Technische und organisatorische Maßnahmen

des Auftragsverarbeiters

SUMUS Software GmbH
Zollernstraße 87
75328 Schömberg
Deutschland

Sitz der Gesellschaft: Schömberg (Kreis Calw)
Amtsgericht Stuttgart | HRB 786168
Geschäftsführer: Gordon Seipold

Telefon: +49 7084 976 976 1
E-Mail: datenschutz@sumus-software.com
Webseite: sumus-software.com

		Beim Auftragsverarbeiter realisierte Maßnahmen	
		technisch	**organisatorisch**
Zutrittskontrolle	**Zutrittskontrolle baulich**	• An- und Ablieferungen Sicherheitssystem: Übergabepunkte und Ladezonen von Datenverarbeitungsanlagen separiert. • Zutrittssicherung Gebäudetechnik: Verteilerräume oder -bereiche gegen unbefugten Zutritt gesichert • Existenz Sicherungsmaßnahmen gegen Überfälle • Existenz nicht maschineller Zutrittskontrollen	• Dokumentation der Zutrittskontrollmaßnahmen • Gebäude-Sicherheitskonzept geht auf Zutrittsmöglichkeiten ein
	Zutrittskontrolle organisatorisch		• Existenz Schlüssel- und Schließordnung
	Rechnerräume ("Closed Shop" - Betrieb)	• Netzwerkkomponenten zutrittsgesichert	• Festlegung Zutrittsbefugter Personen • Zutritt fremder Personen ist geregelt • Zutrittskontrollprüfungen für Wartungspersonal • Bewegungsfreiheit Wartungspersonal anhand vorher festgelegten Privilegien geregelt • Regelmäßiger Test der Schutzmaßnahmen
Zugangskontrolle	**Zugangskontroll-maßnahmen**	• Benutzerregistrierung zur Vergabe von Zugangsberechtigungen für alle Informationssysteme	• Regelwerk zur Zugangskontrolle
	Zugangssicherung Netzwerk	• Zugangsberechtigungen Netzwerkkomponenten • Kabelgebundener Netzwerkzugang: Network Admission Control	• Regelwerk zur Nutzung von Netzdiensten • Freigabe vor Netzzugang geregelt

		Beim Auftragsverarbeiter realisierte Maßnahmen	
		technisch	**organisatorisch**
		• Drahtloser Netzwerkzugang (WLAN) durchgängig gesichert	
	Zugangssicherung Wartung	• Identifikation / Authentisierung bei Zugang von externem Wartungspersonal • Kontrolle von Softwareänderungen bei Wartungseinsätzen	• Verfahren Passworte externes Wartungspersonal • Mitnahme DV-Equipment bei Wartungen geregelt
Zugriffskontrolle	**Zugriffsschutz-maßnahmen**	• Angabe letzter Nutzungszeitpunkt wo möglich • Einsatz von Verschlüsselung auf Datei- / Verzeichnisebene • Einsatz von Verschlüsselung für mobile Datenträger • Einsatz sicherer Verschlüsselungsalgorithmen • Einsatz von Mobile-Device-Management wo möglich • Einsatz von Zwei-Faktor-Authentifizierung wo möglich	• Regelungen hinsichtlich unbeaufsichtigter Benutzerausstattung • Clean Desk / Clear Screen Policy
	Sichere Entsorgung oder Weiterverwendung von Datenträgern / Sichere Löschung von Dokumenten	• Aktenschredder (Sicherheitsgrad mindestens P3)	• Entsorgung von Papierdokumenten und Datenträgern geregelt • Sichere Entsorgung oder Weiterverwendung von mit Speichermedien ausgestatten Geräten geregelt • Beachtung von Aufbewahrungsfristen
Weitergabe-kontrolle	**Verpflichtung der Mitarbeiter auf das Datengeheimnis**		• Verpflichtung erfolgt mit Arbeitsvertrag und in regelmäßigen Abständen • Informationsmaterial wird bereitgestellt

		Beim Auftragsverarbeiter realisierte Maßnahmen	
		technisch	**organisatorisch**
			• Erläuterungen erfolgen und allen Beteiligten sind daher die Belange der Datensicherheit und des Datenschutzes bekannt • Datenschutzschulungen erfolgen regelmäßig • Ausscheidende Mitarbeiter: Regelungen vorhanden
	Physische Datenübergabe	• Sicherheit bei physischer Übergabe durch geeignete Maßnahmen	• Verfahren mit Bezug zur Weitergabekontrolle sind bekannt • Weitergabe von Datenträgern zu Wartungszwecken oder zur Fehleranalyse erfolgt unter definierten Regeln • Datenübergabe nur gegen geeignete Belege • Richtigkeit Adressat wird überprüft
	Elektronische Datenübermittlung	• Protokollierung programmgesteuerter Übermittlungen • Datenverschlüsselung	• Übersicht automatisierter Datenübermittlungen vorhanden • Dokumentation der bei der Übermittlung eingesetzten Programme
	Anonymisierung / Pseudonymi-sierung	• Anonymisierung / Pseudonymisierung automatisiert	• Sicherstellung Nicht-Aufdeckung der Pseudonymisierung
Eingabekontrolle	**Protokolle**	• Schutz der Protokolldaten u.a. durch Verschlüsselung • Speicherung von Protokolldateien unter Beachtung von Löschfristen	• Zweckbestimmung von Protokolldateien • Regelmäßige Kontrollen der Handhabung und Löschfristen

		Beim Auftragsverarbeiter realisierte Maßnahmen	
		technisch	**organisatorisch**
Auftragskontrolle	**Vertragliche Verpflichtung**		• Vertragliche Verpflichtung aller Auftragsdatenverarbeiter
	Auswahl des Auftragnehmers		• Vorherige Information über den Auftragnehmer einholen • Dokumentation des Auswahlverfahrens
	Kontrolle		• Kontrolle der Auftragsdatenverarbeiter
	Weisungen		• Weisungsberechtigte des Auftraggebers sind bekannt • Weisungsempfänger bei dem Auftragnehmer sind bekannt • Schriftliche Weisungen erforderlich • Identitätsprüfung erfolgt
Verfügbarkeits-kontrolle	**Planung**	• Überschwemmungsschutz • Unterirdische Versorgungsleitungen	• Technische Infrastruktur wird regelmäßige überprüft
	Katastrophen-vorsorge und IT-Notfallkonzept	• Ausweichräume vorhanden • Existenz Backup-Rechenzentrum • Sicherstellung von Konnektivität in Notfällen • Aufbewahrung Verfahrensdokumentation Wiederanlauf	• Erreichbarkeit Hilfsorganisationen • Sichtbarkeit von Telefonnummern der Hilfsorganisationen • Regelung Weisungsbefugnisse im Katastrophenfall • Wiederanlaufplanung DV-Bereich im Katastrophenfall • Existenz Prioritätenliste • Existenz Notfallkonzept Netzwerk • Aktualität Verfahrensdokumentation Wiederanlauf • Notfallübungen

		Beim Auftragsverarbeiter realisierte Maßnahmen	
		technisch	**organisatorisch**
	Backupkonzept	• Verschlüsselte Backups an mindestens 2 voneinander getrennte Lokationen • Schutz vor Diebstahl oder Zerstörung • Funktionalitätstest	• Dokumentation der Anforderungen • Prozessbeschreibungen • Verantwortlichkeiten • Kapazitätsplanung
	Aufbewahrung von Geschäftsunter-lagen	• Ausgelagertes Katastrophenarchiv • Wiedervorlage Löschungsfrist	• Archivordnung • Zutritt zum Archiv geregelt • Archivverwalter ist bestimmt • Einlagerung und Ausgabe von Datenträgern bzw. Dokumenten ist geregelt • Löschungsfristen sind bekannt
	Sonstige Sicherheits-maßnahmen	• Dokumentation Schnittstellen IT- und Fachabteilungen	• Mitarbeiterschulungen zu Sicherheitsmaßnahmen • Kompetenzregelungen IT- und Fachabteilungen • Private Nutzung von unternehmenseigenen Laptops & Hardware ist geregelt
Trennungs-kontrolle	**Mandanten-fähigkeit**	• Mandantenfähigkeit der Systeme durch geeignete Maßnahmen durchgängig sichergestellt	• Alle betreffenden Verfahren sind hinsichtlich Mandantentrennung dokumentiert • Mandantenfähigkeit der Verfahren in der Verfahrensdokumentation nachvollziehbar dokumentiert • Mandantenfähigkeit der Verfahren in der Verfahrensdokumentation nachvollziehbar dokumentiert
	Trennung von Office-,	• Netztrennung: Office-, Entwicklungs-, Test- und Wirksysteme liegen in klar	• Konzept zur Gewinnung von und zum Umgang mit Testdaten liegt vor

		Beim Auftragsverarbeiter realisierte Maßnahmen	
		technisch	**organisatorisch**
	Entwicklungs-, Test- und Produktiv-umgebungen	voneinander getrennten Netzsegmenten, wo möglich physikalisch voneinander getrennt. • Testdaten: Entwicklungs- und Testsystem verarbeiten nur Testdaten • Anonymisierung: Testdaten, die aus Echtdaten abgeleitet werden, werden anonymisiert	