Technische und organisatorische Maßnahmen

Datenschutz OMERGY GmbH

0. Organisatorisches

(Maßnahmen, die generelle Auswirkungen auf das Datenschutzniveau haben)

- Die Mitarbeiter werden mit Eintritt in das Beschäftigungsverhältnis über den Datenschutz aufgeklärt sowie auf das Datengeheimnis verpflichtet.
- Die Mitarbeiter werden durch regelmäßige Informationsrundschreiben / Intranet über aktuelle datenschutzrechtliche Entwicklungen sowie besondere zu berücksichtigende Maßnahmen des Datenschutzes, bezogen auf das Unternehmen, informiert.
- Schulungen der Mitarbeiter werden nach Erforderlichkeit im Hinblick auf den jeweiligen Kenntnisstand der Mitarbeiter in regelmäßigen Abständen durchgeführt.

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

Zutrittskontrolle *(Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren)*

- Die Unternehmensräumlichkeiten liegen in der 7. Etage eines Bürokomplexes. Zutritt zu den Unternehmensräumlichkeiten erfolgt über den Hauseingang des Gebäudes sowie den separaten Etagenzugang.
- Der Eintrittsbereich wird von Mitarbeitern kontrolliert.
- In den Unternehmensräumlichkeiten befinden sich keine Server, sondern nur lokale Arbeitsplatzrechner.
- Die Schlüsselvergabe an Mitarbeiter erfolgt mittels Schlüsselquittung (Protokollierung in Personalakte).
- Das operative Arbeiten erfolgt auf Servern, welche bei der Fa. Hetzner gehostet sind. Die Zutrittskontrolle zum Rechenzentrum der Fa. Hetzner wird wie folgt geregelt (siehe auch https://www.hetzner.de/pdf/ADV_TOM.pdf):
  - Elektronisches Zutrittskontrollsystem mit Protokollierung
  - Hochsicherheitszaun um den gesamten Datacenterpark
  - Dokumentierte Schlüsselvergabe an Mitarbeiter und Colocation-Kunden für Colocation Racks (jeder Auftraggeber ausschließlich für seinen Colocation Rack)
  - Richtlinien zur Begleitung und Kennzeichnung von Gästen im Gebäude
  - 24/7 personelle Besetzung der Rechenzentren
  - Videoüberwachung an den Ein- und Ausgängen, Sicherheitsschleusen und Serverräumen

Zugangskontrolle *(Maßnahmen, die geeignet sind, um zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können)*

- Das Passwort zur Administrationsoberfläche der Server bei Fa. Hetzner wird von OMERGY selbst vergeben. Server-Passwörter werden nach erstmaliger Inbetriebnahme von OMERGY selbst geändert und sind der Fa. Hetzner nicht bekannt. Server-Passwörter sind nur ausgewählten Mitarbeitern zugänglich.
- Jeder Mitarbeiter verfügt über ein individuelles Login mit nur ihm bekannten individuellen Passwort (siehe auch „Zugriffskontrolle“).
- Bei Pausen aktiviert sich nach einer bestimmten Zeit eine Bildschirmsperre.
- An- und Abmeldungen werden protokolliert.
- Es wird eine Hardware-Firewall (Marke fortigate) zur Filterung allen ein- und ausgehenden Datenverkehrs eingesetzt.
- Verwendete Browser- und Antivirensoftware ist stets auf die neuste verfügbare Version aktualisiert.
- Es wird innerhalb des Betriebs ein verschlüsseltes W-LAN eingesetzt. Ein Empfang außerhalb des Bürogebäudes ist nicht möglich.

Zugriffskontrolle *(Maßnahmen, die geeignet sind, um zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können)*

- Arbeiten mit personenbezogenen Daten erfolgen ausschließlich über Browser auf der jeweiligen Plattform (G-Suite / Backoffice / CRM). Eine lokale Speicherung und Verarbeitung von Daten erfolgt nicht.
- Für administrative Tätigkeiten (insbesondere Verwaltung von E-Mails, Dokumenten sowie die Nutzung von Kalenderfunktionen) wird auf die G-Suite der Fa. Google zurückgegriffen.
- Die operative Arbeit erfolgt über eine eigene Software (Backoffice / CRM), welche bei der Fa. Hetzner gehostet ist.
- Der Anmeldeprozess eines Mitarbeiters vor Ort erfordert eine Anmeldung an seinem Arbeitsplatzrechner mittels individuellem Login und Passwort.
- Der Mitarbeiter muss sich ferner bei G-Suite anmelden. Nutzer werden hier durch die Administration entsprechend angelegt und freigeschaltet. Die Anmeldung des Mitarbeiters selbst erfolgt wiederum durch Login und Passwort.
- Die Anmeldung im internen operativen System erfolgt mittels individuellem Login und Passwort (Basic-Auth) sowie weiterhin über ein Formularfeld mit weiterem Login und Passwort.
- Beim Ausscheiden von Mitarbeitern werden deren Zugänge deaktiviert.
- Die Mitarbeiter haben nur Zugriff auf die für ihre Tätigkeit relevanten Daten. Es erfolgt eine differenzierte Berechtigungsvergabe. Bei Vertriebsmitarbeitern ist der Zugriff auf reine vertriebsrelevante Daten beschränkt.
- Es erfolgt eine teilweise Einschränkung des Logins via IP-Check.
- Mobile Datenträger werden nicht eingesetzt.

Trennungskontrolle *(Maßnahmen, die geeignet sind, um zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können)*

- Es erfolgt die logische Trennung der Kundendaten innerhalb des Datenbanksystems. Die interne Mandantenfähigkeit ist gewährleistet.
- Entwicklungs- und Produktivsystemen werden getrennt voneinander eingesetzt. Pseudonymisierung (Die Verarbeitung personenbezogener Daten soll, sofern erforderlich und umsetzbar, in einer Weise erfolgen, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.)

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

Weitergabekontrolle *(Maßnahmen, die geeignet sind, um zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist)*

- Weitergaben physischer Datenträger erfolgen nicht. Mobile Datenträger werden nicht eingesetzt.
- Die Datenablage erfolgt auf dem Server und nicht lokal. Die Kommunikation zwischen Arbeitsplatzrechner und Server erfolgt über sichere verschlüsselte Datenübertragung.
- Alle Mitarbeiter sind auf die Einhaltung des Datengeheimnisses verpflichtet.
- Nach Auftragsbeendigung erfolgt die datenschutzgerechte Löschung der nicht mehr erforderlichen Daten.

Eingabekontrolle *(Maßnahmen, die geeignet sind, um zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind)*

- An- und Abmeldungen werden systemintern protokolliert.
- Anmeldehistorie kann in G-Suite und Backoffice eingesehen werden.
- Veränderungen können z.T. in der Versionshistorie eingesehen und anhand derer nachgeprüft werden.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

Verfügbarkeitskontrolle *(Maßnahmen, die geeignet sind, um zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind)*

- Im gesamten Unternehmensgebäude sind Brandmelder installiert. Es sind ausreichend und gewartete Feuerlöscher vorhanden.
- In den Büroräumlichkeiten herrscht Rauchverbot.
- Der Betrieb der Server bei der Fa. Hetzner erfolgt unter Einsatz unterbrechungsfreier Stromversorgung.

- Es besteht ein dauerhaft aktiver DDoS-Schutz.
- Virenschutzsoftware sowie eine Firewall werden eingesetzt. Regelmäßige Aktualisierungen gewährleisten die stete Aktualität.
- Es erfolgt die synchrone fortlaufende Spiegelung aller Daten auf Backup Server bei täglichen Backups aller Daten.
- Backups werden in einem gesichertem BackupSpace bei der Fa. Hetzner gespeichert und zuvor zusätzlich verschlüsselt, um Zugriff Dritter auszuschließen.

Rasche Wiederherstellbarkeit

- Wiedereinspielungstests der Backups in regelmäßigen Abständen.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. D DSGVO; Art. 25 Abs. 1 DSGVO)

Datenschutz-Management

- Es wird ein internes Datenschutzkonzept vorgehalten mit Dokumentation zum Umgang mit personenbezogenen Daten. Die Überprüfung und Kontrolle erfolgt durch den Datenschutzbeauftragten (extern).

Incident-Response-Management

- Im Rahmen des Notfallkonzepts als Bestandteil des Datenschutzkonzepts sind klare Prozesse zum Umgang mit IT-Sicherheitsvorfällen und Datenschutzvorfällen beschrieben.

Datenschutzfreundliche Voreinstellungen

- Abhängig vom jeweiligen Kundenauftrag. Im Rahmen der Landingpageerstellung wird dem Grundsatz Privacy-by-default bestmöglich gefolgt (z. B. Beschränkung der Pflichtangaben im Kontaktformular nur auf die für die Beantwortung der Anfragen erforderlichen Angaben).

5. Auftragskontrolle

(Maßnahmen, die geeignet sind, um zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können)

- Im Rahmen der Nutzung der G-Suite Software ist mit dem Auftragsdienstleister (Google LLC) eine Auftragsdatenverarbeitungsvereinbarung / EU-Standardvertragsklausel abgeschlossen.
- Beim verwendeten Hostingdienst (Hetzner) erfolgt die Anmietung der Netzwerkinfrastruktur, Bandbreite und Serverhardware. Die Installation und Wartung der Server erfolgen durch OMERGY selbst.
- Zugangsdaten (Passwörter) der Server sind allein OMERGY bekannt.
- Serverfestplatten sind mit Vollverschlüsselung versehen zum Zwecke des zusätzlichen Schutzes gegen Diebstahl des Servers oder Auslesen der Festplatten.