage, "selbstständig" betrügerische Vorfälle aufzudecken.

Datenbasis:

Die Analysen werden auf einer Datenbasis realisiert, die sich aus Daten zusammensetzt, die von üblichen Kassensystemen zur Verfügung gestellt werden. Dabei handelt es sich im Einzelhandel beispielsweise um die vom Kassierer/Kassiererin abgerechneten Verkäufe, Stornierungen, Rückgaben, Pfandauszahlungen usw. Bei anderen Branchen (bspw. Gastronomie, Bibliotheken, usw.) werden die für das Einsatzumfeld spezifischen Kassendaten genutzt. Die jeweiligen Daten ergeben sich aus den im jeweiligen Unternehmen/Organisation realisierten Kassiervorfällen.

Diese Daten können dann über einen vom Unternehmen festzulegenden Zeitraum (x-Tage/Wochen) mit einer bestimmten Häufigkeit (y-mal/Jahr) ausgewertet werden. Geprüft wird der Umfang, welcher im Rahmen der Auftragsdatenverarbeitung definiert wurde und aus datenschutzrechtlicher Sicht zulässig ist. Vollerhebungen (permanente Überprüfung einzelner/aller Beschäftigten) sind damit grundsätzlich ausgeschlossen.

Hinweis: Für Daten von externen Stellen gilt folgende Regel: spätestens zwei Wochen nach Zurverfügungstellung der Prüfungsergebnisse werden alle Kassendaten im System der Kassenkennzahlenanalyse vollständig gelöscht. Abweichung hiervon bedürfen einer gesonderten Beauftragung durch die verantwortliche Stelle.

Schwellenwerte:

Damit verhindert wird, dass Bagatellfälle in die Untersuchung mit einfließen, werden für die Auswertungen Schwellenwerte festgelegt. Dies verhindert insbesondere, dass bspw. kleinere Fehler als potenzielle Manipulation bzw. als potenzieller Missbrauch Berücksichtigung finden. Allerdings wird vom Auftraggeber in der jeweiligen Systemkonfiguration definiert, wie hoch die Schwellenwerte sind, und was damit noch als "Bagatellfall" anzusehen ist bzw. was nicht.

Protokolle:

Die nachhaltige Dokumentation angeforderter und genehmigter Zugriffe bzw. Änderungen wird über das Antragsformular „Zugriffe zur zentralen Kassenprüfung“ über das Ticketsystem sichergestellt.

Pseudonymisierung:

Grundsätzlich ist das System so konfiguriert, dass in der Analyse nur pseudonymisierte Daten verwendet werden, indem keine Namen oder sonstige Daten genutzt (im System gespeichert) werden, die direkt mit den Kassierern/Kassiererinnen in Verbindung gebracht werden können. Ein Rückbezug auf Personendaten findet nur dann statt, wenn durch die Analysen ein ausreichender Verdacht auf Manipulationen und/oder ein erheblicher Umfang betrügerischer Aktionen einer bestimmbaren Person gefunden wurden. Aufgrund der Konstruktion des Kassenprüfungssystems ist außerdem grundsätzlich gewährleistet, dass die auswertende Organisation (Lidl Stiftung Co. KG) nicht die das Kassensystem betreibende Organisation ist. Deshalb kann das Zurückführen der ausgewerteten Daten auf reale Personen ausschließlich außerhalb der die Kassenprüfung durchführenden Organisation erfolgen. Damit werden die Persönlichkeitsrechte der Betroffenen besonders geschützt, da nur unter besonderen Bedingungen der Personenbezug überhaupt wieder hergestellt wird.

Die zentrale Kassenprüfung wird grundsätzlich als Service durch die Revision der Lidl Stiftung & Co. KG durchgeführt. Damit erfolgt die Prüfung durch eine neutrale Stelle, welche keiner direkten organisatorischen Verantwortung oder Kennzahlenverantwortung für den Verkauf untersteht. Ausschließlich die Prüfer der zentralen Kassenprüfung in der Abteilung Revision der Lidl Stiftung & Co. KG sind beauftragt, die definierten Prüfprozesse durchzuführen. Die Prüfung erfolgt ohne den Hintergrund einer Leistungskontrolle und dient gleichfalls nicht zur Ermittlung von Schulungsbedarf der Mitarbeiterinnen und Mitarbeiter o.ä. Die Kassenprüfung erlaubt die Gewährleistung einer unternehmensgruppenweit einheitlichen, vergleichbaren Qualität, wenn alle standardisierten Prüfungen nach Vorgabe des Konzepts der zentralen Kassenprüfung durchgeführt werden. Die Betreiberin des Systems, die Lidl Stiftung & Co. KG, stellt sicher, dass das System nur unter Berücksichtigung der o.g. Rahmenbedingungen betrieben wird.

Die zentrale Kassenprüfung erlaubt derzeit standardmäßig folgende Prüfthemen, die auf bestimmte Kassierprozesse im Einzelhandel zurückzuführen sind: Pfand, Storni, Geldrückgaben, Bonabbrüche /-rückstellungen und Preisanzeige auf Bedienerebene. Diese Kassierprozesse sind derzeit als diejenigen bekannt, die eine grundsätzliche Möglichkeit von Unterschlagungen o.ä. beinhalten. Es gibt voraussichtlich noch andere Prozesse, über die in Verkaufsstellen/Kasssenterminals Betrug, Unterschlagungen o.ä. realisiert werden können, doch diese sind bisher (noch) nicht bekannt geworden bzw. als Missbrauchskonstellationen anerkannt. Bei den bisher bekannten Prozessen ist eine organisatorische Umgestaltung, die dann die Möglichkeit eines Missbrauchs verhindern würde, nicht möglich, da beispielsweise eine ausreichende Flexibilität und Freundlichkeit gegenüber den Kunden notwendig ist. Dies würde beispielsweise durch verschärfte direkte Kontrollen eingeschränkt werden.

Die Prüfmethodik unterscheidet sich in eine *"automatische Detailanalyse"* sowie das zur Verfügung stellen von Kennzahlen, die dann in einer *"manuellen Kenzahlenanalyse"* überprüft werden können.

Über diese Kennzahlen können zudem neue Betrugsszenarien ermittelt werden, da das System die grundlegenden Zahlen zur Auswertung zur Verfügung stellt. Dieser manuelle Teil der Prüfung ist nicht Bestandteil der Zertifizierung.

Bei der *automatischen Detailanalyse* werden die Kassendaten mit Hilfe der Software automatisch nach vordefinierten Mustern (= Szenarien) gescannt. Es handelt sich hierbei um Szenarien, die aufgrund des gleichzeitigen Eintritts mehrerer Kriterien und der Überschreitung der Schwellenwerte in Kombination mit einer Häufung auf eine mögliche Manipulation hinweisen. Es werden nur die Kassenbediener angezeigt, die diese Schwellenwerte bzw. Häufigkeiten überschreiten. Eine Änderung dieser Werte ist nur nach Prüfung und anschließender Freigabe/Beauftragung (grundsätzlich sollte der betriebliche/behördliche Datenschutzbeauftragte einbezogen werden) möglich. Die dem Szenario entsprechenden Einzelbons werden pro Bediener von der Software herausgefiltert und dem Bearbeiter ohne direkten Personenbezug (pseudonymisiert) angezeigt. Anschließend führt der Bearbeiter eine manuelle Plausibilitätenprüfung der Ergebnisse (relevante Bons) durch. Dies kann sowohl zur Entlastung als auch zur Bestätigung der Vorwürfe gegenüber dem auffälligen Kassenbediener führen.

Prüfungsumfang:

Jeder Auftraggeber muss entscheiden, wie oft die jeweiligen Kassen in einem bestimmten Zeitraum (beispielsweise pro Jahr) geprüft werden sollen. Ebenso muss festgelegt werden, über welchen Zeitraum die Prüfung (rückwirkend, ausgehend vom Prüfungszeitpunkt) erfolgen soll, z.B. über einen Zeitraum von 12 Wochen. Neben den standardisierten, nicht anlassbezogenen Kontrollen können bei konkreten Verdachtsmomenten auch direkte Kontrollen bspw. einer Verkaufsstelle veranlasst werden, wo nur die Daten der betroffenen Einheit untersucht werden. Hierfür sollten beim Auftraggeber besonders abgesicherte Prozesse definiert werden, die verhindern, dass willkürlich Kontrollen angesetzt werden.

Die Auffälligkeiten aus der Kennzahlenanalyse werden dem Auftraggeber als Prüfbericht zur Verfügung gestellt.

7 Mitbestimmung (Betriebsrat/Personalrat)

Der Einsatz der Zentralen Kassenprüfung in Unternehmen und Organisationen mit Betriebs- oder Personalrat ist ohne deren Zustimmung unzulässig, da durch die Zentrale Kassenprüfung eindeutig Mitbestimmungstatbestände (beispielsweise nach § 87 Abs. 1 Nr. 6 Betriebsverfassungsgesetz) betroffen sind. Die Zustimmung durch den Betriebs- bzw. Personalrat wird üblicherweise in einer Betriebs- bzw. Dienstvereinbarung festgelegt, die im Rahmen einer Interessenabwägung den Schutz der Persönlichkeitsrechte der Arbeitnehmer angemessen berücksichtigt und beispielsweise auch die hier genannten Rahmenbedingungen (Prüfungsumfang, Schwellenwerte usw.) festlegt.

Vor einem Rollout der Zentralen Kassenprüfung in einem Unternehmen/einer Organisation mit Betriebs- oder Personalrat ist deshalb sicher zu stellen, dass das zuständige Gremium sein Mitbestimmungsrecht wahrnehmen konnte und dem Einsatz des Systems zustimmt.

8 Zweck und Einsatzbereich

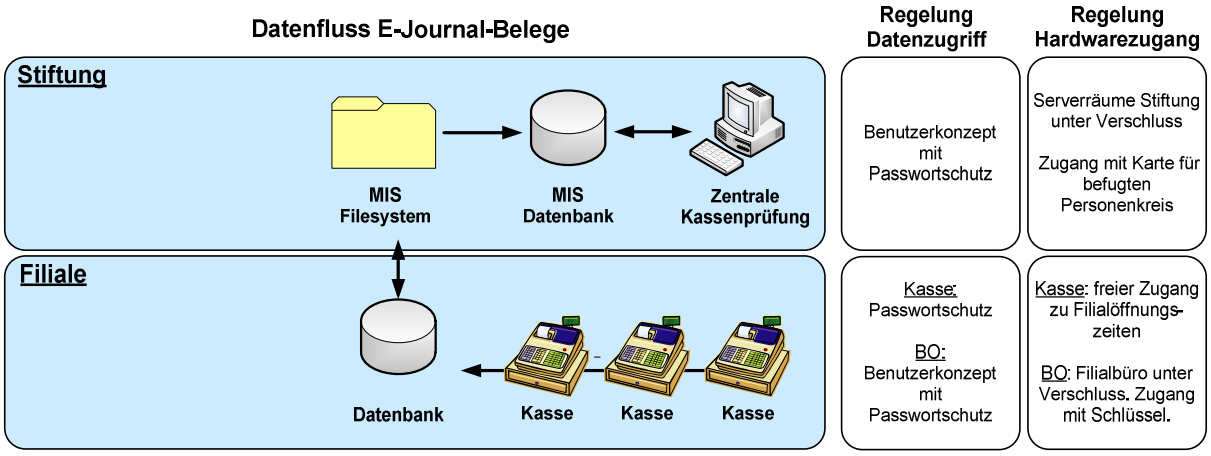
Das zentrale Kassenprüfungssystem dient der Aufdeckung von Manipulationsfällen wie z.B. Pfandmanipulation, dem Erkennen von Betrugs- und Unterschlagungsmethoden und soll zur Verringerung der Inventurdifferenzen, dem sog. Schwund, beitragen. Dies sind die primären Ziele, die mit dem Kassenprüfungssystem verfolgt werden.

Daneben soll eine gezielte Prozessoptimierung durch das Aufzeigen von Schwachstellen sowie die Prävention vor Manipulationen erreicht werden. Dabei sollen eine möglichst geringe Einflussnahme auf die individuellen Rechte der Mitarbeiterinnen und Mitarbeiter erfolgen und durch entsprechende Pseudonymisierungen eine Reduzierung des Drucks erreicht werden, der grundsätzlich von derartigen Prüfungen auf die Beschäftigten ausgeht.

Die Kassenprüfungssoftware dient weiterhin der Information des Managements. Dieses erhält regelmäßig anonymisierte Auswertungen über die Prüfungen und deren Ergebnisse.

Der Einsatz des Systems ist über den Einzelhandel hinaus für jedes Kassensystem denkbar (z.B. Schwimmbad, Theater, Museum), um Kassiervorgänge zu prüfen.

9 Modellierung des Datenflusses



10 Version des zur Prüfung verwendeten Anforderungskatalogs

Anforderungskatalog v 2; Stand: 11.6.2015

11 Zusammenfassung der Prüfungsergebnisse

Kassenprüfungssysteme bilden grundsätzlich eine problematische Datenschutzkategorie. Sehr leicht kann aus einem System, mit dem berechtigterweise nur unerlaubte Verstöße herausgefiltert werden sollen, ein komplexes, auf dauerhafte Überwachung ausgerichtetes System werden, mit dem selbst minimales Fehlverhalten am Arbeitsplatz erkannt werden kann.

Das Kassenprüfungssystem der Lidl Stiftung & Co. KG ermöglicht dagegen eine Systemkonfiguration, in der keine Bagatellfälle verfolgt werden und nur die Verstöße erkennbar gemacht werden, bei denen eine hohe Schädigung des jeweiligen Unternehmens mit großer Wahrscheinlichkeit anzunehmen ist. Allerdings verbleibt die Verantwortung über die letztendliche Systemkonfiguration beim Auftraggeber, der zu entscheiden hat, wie welche Parameter gesetzt und ausgewertet werden. Allerdings hat die Lidl Stiftung & Co. KG ein datenschutzkonformes Grundkonzept entwickelt, das den Auftraggebern zur Übernahme vorgeschlagen wird. Damit lassen sich dann Probleme datenschutzrechtlicher Art vermeiden.

Dies ist jedoch nur deshalb möglich, weil das Kassenprüfungssystem als SAAS (Software as a Service) angeboten wird und entsprechende Möglichkeiten vorkonfiguriert sind, die die Persönlichkeitsrechte der Betroffenen in einem sehr ausgeprägten Maße wahren.

Wesentliche Grundlagen für den datenschutzkonformen Betrieb des Systems sind die Gestaltung der Szenarien, die so aufbereitet worden sind, dass das Erfüllen der Kriterien eines Szenarios mit sehr hoher Wahrscheinlichkeit darauf hinweist, dass ein Kassier/eine Kassiererin einen Verstoß begangen hat, der arbeitsrechtliche oder sogar strafrechtliche Konsequenzen zur Folge haben kann. Eine weitere Grundlage ist die Auswahl der Schwellenwerte, die dazu führt, dass nur wirklich schwerwiegende Verstöße erkannt werden. Hier ist darauf hinzuweisen, dass eine solche Abgrenzung von Bagatellfällen nicht zwingenderweise notwendig wäre, da die herrschende Meinung bereits kleinste Summen als potenzielle Basis für arbeitsrechtliche Konsequenzen akzeptiert. Allerdings wäre eine Folge von zu geringen Schwellwerten, dass viele kleine Fehler als potenzielle Verstöße erkannt und so das Aufdecken von echten Verstößen schwieriger machen würde. Natürlich können zu kleine Schwellenwerte auch negative Auswirkungen auf das Betriebsklima haben, hohen Überwachungsdruck erzeugen und somit eher kontraproduktiv wirken.

Weiterhin ist die Trennung von Auswertung und Erzeugung der Daten sowie die Pseudonymisierung der Kassendaten als sehr positiv zu bewerten. Der Auswertende kennt keinen der potenziellen Kassierer/Kassiererinnen und kann die Daten keiner Person zuordnen. Die Zuordnung zu einer Person ist bei der vorliegenden Konfiguration erst dann möglich, wenn sich ein ausreichender Verdacht auf eine Manipulation oder einen Verstoß ergibt. Aber selbst da erfolgt die Zuordnung zu einer Person nicht durch den Auswertenden, sondern durch den direkten Dienstvorgesetzten beim Auftraggeber, der die eigentliche Personalverantwortung trägt.

Daneben soll eine gezielte Prozessoptimierung durch das Aufzeigen von Schwachstellen sowie die Prävention vor Manipulationen erreicht werden. Dabei sollen eine möglichst geringe Einflussnahme auf die individuellen Rechte der Mitarbeiter erfolgen und eine möglichst große Reduzierung des

Drucks erreicht werden, der grundsätzlich von derartigen Prüfungen ausgeht. Dies ist ein weiterer Grund, weshalb nur die in der Zentrale der Lidl Stiftung & Co. KG angestellten Mitarbeiter in der Revisionsabteilung (Kassenprüfer) prüfen und nicht die Vorgesetzten vor Ort, was mit einer entsprechenden Konfiguration des Systems natürlich möglich wäre.

Die technische Umsetzung des Kassenprüfungssystems orientiert sich grundsätzlich an der Einhaltung hoher Datenschutzvorgaben und stellt alle Möglichkeiten für einen datenschutzkonformen Betrieb zur Verfügung. Im Zusammenhang mit der Auftragsdatenverarbeitung des Kassenprüfungssystems konnte festgestellt werden, dass insbesondere die technischen und organisatorischen Maßnahmen gemäß §§ 5 und 6 LDSG beziehungsweise § 9 BDSG (inklusive Anhang) in sehr konsequenter Form umgesetzt werden. So steht bspw. ein eigener physischer Rechner im sehr hoch gesicherten Rechenzentrum der Lidl-Stiftung & Co. KG zur Verfügung.

12 Beschreibung, wie das IT-Produkt den Datenschutz fördert

Das Kassenprüfungssystem ist von der grundsätzlichen Gestaltung her ein System, das Datenschutzaspekte besonders berücksichtigt.

Hierzu zählt bspw., dass das System nicht von den direkten Vorgesetzten betrieben und ausgewertet wird, sondern von einer unabhängigen Organisation, die mit den eigentlichen Kassenprozessen nichts zu tun hat und diese nur kontrolliert. Weiterhin werden Schwellenwerte und weitere Begrenzungen über das System realisierbar, so dass nur die wirklich schweren Fälle aufgedeckt werden. Zudem wird die Auswertung der Daten nur auf einem pseudonymisierten Datenbestand durchgeführt. Dadurch werden bspw. Daten, die zwar den Rahmenbedingungen eines Fehlverhaltens entsprechen, sich jedoch bei der Plausibilitätskontrolle als mangelhaft erweisen und damit für einen späteren arbeits- oder strafrechtlichen Prozess nicht verwertbar sind, keiner Person zugeordnet.

Die Nutzung von Schwellenwerten ist der weitestgehende Schutz der Persönlichkeitsrechte, weil nur die wirklich schweren Fälle herausgefiltert und Bagatellfälle ausgeschlossen werden. Zudem sind die technisch organisatorischen Maßnahmen gem. §§ 5 und 6 LDSG sowie § 9 BDSG sehr datenschutzförderlich umgesetzt.

Es bleibt jedoch festzustellen, dass die grundsätzliche Konfiguration des Kassenprüfungssystems wesentlich zum datenschutzkonformen Betrieb beiträgt. Deshalb sollte möglichst die Konfiguration übernommen werden, die von der Lidl Stiftung & Co. KG genutzt wird.

Der Betrieb der Zentralen Kassenprüfung hat insgesamt eine große Wirksamkeit und gleichzeitig eine hohe Verlässlichkeit gezeigt. Nach der erstmaligen Feststellung von Manipulationen in Unternehmen ging in der Folge der Umfang der detektierten Verdachtsfälle in der Regel drastisch zurück. Daneben zeigte sich, dass es bisher nur in ganz wenigen Ausnahmefällen zu falschen bzw. unrealistischen Verdächtigungen von Betroffenen gekommen ist, die vor Ort durch Plausibilitätskontrollen u.ä. schnell erkannt werden konnten.

13 Rezertifizierung

Änderungen

Im Rahmen des Betriebs der Zentralen Kassenprüfung der Lidl Stiftung & Co. KG im Zeitraum von 2013-2015 wurden keine Änderungen am Produkt vorgenommen, die den Zertifizierungsbereich betreffen. Zwar wurde in der speziellen Konfiguration der Einsatzrahmenbedingungen der Zentralen Kassenprüfung der Lidl Stiftung & Co. KG Änderungen implementiert, die jedoch im Rahmen der Rezertifizierung nicht zu bewerten waren. Grundsätzlich kann festgestellt werden, dass die technisch-organisatorischen Rahmenbedingungen für den Betrieb des Systems in der Lidl Stiftung & Co. KG weiter verbessert wurden.

Neue Szenarien, die neue, bisher nicht bekannte Manipulationen umfassen, wurden gleichfalls nicht implementiert.

Bezüglich der Rechtslage haben sich für die Beurteilung der Zentralen Kassenprüfung ebenfalls keine Änderungen ergeben.

Für die Zentrale Kassenprüfung der Lidl Stiftung & Co. KG waren im Rezertifizierungszeitraum keine technischen Änderungen notwendig. Das System benötigte keine Patches und es wurde auch kein neuer Release der Software entwickelt und herausgegeben.

14 Votum des Auditors

Hiermit bestätige ich, dass das oben genannte IT-Produkt den Rechtsvorschriften über den Datenschutz und die Datensicherheit in besonderer Weise entspricht. Der Auditor empfiehlt die Rezertifizierung.

Berlin 12.10.2015

Ort, Datum

Unterschrift des Sachverständigen
(rechtlich/technisch)