

Auditierung Datenschutz + Datensicherheit der Unternehmen mailingwork GmbH sowie w3work Gneuß & Arnold GbR, Oederan

Stand 26.03.2015

Die verbundenen Unternehmen sind als Dienstleister im Sinne des § 11 Bundesdatenschutzgesetz tätig, Schwerpunkte Email-Marketing und Kommunikation. Ihre Auftraggeber verlangen regelmäßig im Rahmen der zu regelnden Auftragsdatenverarbeitung einen Nachweis über das Schutzniveau (technische und organisatorische Maßnahmen) der Unternehmen.

Zur Sicherstellung und als weitere Belegmöglichkeit des Schutzniveaus haben sich die Unternehmen Anfang 2014 entschieden, eine externe Überprüfung durchführen zu lassen. Am 11.02.2014 wurde eine eintägige Vor-Ort-Bestandsaufnahme an den Standorten der Unternehmen durchgeführt. In der Folge wurden weitere Punkte anhand der vorgefundenen Begebenheiten ergänzt und ebenfalls gemeinsam mit dem Datenschutzbeauftragten des Unternehmens geprüft. Als Ergebnis liegt ein ausführlicher Audit-Bericht vor.

Basis des Audits sind die technischen und organisatorischen Maßnahmen gemäß Anlage zu § 9 Bundesdatenschutzgesetz sowie relevante Punkte des BSI IT Grundschutzkatalogs. Aus einem Pool von 250 Prüfpunkten konnten im Verlauf des mehrmonatigen Projekts 165 Fragen herangezogen werden. Das Audit wurde in drei Stufen bewertet: Bestandsaufnahme (Februar 2014), Überarbeitung (März - Dezember 2014), Finalisierung (Januar - März 2015).

Bereits im Rahmen Bestandsaufnahme haben die Unternehmen eine überdurchschnittliche Erfüllungsquote von 92% (Standard 65%) erreicht. In der zeitlichen Mitte des Projekts konnte durch Umsetzung erster konkreter Maßnahmen die Quote auf 95% gesteigert werden. In der abschließenden Bewertung haben die Unternehmen 953 von 980 möglichen Punkten erreicht (97,2%).

	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



Während der intensiven Zusammenarbeit mit den Mitarbeitern der Unternehmen ist aufgefallen, dass nicht nur der Datenschutzbeauftragte sehr aktiv und in alle Unternehmensprozesse eingebunden ist, sondern auch die Mitarbeiter das Thema Datenschutz im Arbeitsalltag leben. Durch regelmäßige Sensibilisierungen achten die Mitarbeiter kontinuierlich auf Datenschutz und Datensicherheit, und reduzieren somit die Risiken erheblich.

Neben der stetigen Weiterentwicklung der internen technischen und organisatorischen Schutzmaßnahmen legen die Unternehmen sehr großen Wert auf die Zuverlässigkeit und Sicherheit eingesetzter externer Dienstleister. So werden beim Outsourcing z.B. bei externem Hosting höhere Maßstäbe angelegt, als sie durch das Bundesdatenschutzgesetz vorgesehen sind. Neben dem Nachweis geeigneter Zertifizierungen durch den jeweiligen Dienstleister werden neuralgische Punkte beim Auslagern durch den Datenschutzbeauftragten zusätzlich persönlich vor Ort geprüft. Erst nach erfolgreicher Beseitigung möglicher Schwachpunkte wird die vorgeschriebene Vereinbarung zur Auftragsdatenverarbeitung geschlossen und die Zusammenarbeit begonnen.

Besonders hervorzuheben ist hier die Nutzung eines BSI zertifizierten Rechenzentrums, Zertifikatsnummer BSI-IGZ-0194-2014 (gültig bis 16.12.2017).

Aufgrund des positiven Prüfergebnisses sind die Unternehmen berechtigt, das Zertifikat **a.s.k. companysecure** für einen Zeitraum von 24 Monaten ab Ausstellung (26.03.2015) zu führen.



Das a.s.k. Zertifikat darf durch die Unternehmen sowohl in Print- als auch in Online-Medien verwendet werden. Bei Nutzung im Web ist das Logo mit der Seite <http://www.bdsge-externer-datenschutzbeauftragter.de> zu verlinken.

Eine Nachprüfung zwecks Verlängerung des Zertifikats wäre im Frühjahr 2017 vorzunehmen.

Simmelsdorf, den 26.03.2015

A handwritten signature in black ink that reads 'Sascha Kuhrau'.

Sascha Kuhrau