Technische und organisatorische Massnahmen

Aktualisiert: 6. Juni 2018

In den technischen und organisatorischen Massnahmen (TOM) ist ersichtlich, was durch Dualoo (nachfolgend auch Provider genannt) unternommen wird um die Daten zu schützen und unter welchen Voraussetzungen eine reibungslose Benutzung gewährleistet wird. Diese werden von Zeit zu Zeit durch den Provider upgedatet und bilden immer den aktuellen Stand ab.

Technische Voraussetzungen

Dualoo ist Software as a Service (SaaS) und wird über den Browser (https://login.dualoo.com) ausgeführt. Von der Applikation generierte Dokumente werden als Microsoft Office (docx) und als Adobe (PDF) auf dem Server gespeichert. Alle Daten werden im Zeichensatz UTF-8 abgespeichert, wodurch alle Sprachen abgebildet werden können. Um Dualoo verwenden zu können, wird ein Internetzugang mit einem unterstützten Webbrowser und eine E-Mail Adresse benötigt. Ansonsten ist keine Installation notwendig.

Unterstützte Desktop Browser

Chrome:	45+
Firefox	40+
Internet Explorer	10+
Safari	7+ (Mac OS only)

Datenverarbeitung nach DSGVO

Werden personenbezogene Daten automatisiert bearbeitet oder genutzt, ist die innerbetriebliche Organisation gemäss Datenschutzgesetz (DSGVO) so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei unterstützt Dualoo die Nutzer.

Durch den Provider wird keine Auftragsdatenverarbeitung vorgenommen. Der Provider kann nur für Support- und Unterstützungszwecke und nur mit Einwilligung einen zeitlich begrenzten Zugriff erhalten. Somit entfällt die Verpflichtung zur Erstellung eines Vertrages zur Auftragsdatenverarbeitung nach Art. 4 Ziff. 8 und Art. 28 DSGVO.
Obschon der Provider nicht unter die Auftragsdatenverarbeitung fällt, sind in diesem Dokument nachfolgend auch diese Punkte, welche für die Auftragsdatenverarbeitung verlangt werden aufgeführt.

Wird die Erstellung von einem Standardvertrag, basierend auf den transparent veröffentlichten Nutzungsbedingungen, Datenschutzerklärung und den technischen und organisatorischen Massnahmen, ausdrücklich gewünscht, bietet dies der Provider kostenfrei an.

Sind abweichende Änderungen oder ein eigenes Vertragswerk gefordert, belaufen sich die Kosten auf 300 Fr./ Stunde (nach Aufwand) welche zur Prüfung oder Erstellung eines Vertrages von Seiten des Providers nötig ist.

Zutrittskontrolle / Zugangskontrolle

Zutritt zu den Räumlichkeiten des Providers wird durch Mitarbeiterausweis und persönliche Schlüssel sichergestellt. Zugang zur Applikation, respektiv zu den Daten, funktioniert nur über ein persönliches Login mittels Benutzername (E-Mail Adresse) und Passwort. Das Passwort jedes einzelnen Nutzers wird verschlüsselt (Hashfunktion) in der Datenbank gespeichert.
Nutzerdaten werden ausschliesslich auf dem durch ISO-27001 geschützten Server und nicht auf lokalen Geräten der Mitarbeitenden gespeichert, welches die Datensicherheit gewährleistet. Der Provider hat grundsätzlich keinen Zugang zu den Nutzerdaten, ausser es liegt eine ausdrückliche Genehmigung vor.

Personendatenträgerkontrolle: Die Nutzer sind verantwortlich für einen angemessenen Schutz Ihrer Geräte und der Passwörter. Der Provider kann nicht für entstandene Schäden haftbar gemacht werden, welche durch Vernachlässigung des Schutzes der Geräte und Passwörter der Nutzer entstanden ist.

Zugriffskontrolle

Innerhalb der Applikation können einzelne Rechte vergeben werden (was kann welcher Nutzer). Für die interne Zugriffsberechtigung ist der Nutzer (zb. Administrator im Unternehmen) vollumfänglich verantwortlich. Er steuert, welche Zugriffsberechtigungen die anderen Nutzer (zb. Mitarbeitende) haben.
Der Provider wiederum ist für den Zugriff der Daten von aussen verantwortlich, indem die Daten akkurat geschützt und verschlüsselt werden.

Pseudonymisierung und Verschlüsselung

Alle Daten welche zwischen Nutzer und Server übertragen werden, sind End-to-End-verschlüsselt. Die Verbindung wird mittels TLS 4096bit (SSL) übertragen.

Eingabekontrolle / Protokollierung

Der Provider protokolliert alle Verbindungen zwischen Nutzer und Server.
Liegt ein Straftatbestand vor, ermöglicht der Provider Administratoren Einsicht in das Logfile der Firma.

Verfügbarkeitskontrolle und Belastbarkeit

Datenspeicherung und Hosting werden im Rechenzentrum von Metanet www.metanet.ch in Zürich (Schweiz) gespeichert. Das Rechenzentrum entspricht den höchsten Sicherheitsstandards. Der Betrieb ist nach ISO 9001 zertifiziert. Zusätzlich sind die Rechenzentren in Zürich nach ISO-Norm 27001 für Informationssicherheit zertifiziert sowie PCI DSS akkreditiert.

Backups: Der Provider führt mehrmals täglich Sicherungen der Kundendaten durch. Um Datenverlust auch im Extremfall zu verhindern (bspw. Zerstörung Rechenzentrum durch ein Erdbeben) werden die verschlüsselten Backups parallel in mehreren Rechenzentren im In- und Ausland gespeichert. Rotation: 30 Tage mit 12-Monats-Archiv.

Virenschutz: Der Nutzer trägt die alleinige Verantwortung und ist verpflichtet, die erhaltenen und übermittelten Daten auf Viren zu prüfen. Der Provider durchsucht alle übermittelten Dateien ebenfalls auf Viren. Der Provider kann dafür nicht haftbar gemacht werden, hilft jedoch mit, die Gefahr zu reduzieren.

Energieversorgung / Nachhaltigkeit: Die Server des Providers, die Webseite und die Büroräumlichkeiten werden mit nachhaltiger Energie betrieben.