



Technische und organisatorische Maßnahmen (TOMs) nach Art. 32 DSGVO

Stand: 18.05.2018

1. Zutrittskontrolle

Unbefugter Zutritt zum Gebäude der opwoco GmbH wird durch eine Videoüberwachung, eine Einbruchmeldeanlage sowie Sicherheitsschlösser inkl. personenbezogener Kennnummer verhindert. Darüber hinaus ist das Rechenzentrum der opwoco GmbH zusätzlich verschlossen und durch eine eigene Einbruchmeldeanlage gesichert – Zutritt hierzu hat nur ein ausgewählter Mitarbeiterkreis.

2. Zugangskontrolle

Der Zugang zu den IT-Systemen erfolgt mit Authentifizierung durch individuelle Benutzerkennung und Passwort. Berechtigungen werden nach einem Zugangsberechtigungskonzept vergeben. Die Systeme sind gegen unberechtigten Zugang z.B. durch eine Firewall gesichert.

3. Zugriffskontrolle

Differenzierte Berechtigungen sind in den IT-Systemen festgelegt. Der Zugriff entsprechend Berechtigung wird auch bei Verfahren zur Wiederherstellung von Daten aus Backups gewahrt.

4. Weitergabekontrolle

Alle Mitarbeiter der opwoco GmbH werden auf das Datengeheimnis nach Art. 28 Abs. 3 Satz 2 lit. b DSGVO verpflichtet. Soweit erforderlich werden die Daten gegen Zugriffe auf Netzwerkebene geschützt. Grundsätzlich erfolgt keine Weitergabe der Daten an Dritte (Ausnahme: Subunternehmer, die durch einen gesonderten Vertrag zur Auftragsdatenverarbeitung gemäß DSGVO auf den Datenschutz verpflichtet sind.).

5. Eingabekontrolle

Differenzierte Berechtigungen sind in den IT-Systemen festgelegt. Bestimmte personenbezogenen Daten können automatisch bei Zugriffen auf den Webserver ermittelt und gespeichert werden. Für den Benutzer besteht keine Möglichkeit, diese Daten einzugeben, zu verändern oder zu löschen. Es existiert zusätzlich auch keine Web- oder Software-Oberfläche um diese Daten einzusehen oder zu bearbeiten.

6. Auftragskontrolle

Die opwoco GmbH schließt auf Wunsch einen schriftlichen Vertrag, der den Datenverarbeitungszweck regelt und ein Weisungsrecht enthält. Die Mitarbeiter der opwoco GmbH kennen den Datenverarbeitungszweck. Sie erhalten schriftliche Weisung zum Umgang mit personenbezogenen Daten. Unterauftragsverhältnisse werden schriftlich beauftragt.

7. Verfügbarkeitskontrolle

Das gesamte Gebäude der opwoco GmbH verfügt über eine Brandmeldeanlage und das Rechenzentrum ist in einem abgeschlossenen Bereich untergebracht, zu dem nur ausgewählte Mitarbeiterinnen und Mitarbeiter Zutritt haben. Das Rechenzentrum der opwoco GmbH verfügt über ein eigenes USV-System. Die opwoco GmbH fertigt von den Daten im Rechenzentrum täglich Back-ups an und die Daten werden auf getrennten Systemen gespiegelt, soweit dies Leistungsbestandteil ist. Die Datensicherungen werden zusätzlich bei einem Cloud-Hosting-Anbieter in Deutschland gesichert.

8. Trennungskontrolle

Die Daten des Auftraggebers werden virtuell von anderen Daten getrennt. Die Datensicherung erfolgt auf physikalisch oder virtuell getrennten Einheiten.

9. Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

Bei der opwoco GmbH wird schon bei der Entwicklung der Software Sorge dafür getragen, dass dem Grundsatz der Erforderlichkeit schon im Zusammenhang mit Benutzer-Interfaces Rechnung getragen wird. So sind z.B. Formularfelder, Bildschirmmasken flexibel gestaltbar. So können Pflichtfelder vorgesehen oder Felder deaktiviert werden. Die Software der opwoco GmbH unterstützt die Eingabekontrolle durch einen flexiblen und anpassbaren Audit-Trail, der eine unveränderliche Speicherung von Änderungen an Daten und Nutzerberechtigungen ermöglicht. Berechtigungen auf Daten oder Applikationen können flexibel und granular gesetzt werden.

10. Datenschutzbeauftragter

Bei der opwoco GmbH ist ein Datenschutzbeauftragter gem Art. 37 - 39 DSGVO eingesetzt, der erster Ansprechpartner für Kunden, Partnerunternehmen, Betroffene und Behörden in Datenschutzfragen ist. Der Datenschutzbeauftragte klärt über bestehende datenschutzrechtliche Pflichten auf und überwacht deren Einhaltung. Der Datenschutzbeauftragte berät und unterstützt bei der Durchführung der Datenschutz-Folgenabschätzung nach Art. 35 DSGVO und er führt das Verarbeitungsverzeichnis nach Art. 30 DSGVO. Die Kontaktdaten des Datenschutzbeauftragten werden auf Anfrage mitgeteilt.

11. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Bei der opwoco GmbH ist ein Datenschutzmanagement implementiert. Es gibt eine Leitlinie zu Datenschutz und Datensicherheit und Richtlinien, mit denen die Umsetzung der Ziele der Leitlinie gewährleistet wird. Es ist ein Datenschutzteam gemeinsam mit dem Datenschutzbeauftragten eingerichtet, das Maßnahmen im Bereich von Datenschutz und Datensicherheit plant, umsetzt, evaluiert und Anpassungen vornimmt. Die Richtlinien werden regelmäßig im Hinblick auf ihre Wirksamkeit evaluiert und angepasst. Es ist insbesondere sichergestellt, dass Datenschutzvorfälle von allen Mitarbeitern erkannt und unverzüglich dem Datenschutzbeauftragten gemeldet werden. Für den weiteren Umgang mit solchen Fällen existieren entsprechende Notfall- und Meldungskonzepte.