

Erklärung zum Datenschutz

Im Folgenden gibt die TC TrustCenter GmbH eine Erklärung über die Einhaltung der Vorgaben der Datenschutzgesetze ab. Es wird beschrieben welche Maßnahmen getroffen wurden, um ein hohes Datenschutzniveau zu gewährleisten.

1 Anwendungsbereich

TC TrustCenter betreibt sein Rechenzentrum in Deutschland und unterliegt so dem deutschen und europäischen Recht. Insbesondere sind das Bundesdatenschutzgesetz, das Signaturgesetz, das Telemediengesetz sowie das Telekommunikationsgesetz auf die Dienste von TC TrustCenter anwendbar.

Diese Erklärung zum Datenschutz bezieht sich auf alle von TC TrustCenter auf seinen Webseiten angebotenen Produkte und Dienstleistungen. Weitere Erklärungen zum Datenschutz hinsichtlich der Nutzung der Webseiten von TC TrustCenter finden sich unter: <http://www.trustcenter.de/880.htm>

TC TrustCenter unterscheidet nicht zwischen Daten von Kunden aus Ländern mit einem hohen Niveau einer Datenschutzgesetzgebung und solchen aus Ländern mit niedrigem Niveau oder keiner Datenschutzgesetzgebung. Da die Datenschutzgesetzgebung innerhalb der EU den höchsten Schutz weltweit bietet, erachtet es TC TrustCenter als ausreichend, wenn dieser Schutz gewährleistet ist.

2 Technische und organisatorische Maßnahmen

Da die TC TrustCenter GmbH den deutschen Datenschutzbestimmungen unterliegt, hat TC TrustCenter die Vorgaben an die technischen und organisatorischen Maßnahmen nach § 9 BDSG zu erfüllen. Die folgenden Aussagen in den Ziffern 2.1 bis 2.7 stellen einen Auszug aus den Datenschutz-, bzw. Sicherheitskonzept von TC TrustCenter dar und sind um Detailbeschreibungen gekürzt, deren Kenntnis durch unberechtigte Dritte die Sicherheit von TC TrustCenter gefährden könnte.

2.1 Zutrittskontrolle

Die Server von TC TrustCenter stehen in einem Sicherheitsbereich. Dieser wurde nach Anforderungen des deutschen Signaturgesetzes und des Grundschutzhandbuchs des Bundesamtes für Sicherheit in der Informationstechnologie so gestaltet, dass es ein Zutrittskontrollsystem, eine Alarmanlage und eine permanente Videoüberwachung gibt. Im Sicherheitsbereich befinden sich mehrere Serverräume. Die Serverräume können nur von berechtigten Mitarbeitern der Produktion betreten werden.

Ebenfalls im Sicherheitsbereich befindet sich, in einem gesonderten Raum, das Archiv, in dem auch Datenträger gelagert werden. Eine externe Lagerung der Datenbestände wird im Auftrag von TC TrustCenter durchgeführt.

Die Terminals der Mitarbeiter, auf denen die Clients laufen, sind handelsübliche PCs bzw. Notebooks. Diese Rechner befinden sich ebenfalls im Sicherheitsbereich und sind somit nur befugtem Personal zugänglich. Sie sind durch Benutzername und Passwort sowie durch eine

eine rollenzugewiesene Berechtigungsvergabe vor unberechtigtem Zugriff abgesichert. Die Mitarbeiter sind verpflichtet, hinreichend sichere Passwörter zu wählen und diese regelmäßig zu ändern.

2.2 Zugangskontrolle

Personenbezogene Daten sind in verschiedenen Datenbanken gespeichert. Die Kundendatenbank wird auf zwei TC TrustCenter-internen Servern betrieben. Eine weitere Datenbank sowie der X.500 Verzeichnisdienst speichern Zertifikatsdaten, diese Daten stehen auf den vom Internet zugänglichen Webservern zur Verfügung. Die Datenbank des Verzeichnisdienstes für qualifizierte Zertifikate enthält nur die abrufbaren qualifizierten Zertifikate. Die Daten auf den Webservern sind, wie gesagt, Zertifikatsdaten, deren Veröffentlichung die Kunden zugestimmt haben. Softwareseitig sind alle Tools zur Datenbearbeitung mit Client-Authentisierung ausgestattet.

2.3 Zugriffskontrolle

Durch ein Rollenkonzept und verschiedene Benutzergruppen wird der Zugang zur Kundendatenbank, den anderen Datenbanken, den Betriebssystemen und den installierten Applikationen verhindert, wenn er nicht wirklich erforderlich ist.

Darüber hinaus bestehen diverse technische Vorkehrungen, wie etwa physikalischer Zugang nur mit persönlicher SmartCard, starke Authentisierung für HTML Clients über Zertifikate oder verschlüsselter Datenaustausch via SSL.

Eingaben in die Kundendatenbank werden durch Mitarbeiter der Registrierungsstelle und durch automatische Prozesse durchgeführt. Die Verhinderung unbefugten Zugriffs erfolgt unter anderem durch folgende Maßnahmen: Zugangbeschränkung über ein TC Class 3-Zertifikat, Rollen- und Rechtekonzept, konsequentes Setzen der entsprechenden Zugriffskontrolllisten innerhalb der Datenverarbeitungssysteme, Protokollierung von Veränderungen und Löschungen, Unerreichbarkeit von Datenverarbeitungssysteme hinter Firewalls von außen, Benutzerkennungen, Passwortschutz mit Passwortwahl durch Mitarbeiter, Abmeldegebot, durch eingeschränkter Rechteerweiterung, Transportkontrolle getrennt nach gegenständlichem und nicht-gegenständlichem Transport von Daten, Datenträgerkontrolle sowie einer Übermittlungskontrolle.

2.4 Weitergabekontrolle

Der Transport von Daten ist in den nicht-gegenständlichen und gegenständlichen Transport zu trennen.

Personenbezogene Daten können sowohl von Webservern als auch aus der Kundendatenbank übermittelt werden. Das Herunterladen von Webservern wird durch Log-Dateien protokolliert. Ein direktes Übermitteln von Daten aus der Kundendatenbank ist nicht möglich. Eine Umgehung der technischen Maßnahmen ist nur durch Netzwerkadministratoren nach Genehmigung zulässig und wird protokolliert. TC TrustCenter die Daten nur verschlüsselter Form versendet. Hierbei werden entweder die Datensätze oder die Verbindung verschlüsselt. Insbesondere wird bei Zertifikate gekennzeichnet, ob diese öffentlich abrufbar sein sollen.

Ein gegenständlicher Transport von Datenträgern kann zum Kunden oder dem zum externen Backup-Dienstleister zu unterscheiden. Datenträger, die zum Kunden gesandt werden, sind

zum einen SmartCards und zum anderen Disketten sind speziell gesichert. Die Sicherung der Daten die zu einem externen Backup-Dienstleister erfolgt nach anerkannten und langfristig etablierten Verfahren. Der Backup-Dienstleister hat keinen Zugriff auf die Daten selbst.

2.5 Eingabekontrolle

Jede Änderung der Kundendatenbank wird mit Bearbeiter-ID in Log-Files protokolliert. Daten, die verändert wurden, werden nicht verworfen, sondern in einem gesonderten Bereich der Datenbank permanent gespeichert. Soweit das die Kundendatenbank betrifft, geschieht dies über einen speziell von TC TrustCenter implementierten Backup-Mechanismus.

Weil sich jeder Nutzer anmelden muss, wird vom dem System registriert, wer wann welche Handlung ausführt.

2.6 Auftragskontrolle

Das Modell von TC TrustCenter sieht vor, dass sowohl einzelne Personen als auch Organisationen ihre Daten von TC TrustCenter verarbeiten lassen können. TC TrustCenter legt den Begriff des Auftraggebers bewusst weit aus, da im Rahmen der angebotenen Zertifizierungsdienste, sowohl bei regulierten als auch bei nicht regulierten Verfahren, auf Grund der Vorgaben des § 14 SigG der Zertifikatsinhaber als Betroffener i. S. d. Datenschutzes immer Kenntnis über die Verarbeitung seiner Daten durch den Zertifizierungsdiensteanbieter haben muss. Zum Begriff der Organisation ist auszuführen, dass hiermit generell alle nicht individuellen Zertifikatsinhaber gemeint sind, die bei TC TrustCenter die Verarbeitung von Daten in Auftrag geben. In der Zertifizierungspraxis von TC TrustCenter sind dies sowohl privatwirtschaftliche Unternehmen, die Mitarbeiter- und Kundendaten verarbeiten lassen, als auch öffentliche Stellen, wie Behörden oder Anstalten des öffentlichen Rechts.

2.7 Verfügbarkeitskontrolle

Es wird eine externe Backup-Lagerung für kritische Daten vorgenommen. Diese externe Auslagerung erfüllt Sicherheitskriterien wie einer automatische Alarmschaltung zur Feuerwehr und Polizei, permanente Videoüberwachung, keine unkontrollierte Begehrbarkeit, Zugangskontrollen oder Sicherheitsschleusen, sowie festgelegte Prozeduren für Datenträgertausch, Sonderabrufe, Legitimationen und der Verschwiegenheitsverpflichtung aller Mitarbeiter.

Das Notstrommanagement wird durch eine unterbrechungsfreie Stromversorgung (USV) und durch einen Notstromdieselgenerator als infrastrukturelle Maßnahmen sichergestellt.

2.8 Trennungsgebot

Es ist zwischen den verschiedenen Arten von Daten, die bei TC TrustCenter verarbeitet werden zu differenzieren.

Zunächst werden Daten erhoben die zur Zertifikatesausstellung benötigt und nur in diesem Rahmen verarbeitet werden.

Davon zu unterscheiden sind die Rechnungsdaten, die auf einem zweiten System verarbeitet werden, das hiervon physikalisch getrennt ist.

Des Weiteren gibt es Kundendaten, die nicht im operativen Betrieb des Zertifizierungsdiensteanbieters anfallen, sondern die vom Vertrieb und Marketing zu Vertriebs- und Werbezwecken in einem wieder dritten System verarbeitet werden.

Letztlich, auf einem vierten System, werden Mitarbeiterdaten verarbeitet.

Hauptmerkmal ist auf die Zertifikatsdaten zu legen. Dieses System ist so aufgesetzt, dass es mandantenfähig ist. Daten von verschiedenen Kunden, bzw. aus verschiedenen Produktlinien werden nicht miteinander vermischt. Die in der Datenbank enthaltenen Daten werden nach der Ausstellung eines Zertifikates nur für die Dienste eines Zertifizierungsdiensteanbieters, wie dem Verzeichnisdienst und dem Sperrdienst, vorgehalten.

2.9 Certification Practice Statement

Die weiteren technischen und organisatorischen Maßnahmen, die TC TrustCenter ergriffen und umgesetzt hat, um ein hohes Niveau des Datenschutzes sicherzustellen, sind in dem Certification Practice Statement – kurz CPS genannt – zu finden: www.trustcenter.de/cps

2.10 Auditierung

Bestimmte Zertifizierungsdienste von TC TrustCenter, wie etwa für QSign (konform zum deutschen Signaturgesetz) oder Dienste nach Class 2 (konform zu ETSI TS 102042 LCP)- oder Class 3 (konform zu ETSI 102042 NCP) werden regelmäßig durch eine anerkannte Prüf- und Bestätigungsstelle auditiert. Die Auditierung umfasst auch die zuvor genannten Aussagen.

3 Allgemeine Aussagen

3.1 TC TrustCenter wird nur die personenbezogenen Daten erheben, verarbeiten und nutzen, die für die Durchführung der Zertifizierungs- oder anderer Dienste notwendig sind. TC TrustCenter bietet auch Kreditkartenzahlung an und erhebt hierfür solche Kreditkarteninformationen, die für die Zahlungsabwicklung notwendig sind und leitet diese Daten zur Zahlungsabwicklung an Zahlungsdienstleister weiter.

Die Kreditkarteninformationen werden verschlüsselt bei TC TrustCenter gespeichert. Eine weitergehende Nutzung findet nicht statt.

3.2 TC TrustCenter erhebt keine Daten über die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit, über Gesundheit oder das Sexualleben, strafbare Handlungen oder Ordnungswidrigkeiten.

3.3 TC TrustCenter wird personenbezogene Daten nur auf Grundlage von vertraglichen Vereinbarungen oder gesetzlicher Anforderungen veröffentlichen oder weitergeben. In diesen Fällen wird TC TrustCenter den Betroffenen hierüber umgehend informieren.

3.4 Bei der Erhebung personenbezogener Daten durch TC TrustCenter lässt sich TC TrustCenter die Einwilligung des Kunden zur datenschutzkonformen Verarbeitung dieser Daten geben. Erfolgt die Erhebung durch einen Dritten, ist dieser Dritte verpflichtet, diese

Einwilligung einzuholen. Zur Überprüfung der Daten hat TC TrustCenter das Recht, Auskünfte bei Dritten zu erheben und insbesondere Datenbanken Dritter zu nutzen.

3.5 TC TrustCenter verkauft oder handelt nicht mit personenbezogenen Daten. TC TrustCenter tauscht diese nicht mit Dritten aus und macht diese nicht Dritten zugänglich, soweit dies nicht durch bindendes Recht verlangt wird.

3.6 TC TrustCenter nutzt personenbezogene Daten nicht, um Nutzerprofile zu erstellen. TC TrustCenter behält sich das Recht vor, Kundendaten und somit auch personenbezogene Daten zu eigenen Zwecken auszuwerten.

3.7 Falls vertraglich vereinbart, kann TC TrustCenter Referenzkunden benennen. In keinem Fall werden personenbezogene Daten genannt.

3.8 Im Rahmen der Kommunikation mit dem Kunden wird TC TrustCenter personenbezogene Daten nur für Mitteilungen nutzen, die das Produkt des Kunden betreffen. Für Werbung über andere Produkte von TC TrustCenter werden die Informationen nur dann genutzt, wenn der Betroffene dem ausdrücklich zugestimmt hat, wie zum Beispiel für Newsletter.

3.9 TC TrustCenter zertifiziert nur die Informationen, die in einem Zertifikat enthalten sind. Mit der Zertifizierung werden keine weiteren Aussagen über den Kunden wie etwa seine Kredit- oder Vertrauenswürdigkeit gemacht. Insbesondere werden keine Aussagen über das Datenschutzniveau der Kunden getätigt.

3.10 Alle Mitarbeiter von TC TrustCenter sind auf das Datengeheimnis verpflichtet worden und haben an Schulungen zum Datenschutz teilgenommen. Weiter sind alle Mitarbeiter allgemein auf das Geschäfts- und Betriebsgeheimnis verpflichtet worden. Von allen Mitarbeitern liegen einwandfreie Führungszeugnisse vor.

3.11 Betroffene, deren personenbezogene Daten von TC TrustCenter gespeichert werden, können gemäß § 19 BDSG bei TC TrustCenter Auskunft verlangen über die zu ihrer Person gespeicherten Daten, auch soweit sie sich auf die Herkunft dieser Daten beziehen, Empfänger oder Kategorien von Empfängern, an die Daten weitergegeben werden, und den Zweck der Speicherung.

3.12 TC TrustCenter hat einen betrieblichen Datenschutzbeauftragten bestellt. Hinweise, Fragen, Auskunftsersuchen, Anregungen oder Kritik können Sie an privacy@trustcenter.de richten.

Hamburg, im Oktober 2010