Technische und organisatorische Maßnahmen der dokuhaus Archivcenter GmbH

Inhaltsverzeichnis:

	Erstellt/Geändert	Geprüft	Freigegeben
	Frank Zenker	Dagmar Hentschel	Josef R. Weber
Datum	12.01.2012	25.01.12	31.01.12
Unterschrift			

1. Einleitung

Bei der dokuhaus Archivcenter GmbH werden Sozialdaten der Auftraggeber erhoben und verarbeitet. Diese unterliegen generell einem besonderen Schutz.

Werden Sozialdaten automatisiert verarbeitet oder genutzt, ist die innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dazu gehört auch, dass die Zugriffe auf Sozialdaten, aber auch auf Daten der dokuhaus Archivcenter GmbH durch Berechtigungskonzepte geregelt werden.

2. Gesetzliche Grundlage

§ 78a SGB X Technische und organisatorische Maßnahmen

„Die in § 35 des Ersten Buches des Sozialgesetzbuches (SGB) genannten Stellen, die selbst oder im Auftrag Sozialdaten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen einschließlich der Dienstanweisungen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften des Gesetzes, insbesondere die in der Anlage zu dieser Vorschrift genannten Anforderungen zu gewährleisten. Maßnahmen sind nicht erforderlich, wenn ihr Aufwand in keinem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht."

Anlage zu § 78a SGB X

„Werden Sozialdaten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden Sozialdaten oder Kategorien von Sozialdaten geeignet sind."

a. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen Sozialdaten verarbeitet oder genutzt werden, zu verwehren. (Zutrittskontrolle 3.1),

b. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle 3.2),

c. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass Sozialdaten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle 3.3),

d. zu gewährleisten, dass Sozialdaten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung von Sozialdaten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle 3.4),

e. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem Sozialdaten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle 3.5),

f. zu gewährleisten, dass Sozialdaten, die im Auftrag erhoben, verarbeitet oder genutzt werden, nur entsprechend den Weisungen des Auftraggebers erhoben, verarbeitet oder genutzt werden können (Auftragskontrolle 3.6),

g. zu gewährleisten, dass Sozialdaten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle 3.7),

h. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Sozialdaten getrennt verarbeitet werden können (Trennungsgebot 3.8).

3. Maßnahmen der dokuhaus Archivcenter GmbH zur Umsetzung

3.1 Zutrittskontrolle

„Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen zu verwehren, mit denen Sozialdaten verarbeitet oder genutzt werden."

Die Zutrittsberechtigung in das Gebäude der dokuhaus Archivcenter GmbH wird durch einen entsprechenden personalisierten Transponder (Chip) für alle Mitarbeiter der dokuhaus Archivcenter GmbH sichergestellt. Gäste und Dritte müssen nach persönlicher Anmeldung im I.OG (Empfang) ausschließlich von einem Mitarbeiter der dokuhaus Archivcenter GmbH dort abgeholt und für die Dauer ihrer

Tätigkeit von einem Mitarbeiter der dokuhaus Archivcenter GmbH beaufsichtigt werden. Besucher und Techniker erhalten für ihren Aufenthalt einen eigens dafür ausgestellten Besucherausweis, der nach Ende des Aufenthaltes von einem Mitarbeiter des Sekretariats der dokuhaus Archivcenter GmbH entgegen zu nehmen ist. Der Zugang für Gäste und Dritte ist ausschließlich über den Haupteingang des Gebäudes möglich.

Anlieferunternehmen erhalten nach persönlicher Anmeldung im Lagerbüro (EG) den entsprechenden Entladebereich mitgeteilt. Für die Dauer Ihrer Tätigkeit werden die Anlieferunternehmen von einem Mitarbeiter der dokuhaus Archivcenter GmbH beaufsichtigt.

Sämtliche Schlüssel und Transponderausgaben werden in einem Schlüsselausgabeverzeichnis dokumentiert. Diese wird durch einen Verantwortlichen in der Verwaltung geführt. Bei Verlust oder Entwendung eines Schlüssels bzw. Transponders ist der Verantwortliche in der Verwaltung unverzüglich zu informieren.

Die Technikräume sind permanent abgeschlossen. Zutritt zu den Datenverarbeitungsanlagen haben ausschließlich die Mitarbeiter der EDV und der Datenschutzbeauftragte. Für alle Techniker und Dritte werden Anwesenheitsaufzeichnungen geführt.

Außerhalb der Betriebszeiten erfolgt eine Überwachung durch einen externen Dienstleister, in dieser Zeit ist die Gebäude-Alarmanlage aktiviert mit einer Verbindung zum externen Wachdienst, Polizei und Feuerwehr.

3.2 Zugangskontrolle

„Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können."

Die unbefugte Nutzung von Datenverarbeitungssystemen wird durch folgende Maßnahmen verhindert:

Die Authentifizierung erfolgt durch Benutzernamen in Kombination mit einem gültigen Passwort. Jeder Berechtigte verfügt über ein eigenes, nur ihm bekanntes Passwort.

Das Passwort für die Anmeldung in der Domäne der dokuhaus Archivcenter GmbH ist analog der Standardpasswortrichtlinien für Windows Server 2008 aufgebaut. Das Passwort ist ein Jahr gültig. Nach 3 ungültigen Versuchen wird der

Benutzer für das System gesperrt. Die Entsperrung des Benutzers ist nur durch den Systemadministrator möglich.

3.3 Zugriffskontrolle

„Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können. Auch ist zu gewährleisten, dass Sozialdaten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können."

Das unbefugte Lesen, Kopieren, Verändern oder Entfernen von Datenträger wird durch folgende Maßnahmen verhindert:

Es werden an allen Arbeitsplätzen in den Geschäftsräumen der dokuhaus Archivcenter GmbH die USB Schnittstellen zum unbefugten kopieren von Daten gesperrt. Sämtliche Daten werden auf zentralen Speicherplätzen der Server gespeichert und sind somit nicht frei zugänglich. Über eine zentrale Rechteverwaltung wird der Zugriff auf die Daten geregelt. Der Systemadministrator gibt die entsprechenden Daten für das System und die Benutzer frei.

An den Arbeitsplätzen werden nur die für die jeweilige Arbeit erforderlichen Schnittstellen freigegeben.

Alle Zugriffsberechtigungen bei der dokuhaus Archivcenter GmbH erfolgen anhand von eindeutig definierten und zugewiesenen Berechtigungsprofilen.

Datenträger, die der dokuhaus Archivcenter GmbH von Auftraggebern zur Verfügung gestellt werden, werden im Safe aufbewahrt und ggf. auf Anweisung des Auftraggebers nach den Bestimmungen des BDSG vernichtet.

Die dokuhaus Archivcenter GmbH arbeitet bei der Vernichtung mit zertifizierten Dienstleistern zusammen. Die Dienstleister sind ebenfalls nach ISO 9001:2008 zertifiziert. Dieses wird in regelmäßigen Abständen durch die dokuhaus Archivcenter GmbH kontrolliert und dokumentiert.

3.4 Weitergabekontrolle

„Es ist zu gewährleisten, dass Sozialdaten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Es muss überprüft und festgestellt werden können, an welchen Stellen eine Übermittlung von Sozialdaten durch Einrichtungen zur Datenübertragung vorgesehen ist."

Das unbefugte Lesen, Kopieren, Verändern oder Entfernen von Daten bei der Übertragung sowie beim Transport von Datenträgern wird durch folgende Maßnahmen verhindert:

Sozialdaten und personenbezogene Daten werden nur unter Einsatz geeigneter Verschlüsselungsverfahren elektronisch übertragen. Dies gilt auch für die Anlagen. Dabei nutzt die dokuhaus Archivcenter GmbH Verschlüsselungsverfahren der TC TrustCenter GmbH

Müssen Daten per Datenträger versandt werden, werden die Daten verschlüsselt und mit Empfangsbestätigung verschickt.

3.5 Eingabekontrolle

„Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem Sozialdaten in Daten Verarbeitungssysteme eingegeben, verändert oder entfernt worden sind."

Ob und von wem Daten in die Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, kann durch Auswertung der Ereignisprotokolle, Logfiles sowie des Fallverlaufs nachträglich überprüft und festgestellt werden. In der Regel werden die Daten nach 3 Monaten gelöscht bzw. vernichtet. Im Verfahrensverzeichnis werden über die ausgelagerten Daten gesonderte Reglungen getroffen.

3.6 Auftragskontrolle

„Es ist zu gewährleisten, dass Sozialdaten, die im Auftrag erhoben, verarbeitet oder genutzt werden, nur entsprechend den Weisungen des Auftraggebers erhoben, verarbeitet oder genutzt werden können."

Die dokuhaus Archivcenter GmbH gewährleistet, dass die Verarbeitung personenbezogener Daten im Auftrag nur entsprechend den Weisungen des Auftraggebers erfolgt. Der Aufraggeber bleibt mittelbarer Besitzer aller Daten. Nur mit Zustimmung des Auftraggebers erfolgt eine Weiterbeauftragung von Leistungen an Subunternehmen. Insbesondere bei der Aktenvernichtung wird gewährleistet, dass die entsprechenden Unternehmen den datenschutzrechtlichen Ansprüchen der dokuhaus Archivcenter GmbH bzw. der Auftraggeber entsprechen.

3.7 Verfügbarkeitskontrolle

„Es ist zu gewährleisten, dass Sozialdaten gegen zufällige Zerstörung oder Verlust geschützt sind."

Durch ein tägliches Backup mit einer Revisionsmöglichkeit von sieben Tagen wird gewährleistet, dass die Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Bei der dokuhaus Archivcenter GmbH gibt es einen Notfallplan. Ein zweiter Standort für die Ablage der elektronischen Daten (Datenbank) sichert die Verfügbarkeit im Notfall. Bei Ausfall der technischen Einrichtungen ist die wieder Inbetriebnahme und Störungsbeseitigung durch einen externen Dienstleister gesichert. Die Verfügbarkeit wird durch den externen Dienstleister in 24h gewährleistet. Durch bestimmte technische Voraussetzungen (Notfall Laptop) wird der Zugriff auf die Kundendatenbank in dieser Zeit durch die dokuhaus Archivcenter GmbH gewährleistet.

3.8 Trennungsgebot

Alle Kunden und Mitarbeiterdaten werden in einem Lager- und Verwaltungsprogramm verarbeitet. Dort sind alle Kundendaten und Mitarbeiterdaten in unterschiedlichen Datenbanken abgelegt. Der Zugriff auf diese Daten wird durch ein getrennt vom System laufendes Berechtigungssystem geregelt. Dies erfolgt durch Eingabe eines Benutzernamen und Passwortes.

4. Organisation

Die innerbetriebliche Organisation ist durch folgende Maßnahmen so gestaltet, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Die Bestimmungen des BSI zum IT-Grundschutz werden sichergestellt und regelmäßig überprüft.

Alle Mitarbeiter der dokuhaus Archivcenter GmbH sind mit Aufnahme der Beschäftigung auf das Datengeheimnis nach § 5 Bundesdatenschutzgesetzt verpflichtet. Zusätzlich erfolgt eine Verpflichtung nach § 1 des Gesetzes über die förmliche Verpflichtung nichtbeamteter Personen (Verpflichtungsgesetz) vom 2.Mätz 1974 (BGBI. I S. 547)

Es werden regelmäßige Schulungen im Rahmen der DIN EN ISO 9001:2008 zum Datenschutz sowie zum IT Grundschutz nach dem BSI durchgeführt.

Es wurde nebenamtlich schriftlich ein Datenschutzbeauftragter bestellt, der der Geschäftsleitung direkt unterstellt ist. Sein Aufgabengebiet erstreckt sich in seiner Funktion als DSB u. a. auf die regelmäßige Schulung von Mitarbeitern zu Themen Datenschutzes, Führung und Überprüfung der Verfahrensverzeichnisse, Beratung der Geschäftsleitung zum Datenschutz sowie die Überprüfung der externen Dienstleister hinsichtlich der Einhaltung zum Datenschutz.

Es wird ein Sicherheits- und Notfallkonzept in Abstimmung mit der Geschäftsleitung, dem IT Verantwortlichen, sowie dem DSB erstellt und regelmäßig überprüft werden.

Für sämtliche Prozesse und Verfahren, die Themen des Datenschutzes tangieren, werden entsprechende Arbeits- und Dienstanweisungen erstellt.

Die dokuhaus Archivcenter GmbH führt zu den Themen Datensicherheit und Datenschutz regelmäßig interne Schulungen durch. Weiterhin ist das Thema Teil der Zertifizierung nach DIN EN ISO 9001:2008.