Technische und organisatorische Maßnahmen Sage Webshop

Stand: 13.5.2018, **Quelle:** ePages GmbH, Hamburg

Beschreibung der zwischen den Parteien vereinbarten technischen und organisatorischen Maßnahmen (im Folgenden „TOMs“) zum angemessenen Schutz der Daten des Auftraggebers nach Art. 32 DSGVO.

Vertraulichkeit (Art. 32 Abs. 1 lit.b DSGVO)

Zutrittskontrolle

Konkrete Maßnahmen, mit denen Unbefugten der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehrt wird:

- Zutritt nur über Chip-Karte (RFID)
- elektrische Türöffner

Rechenzentrum/ Data Center

- Zugang Rechenzentrum nur für autorisierte Mitarbeiter via Identifizierungsprotokolle: Berührungslos lesbare Karte, PIN, biometrischer Fingerabdruck
- Permanente Überwachung aller Zufahrten/Eingänge des Rechenzentrums
- Das Data Center (IPHH Internet Port Hamburg GmbH) ist ISO/IEC 27001:2013 zertifiziert (Zertifikat-Registrier-Nr.: 01 153 1600453)

Zugangskontrolle

Konkrete Maßnahmen, mit denen die Nutzung von Datenverarbeitungssystemen durch Unbefugte verhindert wird:

- Verbindung über SSH mit private_Key oder Passwort-Authentifizierung
- Verbindung von extern über IPsec VPN mit User-Login und PreSharedKey (Live Systeme)
- Sperrung des Logins bei 5 Fehlversuchen für 15min

Zugriffskontrolle

Konkrete Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugangsberechtigung 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:

- Zugriff nur für autorisierte Nutzer

Trennungskontrolle

Konkrete Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:

- getrennte Systeme für Live und Test
- Struktur: VM ohne Live-Daten; Testsystem; Live-System

Pseudonymisierung (Art. 32 Abs. 1 lit.a) DSGVO; Art. 25 Abs. 1 DS-GVO)

Konkrete Maßnahmen, die gewährleisten, dass die Verarbeitung von personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können (sofern zusätzliche Informationen gesondert aufbewahrt werden und entsprechenden technischen organisatorischen Maßnahmen unterliegen):

- Pseudonymisierung der IP-Adressen in Webserver-Log-Dateien

Integrität (Art. 32 Abs. 1 lit.b) DSGVO)

Weitergabekontrolle

Konkrete Maßnahmen, die 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:

- Verpflichtung der Mitarbeiter auf BSDG / DSGVO
- Sicherung gegen Zugriff auf Netzwerkebene
- Verschlüsselung von Daten

Eingabekontrolle

Konkrete Maßnahmen, die gewährleisten, dass nachträglich überprüft werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt werden können:

- Daten liegen im Auftragnehmer-internen Versionierungssystem und somit ist jederzeit nachvollziehbar, wer, wann, wo, welche Änderungen vorgenommen bzw. diese auf Providersystemen installiert hat

Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit.b) DSGVO)

Verfügbarkeitskontrolle

Konkrete Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

- Betrieb der Server und Backup von Datenbanken und Webroot gemäß internem Betriebshandbuch

Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit.c DSGVO)

- Grundinstallation kann anhand der im Versionierungssystem vorhandenen Daten jederzeit wiederhergestellt werden (Hard- und Software inklusive Installation)
- Wiederherstellung der Datenbanken kann durch Einspielen des entsprechenden Dumps erfolgen; das Wiederherstellen des Webroot-Verzeichnisses durch Einspielen des entsprechenden Backups

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit.d) DSGVO; Art. 25 Abs. 1 DSGVO)

Datenschutz-Management

Konkrete Maßnahmen, die gewährleisten, dass ein Datenschutz-Management zur Überwachung vorhanden ist:

- regelmäßige, außerplanmäßige und auf Incidents basierende Audits in den Lokationen des Auftragnehmers

Incident-Response-Management

Konkrete Maßnahmen, die gewährleisten, dass ein Incident-Response-Management vorhanden ist:

- gemäß Application Management Service Level Agreement

Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Konkrete Maßnahmen, die gewährleisten, dass durch Voreinstellungen grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden und personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden:

- IP-basiertes Whitelisting für Zugriff auf Server, Testsystem und interne Tools
- VPN-Verbindung von extern nur für dedizierte Nutzer

Auftragskontrolle

Konkrete Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können:

- schriftlicher Vertrag zwischen Auftraggeber und Auftragnehmer
- Datenverarbeitungszweck ist im Vertrag geregelt
- Datenverarbeitungszweck ist den entsprechenden Mitarbeitern bekannt
- Mitarbeiter erhalten Weisung zum Umgang mit personenbezogenen Daten