

Audit
Datenschutz + Datensicherheit
der
mailingwork GmbH, Chemnitz
sowie
w3work Gneuß & Arnold GbR, Oederan
Stand 28.04.2020

Die verbundenen Unternehmen sind als Dienstleister im Sinne des Art. 28 DSGVO tätig, Schwerpunkte Email-Marketing und Kommunikation. Ihre Auftraggeber verlangen regelmäßig im Rahmen der zu regelnden Auftragsverarbeitung einen Nachweis über das Schutzniveau (technische und organisatorische Maßnahmen – kurz TOM) der Unternehmen.

Bewertung / Einstufung

	Ergebnis	Handlungsbedarf
XXX	Ohne Risiko oder nur sehr geringes Risiko	keiner
	Einige Risiken liegen vor, die jedoch keiner sofortigen Abstellung bedürfen	vorhanden, jedoch sukzessive Bearbeitung möglich
	Erhebliche Risiken, eine Zusammenarbeit kann auf dieser Basis im Moment nicht empfohlen werden	dringend

Beschreibung / Zusammenfassung der bisherigen Audits

Die Unternehmen hatten sich im Frühjahr 2014 einer ersten Überprüfung durch a.s.k. Datenschutz unterzogen. Im Rahmen dieser Überprüfung wurden aus einem Pool von 250 Fragen insgesamt 165 auf die Unternehmen zutreffende Prüfpunkte eingehend beleuchtet. Basis der Überprüfung waren die technischen und organisatorischen Maßnahmen gemäß Anlage zu § 9 Bundesdatenschutzgesetz sowie relevante Punkte des BSI IT-Grundschutzkatalogs Standard. Nach einer anfänglichen Erfüllungsquote von 92% (Standard 65%) konnte durch konsequente Bearbeitung der identifizierten Schwachstellen zum Ende des damaligen Projekts im März 2015 eine Umsetzungsquote von weit überdurchschnittlichen 97,2% erreicht werden.

Im Herbst 2015 bezog die mailingwork GmbH am Standort Chemnitz neue Räumlichkeiten. Zur Sicherstellung und als weitere Belegmöglichkeit des Schutzniveaus hatten sich die Unternehmen Anfang 2016 erneut für eine Über- und Nachprüfung durch a.s.k. Datenschutz entschieden.



Ein einer eintägigen Vor-Ort-Bestandsaufnahme inklusive Begehung der neuen Räumlichkeiten am 03.02.2016 wurde das aktuelle Schutzniveau auf Basis der Ergebnisse aus 2014/2015 überprüft. Am neuen Standort sind im Rahmen der Begehung keine Mängel in der Objektsicherung aufgefallen. Durch eine konsequent weitergeführte Virtualisierung im Serverbereich konnte das bereits schon vorhandene Schutzniveau - gerade in Bezug auf Backup und Recovery - nochmals verbessert werden.

Neue oder geänderte Verfahren wurden zeitnah mit dem Datenschutzbeauftragten abgestimmt, der eng in die Auswahl und Entscheidungsfindung einbezogen ist. Die Dokumentationen des internen Datenschutzbeauftragten sind aktuell und nachvollziehbar. Die Mitarbeiterschulungen und Sensibilisierungen werden regelmäßig durchgeführt. Im Rahmen einiger Gespräche mit zufällig ausgewählten Mitarbeitern konnte eine hohe Sensibilität für die aktuelle Bedrohungslage und den Umgang mit Kundendaten festgestellt werden.

Im Rahmen neu eingeführter Verfahren wurden bei Vorliegen einer Auftragsdatenverarbeitung nach § 11 BDSG die betroffenen Dienstleister sorgfältig ausgewählt, der vorgeschriebenen Überprüfung des Schutzniveaus unterzogen sowie die notwendige Vereinbarung zur Auftragsdatenverarbeitung geschlossen.

Erhaltungsaudit 2017

Im Rahmen des Erhaltungsaudits am 28.07.2017 haben sich keine Veränderungen gegenüber den bisherigen Ergebnissen feststellen lassen.

Aufgrund des positiven Prüfergebnisses sind die Unternehmen berechtigt, das Zertifikat a.s.k. company**secure** weiterhin für einen Zeitraum von 24 Monaten ab Datum dieses Prüfberichts zu führen. Eine Nachprüfung zwecks Verlängerung des Zertifikats wäre im Sommer / Herbst 2019 vorzunehmen.



Erhaltungsaudit 2019/2020

Im Zuge der Aktualisierung und Anpassung auf die Anforderungen aus Art. 32 DSGVO Sicherheit der Verarbeitung haben sich die Unternehmen im Zeitraum 09/2019 bis 04/2020 einem weiteren Audit der technischen und organisatorischen Maßnahmen unterzogen.

Die bisher sehr guten Ergebnisse konnten trotz der Ausweitung des Prüfumfanges beibehalten werden.

Nach wie vor wird ein BSI zertifiziertes Rechenzentrum, Zertifikatsnummer BSI-IGZ-0303-2017 (gültig bis 16.12.2020) genutzt.

Simmelsdorf, den 28.04.2020

A handwritten signature in black ink, reading 'Sascha Kuhrau'. The signature is written in a cursive, slightly slanted style.

Sascha Kuhrau (Prüfer)