Jahresbericht 2017

über den Stand der Umsetzung

Datenschutz Grundschutzes

gemäß definiertem Schutzzweck

bei der

ecs electronic cash syländer gmbh

Aichet 5

83137 Schonstett

erstellt durch

Lothar Becker
Dipl. Betriebswirt

DSZ Datenschutzauditor - Datenschutzauditor TÜV Rheinland

Datenschutz & IT
Thalacker 5a

83043 Bad Aibling
Tel.: +49 (0)8061/495743
Fax: +49 (0)8061/495744
Email: info@datenschutz-it.de
Web: www.datenschutz-it.de

Inhaltsverzeichnis

1 Kontaktdaten

1.1 Kanzleidaten

Name	ecs electronic cash syländer gmbh,
Strasse / Ort	Aichet 5, 83137 Schonstett
Telefon / Fax	+49 (0) 80 55 / 909 - 0 +49 (0) 80 55 / 909 - 109
EMail	info@sylaender.de

1.2 Datenschutzbetreuung

Name	Datenschutz & IT
Strasse / Ort	Thalacker 5a, 83043 Bad Aibling
Telefon / Fax	+49 (0)8061/4957-43 / +49 (0)8061/4957-44
Internet / EMail	www.datenschutz-it.de / info@datenschutz-it.de

1.2.1 Berater von Datenschutz & IT

Name	Funktion	Telefon	EMail
Lothar Becker	Datenschutz Auditor	+49 (0)8061/4957-43	lothar.becker@datenschutz-it.de

2 Auftrag

Im Rahmen des Betreuungsauftrages der **ecs electronic cash syländer gmbh** wurde dieser Jahresbericht für 2017 erstellt.

Das Ergebnis dieses Berichtes gibt Aufschluss über die Umsetzung des Datenschutzes zur Erlangung des Grundschutzes gemäß den Vorschriften des BDSG und den Empfehlungen des BSI.

Schwerpunkte liegen im Bereich der Pflichten zur Erlangung des vom Bundesdatenschutzgesetz (BDSG) geforderten Grundschutzes und der technischen und Organisatorischen Maßnahmen gem. § 9 BDSG.

3 Pflichten zur Umsetzung des Datenschutzes

Die **ecs electronic cash syländer gmbh** ist ein Unternehmen , das zum Zwecke der Durchführung von Handel, Vertrieb und Abrechnung von elektronischen Zahlungssystemen und deren Planung personenbezogene Daten erhebt, speichert, verarbeitet und ggf. übermittelt.

In diesem Zusammenhang werden auch personenbezogene Daten von Kunden, Lieferanten und Dienstleistern gemäß § 28 BDSG zur Erfüllung der Geschäftszwecke und von Mitarbeitern gemäß § 32 BDSG im Rahmen von Beschäftigungsverhältnissen erhoben, verarbeitet und genutzt.

Da diese personenbezogenen Daten in automatisierten Verfahren verarbeitet werden, unterliegen diese gemäß § 4d Abs. 1 BDSG der Meldepflicht, die jedoch entfällt, wenn ein betrieblicher Datenschutzbeauftragter bestellt wird. Ferner würde die Meldepflicht gemäß § 4d Abs. 3 BDSG entfallen, wenn das Unternehmen weniger als 10 Personen mit der Verarbeitung von personenbezogenen Daten beschäftigen würde. Gleichzeitig würde auch gemäß § 4f Abs. 1 BDSG die Pflicht zur Bestellung eines Datenschutzbeauftragten entfallen.

Da bei der **ecs electronic cash syländer gmbh** derzeit 15 mit der automatisierten Verarbeitung von personenbezogenen Daten beschäftigt sind bzw. im Rahmen ihrer Tätigkeit Kenntnis erlangen könnten, gilt o.g. Einschränkung nicht.

Daraus ergibt sich für die **ecs electronic cash syländer gmbh** die Pflicht zur Umsetzung des Datenschutzes und zur Bestellung eines betrieblichen Datenschutzbeauftragten.

3.1 Bestellung eines betrieblichen Datenschutzbeauftragten

Derzeit ist ein Datenschutzbeauftragter, der alle Voraussetzungen des § 4f Abs. 2 BDSG erfüllt, schriftlich bestellt.

3.2 Öffentliches Verfahrensverzeichnis für Jedermann

Es ist ein aktuelles öffentliches Verfahrensverzeichnis für "Jedermann" erstellt.

3.3 Internes Verarbeitungsverzeichnis

Es wird ein internes Verfahrensverzeichnis geführt, das alle Geschäftsprozesse beschreibt. Alle Verfahren wurden auf Datenschutzkonformität geprüft und freigegeben. Es bestehen keine Einschränkungen im Bezug auf die datenschutzgerechte Umsetzung.

3.4 Datenschutz- / IT-Sicherheitskonzept

Es liegt ein Datenschutz- und IT-Sicherheitskonzept vor.

3.5 Datenschutz-Policy für die Mitarbeiter

Aus dem Datenschutz- und IT-Sicherheitskonzept wurde ein Regelwerk zur datenschutzgerechten Arbeit mit personenbezogenen Daten in Form einer Datenschutz Mitarbeiter Policy erstellt. Diese wurde allen Mitarbeitern zur Durchsicht und zur Gegenzeichnung vorgelegt.

3.6 Geheimhaltungsverpflichtung gem. § 5 BDSG

Das BDSG schreibt im § 5 vor, dass jeder Mitarbeiter auf die Verschwiegenheit verpflichtet werden muss. Alle Mitarbeiter des Unternehmens sind auf Verschwiegenheit gem. § 5 BDSG verpflichtet.

3.7 Datenschutzschulung für die Mitarbeiter

Das BDSG schreibt im § 4g Abs. 1 S. 1 vor, dass die Mitarbeiter mit den besonderen Erfordernissen des Datenschutzes vertraut zu machen sind.

Hier sollten insbesondere die in der Datenschutz-Policy festgelegten Regeln und die wichtigsten Bestimmungen des BDSG vermittelt werden.

Alle Mitarbeiter werden regelmäßig in Form von Schulungen für die Gefahren bei der Arbeit mit personenbezogenen Daten sensibilisiert und in datenschutzkonformes Arbeiten eingewiesen. Für Anfang 2016 ist eine Schulung neuer Mitarbeiter geplant..

4 Technische und organisatorische Maßnahmen

Im § 9 + Anlagen BDSG ist vorgeschrieben, dass Unternehmen technische und organisatorische Maßnahmen im angemessenen Verhältnis zu ihrem Schutzzweck umsetzen müssen. Hier sind folgende Kontrollen definiert:

4.1 Zutrittskontrolle

Es muss gewährleistet sein, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren

Die Zutrittskontrolle ist dem Schutzzweck entsprechend umgesetzt. Unbefugte können Bereiche, in denen personenbezogene Daten verarbeitet werden weder eingesehen noch betreten. Besucher müssen am Eingang läuten und werden von Mitarbeitern in ein Besprechungszimmer geführt. Papierdokumente werden sicher in Archiven verwahrt, zu Druckern und Faxgeräten haben ausschließlich die Mitarbeiter Zutritt.

4.2 Zugangskontrolle

Es muss verhindert werden, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Die Zugangskontrolle ist durch geeignete Authentifizierungsverfahren dem Schutzzweck entsprechen umgesetzt. Regeln für Passwörter sind in einer Policy unternehmensweit festgelegt. Die Passwortlänge beträgt 11 Stellen, die Vergabe von Trivialpasswörtern ist nicht möglich und Passwörter werden regelmäßig gewechselt.

4.3 Zugriffskontrolle

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

In Unternehmensapplikationen und im Verzeichnissystem wird über Access Control Lists der Zugriff auf Daten so geregelt, dass unbefugte Zugriffe nicht möglich sind. Es wird durchgängig nach dem "Need-to-know" Prinzip verfahren.

4.4 Eingabekontrolle

Es muss gewährleistet werden, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Die Unternehmensaplikationen protokollieren alle Eingaben, Änderungen oder Löschungen, soweit dies technisch möglich ist. Somit kann weitgehend nachvollzogen werden, wer welche Daten erhoben, verarbeitet oder gelöscht hat.

4.5 Weitergabekontrolle

Es muss sichergestellt sein, dass personenbezogene Daten 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 personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Die Weitergabe der Daten erfolgt, soweit auf elektronischen Wege notwendig, weitgehend verschlüsselt. Sensible Emails werden verschlüsselt übertragen. Es sind keine Funknetzwerke im Einsatz. Eine Übertragung der Daten in Drittstaaten außerhalb der EU/EWR erfolgt nicht.

4.6 Auftragskontrolle

Im § 11 BDSG ist vorgeschrieben, dass Unternehmen, die Daten im Auftrag erfassen, verarbeiten oder nutzen, schriftlich zur Einhaltung der datenschutzrechtlichen Bestimmungen verpflichtet werden müssen. Diese Dienstleister sind sorgfältig auszuwählen und der Auftraggeber muss sich davon überzeugen, dass der Auftragnehmer datenschutzgerecht handelt.

Alle Dienstleister, die den Sachverhalt des § 11 BDSG erfüllen, wurden sorgfältig ausgewählt, überprüft und per Vertrag zur Einhaltung des Datenschutzes verpflichtet. Die technischen und organisatorischen Maßnahmen werden regelmäßig hinterfragt.

4.7 Verfügbarkeitskontrolle

Das BDSG, aber auch AO und GoBS schreiben vor, dass personen- und unternehmensbezogene Daten verfügbar gehalten werden müssen und diese bei Hard- oder Softwareproblemen, aber auch durch Katastrophen nicht verloren gehen dürfen.

Die Verfügbarkeitskontrolle ist dem Schutzzweck entsprechend umgesetz. Sicherungsbänder sind verschlüsselt und werden täglich extern gelagert.

4.8 Trennungsgebot

Das BDSG schreibt vor, dass Daten nur ihrem Erhebungszweck entsprechend verwendet werden dürfen. Für verschiedene Zwecke erhobene Daten müssen auch getrennt verarbeitet werden können.

Durch den Einsatz eines umfangreichen Berechtigungssystems ist die zweckgebundene Trennung von Daten im vollen Umfang gewährleistet. Die Vermischung von verschiedenen Kategorien von Personendaten oder unbefugte Zugriffe sind ausgeschlossen.

5 Abschließende Beurteilung

Dem Unternehmen kann bescheinigt werden, dass der Datenschutz konsequent und ohne Kompromisse umgesetzt wurde. Alle technischen und organisatorischen Maßnahmen sind schlüssig und tragen dem hohen Schutzbedarf Rechnung.

Bad Aibling, 25. Januar 2017

Lothar Becker
Dipl. Betriebswirt
DSZ Datenschutzauditor - Datenschutzauditor TÜV Rheinland