Technische und organisatorische Maßnahmen

Zur Erfüllung der Anforderungen an Datenschutz und Datensicherheit gemäß § 9 BDSG und der Anlage zu § 9 Satz 1 BDSG wurden von der Deutschen Post AG bei SIMSme umfangreiche technische und organisatorische Maßnahmen (TOMs) etabliert.

1 Zutrittskontrolle

Das Rechenzentrum ist nach ISO 27001 zertifiziert.

2 Zugangskontrolle

Das Rechenzentrum ist nach ISO 27001 zertifiziert.

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.

Hierzu sind folgende Maßnahmen eingeführt:

- Protokollierung befugter und unbefugter Zugriffsversuche
- Trennung von IT-System-Administrations- und –Nutzungsfunktionen
- Dokumentation von Änderungen der Zugriffsberechtigungen, wie Zuweisen, Ändern und Entziehen von Rechten
- Zeitliche Befristung von Benutzerkonten
- Dokumentation der Administration und der Veränderung von Benutzeridentitäten
- Regelmäßiger Rezertifizierungsprozess von Zugriffsberechtigungen

4 Weitergabekontrolle

Es ist zu gewährleisten, 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.

Hierzu sind folgende Maßnahmen eingeführt:

- Härtung der Verfahrensserver
- physikalische und logische Segmentierung des Netzwerks
- Schutz der Kommunikation und Schnittstellen

5 Eingabekontrolle

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

Hierzu sind folgende Maßnahmen eingeführt:

- Speicherung von unverschlüsselten personenbezogenen Daten ausschließlich im Rahmen der Benutzerregistrierung. Einziges personenbezogenes Datum ist die Mobilfunknummer.
- Bestätigung der Mobilfunknummer über SMS durch den Anwender.
- Zentrale, protokollierte Speicherung der Registrierungsdaten

6 Auftragskontrolle

Es ist zu gewährleisten, dass der Auftragnehmer den Auftraggeber bei der Durchführung der in dem Vertrag geregelten Kontrollen unterstützt.

Hierzu sind folgende Maßnahmen eingeführt:

- Falls Deutsche Post AG Auftraggeber ist: Verpflichtung des Auftragnehmers gemäß §11 BDSG
- Sonst: Verpflichtung des Unterauftragnehmers für Betriebs- und Wartungsaufgaben gemäß §11 BDSG

7 Verfügbarkeitskontrolle

Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Hierzu sind folgende Maßnahmen eingeführt:

- Durchführung Backup
- Redundante Auslegung zentraler Komponenten
- Etablierung einer geeigneten Viren-Schutzstrategie

8 Trennungsgebot

Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Hierzu sind folgende Maßnahmen eingeführt:

- Trennung von Produktiv- und Testsystemen
- Trennung von Mandaten durch kryptografische Verfahren