Datenverarbeitungsvereinbarung
Anlage 1: **Datenschutzkonzept**

Stand: Version 2.5, 17.08.2023
Ansprechpartner: Matthias Menne, Datenschutzbeauftragter onOffice GmbH

Einleitung

Anlage 1 beschreibt die technisch-organisatorischen Maßnahmen nach Art. 32 DS-GVO, die die Sicherheit der folgenden durch den Vertrag abgedeckten Verarbeitungen garantieren soll:

- Bereitstellen der Online-CRM-Softwarelösung onOffice enterprise
- Hosten von Webseiten
- Datenimporte
- Datentransfers
- E-Mail-Hosting

Viele dieser Verarbeitungen finden auf denselben IT-Systemen und unter denselben Sicherheitsvorkehrungen statt. Deshalb werden am Beginn jedes Kapitel diese gemeinsamen Sicherheitsvorkehrungen beschrieben und danach auf die einzelnen Verarbeitungen eingegangen.

Verschlüsselung

Der Netzwerk-Verkehr von und zu onOffice enterprise ist https-gesichert. Es werden die TLS-Versionen 1.0, 1.1 und 1.2 unterstützt. Das Zertifikat wurde von „GMO GlobalSign Inc“, Portsmouth NH, USA ausgegeben.

Webseiten können durch die CA „Let’s Encrypt“, San Francisco CA, USA verifizierte Zertifikate gesichert werden.

Im Rahmen von Datenimporten eingesendete Datenträger werden vor der Rücksendung an den Kunden verschlüsselt.

Beim E-Mail-Versand wird TLS mit Perfect Forward Security verwendet, soweit der Empfänger-Server dies unterstützt.

Vertraulichkeit

Die Vertraulichkeit der personenbezogenen Daten wird dadurch sichergestellt, dass nur berechtigte Personen darauf physischen oder logischen Zugriff darauf haben.

Zutrittskontrolle

Soweit nicht anders angegeben, finden alle Verarbeitungen im Rechenzentrum der Telehouse Deutschland GmbH statt (siehe Anlage 2).

Hier ist eine Zutrittskontrolle durch ein berührungsloses Ausweissystem, 24/7-Bewachung durch einen Werkschutz und eine Videoüberwachung gegeben. Die Zutrittsberechtigung zu den einzelnen Serverräumen ist für jeden Raum eigens programmiert.

Back-ups werden in von Telehouse Deutschland GmbH angemieteten Räumen im Düsseldorfer Rechenzentrum der Equinix (Germany) GmbH gespeichert.

Die Mitarbeitende beider Rechenzentren haben keinen Zugriff auf die gespeicherten Daten.

In den Geschäftsräumen der onOffice GmbH in Aachen werden personenbezogene Daten des Auftraggebers nur kurzfristig und entweder zu internen Softwaretests (soweit unbedingt erforderlich) oder für Datenimporte gespeichert. Die Schlüsselvergabe an Mitarbeitende ist geregelt und dokumentiert. Außerhalb der Geschäftszeiten sind die Geschäftsräume durch eine Alarmanlage gesichert, im Alarmfall wird automatisch ein Wachschutz benachrichtigt.

Im Rahmen von Datenimporten eingesendete Datenträger werden gesichert in den Geschäftsräumen aufbewahrt. Der Verbleib der Datenträger wird schriftlich dokumentiert. Die Datenimporte werden auf einem Server in den Geschäftsräumen der onOffice GmbH in Aachen durchgeführt. Der Server steht in einem eigenen Serverraum, der durch eine Alarmanlage, Zugangsprotokollierung und Videoüberwachung gesichert ist.

Zugangskontrolle

Der Zugang zu onOffice enterprise ist nur möglich mit der Eingabe des richtigen Kundennamens, dem Namen eines aktiven, nicht gesperrten Benutzers und des gültigen Passwortes. Der Benutzername und das Passwort sind bei der Eingabe nicht im Klartext zu sehen. Die Häufigkeit mit der ein Passwort geändert werden muss, kann von einem Benutzer mit Administratorrechten über die Software eingestellt werden. Die Komplexität eines Passwortes wird bei Neueingabe automatisch überprüft; unterschreitet diese einen bestimmten Wert, wird das Passwort nicht angenommen.

Der Zugang zu Produktivsystemen ist auf den unbedingt erforderlichen Personenkreis beschränkt und durch Public-Private-Key-Authentifizierung gesichert. Beim Ausscheiden eines onOffice Mitarbeitendens werden die Zugänge gelöscht.

Die auf den Servern installierte Standardsoftware wird regelmäßig darauf überprüft, ob es sicherheitskritische Updates gibt. Diese werden dann so schnell, wie ohne die Verfügbarkeit zu gefährden möglich, eingespielt.

Personenbezogene Daten des Auftraggebers werden von Mitarbeitern der onOffice GmbH nur soweit notwendig außerhalb der Geschäftsräume verarbeitet. Die IT-Sicherheitsrichtlinie wird in diesem Fall genauso eingehalten wie innerhalb der Geschäftsräume.

Der Netzwerk-Verkehr wird durch eine hardwarenahe Firewall überwacht.

Zugriffskontrolle

In onOffice enterprise lässt sich der Zugriff auf Datensätze benutzerbezogen einschränken. Dazu müssen die Datensätze bestimmten Benutzern oder Gruppen zugeordnet und die Rechte der Benutzer geeignet eingeschränkt werden. Zusätzlich lässt sich noch ein Modul buchen, mit dem sich für jeden Benutzer die Lese- und Schreibrechte für einzelne Adress- / Objekt- / Historien-Datensätze setzen lassen. Benutzer können eine Liste der zuletzt von ihnen geöffneten Datensätze erstellen.

E-Mail-Postfächer in onOffice enterprise lassen sich einem oder mehreren Benutzern zuordnen. Das Postfach ist dann nicht mehr für andere Benutzer einsehbar.

Integrität

In onOffice enterprise ausgeführte Änderungen an Adress- und Objektdaten werden protokolliert. Diese Änderungen können von Benutzer mit Administratorrechten nachvollzogen werden.

onOffice enterprise ist mandantenfähig. Die Daten jedes Kunden werden in einer eigenen Datenbank gespeichert. Es ist für einen Benutzer nicht möglich, Daten anderer Kundenversionen einzusehen, ohne sich unter Angabe des Mandantennamens, des Benutzers und des Passworts in eine andere Version einzuloggen.

Änderungen an der Codebasis von onOffice enterprise werden sorgfältig getestet und dann erst für einige Wochen einem begrenzten Kundenkreis zur Verfügung gestellt. Erst danach werden sie für alle Kunden ausgerollt. Fehlerbehebungen werden für alle Kunden zweimal die Woche eingespielt, in dringenden Fällen sofort.

E-Mail-Anhänge werden auf Viren überprüft, ein Virenschutz für die anderen Verarbeitungen wird geprüft oder schon ausgerollt.

Verfügbarkeit

Kunden-Datenbanken werden jede Nacht durch ein Full-Back-up gesichert. Diese Back-ups werden in von Telehouse Deutschland GmbH angemieteten Räumen im Düsseldorfer Rechenzentrum der Equinix (Germany) GmbH gespeichert (siehe Anlage 2). Kunden-Dateien werden einmal im Monat durch Full-, und jede Nacht durch ein inkrementelles Back-up gesichert.

Mit Ausnahme von „Datenimporte“ und „Datentransfers“ werden alle Verarbeitungen im Telehouse-Rechenzentrum durchgeführt. Die Verfügbarkeit der Daten ist durch eine N+1-redundante Notstromversorgung, Brandschutz mit optischen / thermischen Feuermeldern und Inergen-Löschanlagen sowie redundante Netzwerkanbindungen an mehrere Carrier gesichert.

Für alle Verarbeitungen steht genug Rechenkapazität zur Verfügung, um den Ausfall mehrerer Server auszugleichen. Die Kundendaten werden in einem RAID5-System gespeichert.

Zum Schutz vor DDoS-Attacken nimmt onOffice am Prolexic Network von Akamai teil. Alle Anfragen an Systeme der onOffice GmbH werden über Server von Akamai geroutet. Dabei werden Anfragen, die Teil einer DDoS-Attacke sind, ausgefiltert.

Rechtmäßigkeit der Verarbeitung

Alle Mitarbeitenden der onOffice GmbH sind auf das Datengeheimnis verpflichtet und werden zum Thema Datenschutz und IT-Sicherheit geschult.

Mit allen Unterauftragnehmern wurden Auftragsverarbeitungs-Vereinbarungen geschlossen. Die Unterauftragnehmer werden vor Vertragsabschluss auf Eignung überprüft. Damit wird garantiert, dass auch die Mitarbeitenden der Unterauftragnehmer zur Geheimhaltung verpflichtet wurden.

Bei der Planung von Funktionalitäten und Prozessen wird das Prinzip der Datenminimierung immer miteinbezogen („Privacy by Design").

Datenschutz-Management

Das Datenschutzkonzept wird durch Arbeitsanweisungen, Vereinbarungen und technisch-organisatorische Maßnahmen umgesetzt. Die Eignung des Datenschutzkonzeptes wird mindestens jährlich überprüft. Bei Bedarf wird das Datenschutzkonzept oder die Umsetzung des Datenschutzkonzeptes angepasst.

Incident-Response-Management

Die für die Verarbeitungen verwendeten IT-Systeme werden permanent überwacht. Bei Vorfällen wird der Zugriff auf personenbezogene Daten schnellstmöglich wiederhergestellt. Nach Vorfällen wird im Rahmen einer Nachbereitung überprüft, ob das IT-Sicherheitskonzept oder das IT-Notfall-Konzept überarbeitet werden muss und ob die technisch-organisatorischen Maßnahmen und die IT-Infrastruktur ausreichen, um einen Vorfall der gleichen Art in der Zukunft zu verhindern.

Datenverarbeitung in Drittstaaten

onOffice verwendet Akamais Prolexic Network. Um einen optimalen Schutz vor DDoS-Attacken sicherzustellen, wird der Traffic zu den Systemen der onOffice GmbH über Server in der ganzen Welt geroutet. Die Überwachung des Traffics wird in den USA durchgeführt. Deshalb werden unter Umständen folgende personenbezogene Daten außerhalb der EU verarbeitet:

1. die IP-Adresse des Clients
2. die Domain, die abgefragt wurde
3. bei nicht https-gesichertem Traffic: die URL

onOffice hat mit Akamai die EU-Standardvertragsklauseln in der Fassung vom Juni 2021 abgeschlossen, unter Verwendung des Moduls 3 (Verarbeiter und Verarbeiter).

Eine Prüfung der Rechtslage in den USA und eine Risikoanalyse wurden durchgeführt. Weitere Sicherheitsmaßnahmen müssen vom Verantwortlichen nicht ergriffen werden.