Technische und organisatorische Maßnahmen gem. Art. 32 DSGVO

DUSOFFICE GmbH & Co. KG - TARIS

Sicherheitskonzept

Technische und organisatorische Maßnahmen gem. Art. 32 DSGVO

Grundsätzliche Maßnahmen

Grundsätzliche Maßnahmen, die der Wahrung der Betroffenenrechte, unverzüglichen Reaktion in Notfällen, den Vorgaben der Technikgestaltung und dem Datenschutz auf Mitarbeiterebene dienen:

- Es besteht ein Konzept, welches die Wahrung der Rechte der Betroffenen (Auskunft, Berichtigung, Löschung oder Einschränkung der Verarbeitung, Datentransfer, Widerrufe & Widersprüche) innerhalb der gesetzlichen Fristen gewährleistet. Es umfasst Formulare, Anleitungen und eingerichtete Umsetzungsverfahren sowie die Benennung der für die Umsetzung zuständigen Personen.
  DUSOFFICE bearbeitet Betroffenenanfragen zentral über das DSMS. Anfragen werden identitätsgeprüft, fristüberwacht und dokumentiert. Soweit DUSOFFICE als Auftragsverarbeiter tätig ist, wird der verantwortliche Kunde unverzüglich eingebunden und die Umsetzung erfolgt nach dokumentierter Weisung. Die gesetzliche Monatsfrist sowie erforderliche Informationen, Berichtigungen, Löschungen, Einschränkungen, Widersprüche und Datenübertragungen werden im Verfahren berücksichtigt.

- Es besteht ein betriebsinternes Datenschutz-Management, dessen Einhaltung ständig überwacht wird sowie anlassbezogen und mindestens halbjährlich evaluiert wird.
  Für das Datenschutzmanagement wird die Software DPMS eingesetzt. Das Datenschutzmanagementsystem wird fortlaufend betrieben, mindestens halbjährlich sowie anlassbezogen überprüft und dokumentiert. Zuständigkeiten, Datenschutzvorfälle, Betroffenenrechte, Dienstleisterkontrollen und erforderliche Maßnahmen werden nachvollziehbar im Managementsystem geführt.

- Die an Mitarbeiter ausgegebene Schlüssel, Zugangskarten oder Codes sowie im Hinblick auf die Verarbeitung personenbezogener Daten erteilte Berechtigungen, werden nach deren Ausscheiden aus dem Unternehmen, bzw. Wechsel der Zuständigkeiten eingezogen, bzw. entzogen.
  Konten, Rollen, Schlüssel, Geräte und sonstige Berechtigungen werden bei Ausscheiden, Aufgabenwechsel oder Vertragsende unverzüglich gesperrt, entzogen oder angepasst. Benutzerkonten können durch Administratoren derselben oder einer höheren Ebene innerhalb des jeweiligen Plattform-, Partner- oder Kundenbereichs verwaltet werden. Alle administrativen Kontohandlungen werden protokolliert.

- Mitarbeiter werden im Hinblick auf den Datenschutz auf Verschwiegenheit verpflichtet, belehrt und instruiert, als auch auf mögliche Haftungsfolgen hingewiesen. Sofern Mitarbeiter außerhalb betriebsinterner Räumlichkeiten tätig werden oder Privatgeräte für betriebliche Tätigkeiten einsetzen, existieren spezielle Regelungen zum Schutz der Daten in diesen Konstellationen und der Sicherung der Rechte von Auftraggebern einer Auftragsverarbeitung.
  Alle berechtigten Personen werden vor dem ersten Zugriff auf Vertraulichkeit, Weisungs- und Zweckbindung verpflichtet und rollenbezogen zu Datenschutz, Informationssicherheit, Phishing, sicherer Authentisierung und Vorfallmeldung unterwiesen. Schulungen erfolgen bei Eintritt, Rollen- oder Prozessänderungen sowie mindestens jährlich. Homeoffice ist nur mit geschützten, verwalteten und verschlüsselten Endgeräten zulässig; lokale Kopien und Ausdrucke von Gesprächsdaten sind untersagt.

- Die eingesetzte Software wird stets auf dem aktuell verfügbaren Stand gehalten, ebenso wie Virenscanner und Firewalls.
  Betriebssysteme, Anwendungen, Virenschutz und Firewalls werden regelmäßig überprüft und auf einem aktuellen Sicherheitsstand gehalten. Der Virenschutz ist umgesetzt. Sicherheitsrelevante Ereignisse und

der Schutzstatus werden zentral über Wazuh überwacht; Auffälligkeiten werden nach dem festgelegten Incident-Prozess bearbeitet.

- Der Schutz von personenbezogenen Daten wird unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen bereits bei der Entwicklung, bzw. Auswahl von Hardware, Software sowie Verfahren, entsprechend dem Prinzip des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen berücksichtigt (Art. 25 DSGVO).
  Datenschutz und Informationssicherheit werden bei Planung, Entwicklung und Änderung von TARIS berücksichtigt. Entwicklungs-, Test- und Produktivumgebung verwenden getrennte Hosting-Umgebungen und Datenbanken. Datenminimierung, datenschutzfreundliche Voreinstellungen, Berechtigungen, Löschregeln, Protokollierung, sichere Schnittstellen sowie Prüf- und Freigabeschritte sind verbindliche Entwicklungsanforderungen.

- Es besteht ein Konzept, das eine unverzügliche und den gesetzlichen Anforderungen entsprechende Reaktion auf Verletzungen des Schutzes personenbezogener Daten (Prüfung, Dokumentation, Meldung) gewährleistet. Es umfasst Formulare, Anleitungen und eingerichtete Umsetzungsverfahren sowie die Benennung der für die Umsetzung zuständigen Personen.
  Auffällige protokollierte Zugriffsmuster erzeugen automatisch eine E-Mail mit Protokollen an datenschutz@hallo-it.de. Interne Meldungen werden im DSMS erfasst; weitere Meldewege sind E-Mail und hallo-it.hinweis.digital. Datenschutzbeauftragter und IT-Administrator bearbeiten Vorfälle gemeinsam. Das DSMS unterstützt Risikobewertung, Dokumentation, 72-Stunden-Frist, Kundeninformation sowie erforderliche Meldungen an Aufsichtsbehörden und betroffene Personen. Die Verantwortung verbleibt beim jeweiligen Verantwortlichen.

Zutrittskontrolle

- Sicherheitsschlösser
  Die TARIS-Server befinden sich in ISO/IEC-27001:2022-zertifizierten Hetzner-Rechenzentren. Der physische Zutritt zu Server- und Technikbereichen ist durch gesicherte Rechenzentrumsbereiche und technische Schließsysteme auf autorisierte Personen beschränkt. In den Geschäftsräumen von DUSOFFICE und Hallo-IT werden keine lokalen oder papiergebundenen Kopien der TARIS-Gesprächsdaten vorgehalten.

- Chipkarten-/Transponder-Schließsystem
  Hetzner begrenzt den Zutritt zu den Rechenzentrumsbereichen über technisch kontrollierte Schließ- und Transpondersysteme mit verwalteten Berechtigungen und protokollierten Zutritten. Gültigkeit und Geltungsbereich werden über Vertrag, TOM-Anlage und aktuelle Zertifizierungs-/Prüfnachweise kontrolliert.

- Zutrittsregelungen für betriebsfremde Personen
  Betriebsfremde Personen erhalten Zutritt zu den genutzten Rechenzentrumsbereichen ausschließlich nach den dokumentierten Zutritts- und Besucherregelungen von Hetzner. Berechtigungen, Begleitung und Zutrittsprotokollierung richten sich nach Schutzbereich und Anlass. Arbeitsplätze und Administrationsgeräte bei DUSOFFICE und Hallo-IT sind trotz fehlender lokaler Datenkopien vor unbefugter Nutzung und Einsicht zu schützen.

Zugangskontrolle / Zugriffskontrolle

- Firewall (Software)

TARIS-Produktivsystem und Kundenportal sind voneinander getrennt und durch Software-Firewalls geschützt. CrowdSec erkennt und blockiert auffällige Zugriffsmuster. Sämtliche regulären Zugriffe werden über einen vorgeschalteten Traffic-Proxy geführt; direkte Backendzugriffe werden durch restriktive Netzwerkregeln begrenzt. Firewallregeln folgen dem Grundsatz der standardmäßigen Verweigerung und werden dokumentiert und überwacht.

- Authentifikation mit Benutzer und Passwort und bei erhöhtem Schutzbedarf durch eine zusätzliche Multifaktor-Authentisierung
  Die Anmeldung erfolgt mit Benutzername und Passwort oder Passkey sowie einem zusätzlichen Faktor über Magic-Link, SMS-Code oder TOTP. Plattform- und Partner-Admins sind zusätzlich auf freigegebene IP-Adressen beschränkt. Passwort-Reset erfolgt per E-Mail mit 2FA; 2FA-Reset nur über Support. Fehlversuche führen gestuft zu IP-Sperren. Benutzersitzungen enden nach 60 Minuten; ein geschütztes 2FA-Merkcookie kann 30 Tage gelten.

- Mindestpasswortlängen und Passwortmanager
  Für interne Zugänge wird Bitwarden zur sicheren Speicherung und gezielten Weitergabe von Zugangsdaten verwendet. Es gelten Mindestpasswörter von 12 Zeichen einschließlich Sonderzeichen, Buchstaben und Zahlen. Die Ablösung des Cloud-Bitwarden durch eine selbst gehostete Bitwarden-Instanz ist geplant.

- Ordnungsgemäße Vernichtung von Datenträgern
  Datenträger und Speichermedien werden vor Rückgabe, Wiederverwendung oder Entsorgung nach anerkannten Verfahren sicher gelöscht oder physisch vernichtet. Die Regelung umfasst insbesondere Server-/Storage-Komponenten, Sicherungsmedien und verwaltete Endgeräte. Bei externen Dienstleistern werden Lösch- und Vernichtungsnachweise vertraglich eingefordert. Lokale oder papiergebundene Kopien von TARIS-Gesprächsdaten sind untersagt.

- Protokollierung von Zugriffen auf Daten
  Sämtliche Benutzer- und Administratoraktionen in TARIS werden protokolliert. Die Protokolle werden sechs Monate aufbewahrt und anschließend automatisch gelöscht. Erfasst werden insbesondere Anmeldung, Konten-/Rollenverwaltung, Zugriffe auf Gesprächsdaten, Exporte, Änderungen, Löschungen, Speicherfrist- und Konfigurationsänderungen. Protokollzugriffe sind beschränkt; Geheimnisse und vollständige Gesprächsinhalte werden nicht in Aktionslogs übernommen.

- Verschlüsselung von mobilen Datenträgern und Geräten
  Administrationsgeräte sind verwaltet und verschlüsselt. Virtuelle Festplatten der VMs können mit nativer ZFS-Verschlüsselung verschlüsselt werden; diese Option ist derzeit bei bestimmten Mindestabnahmemengen verfügbar. Private Geräte, unverschlüsselte Datenträger und lokale Kopien von Gesprächsdaten sind für die Verarbeitung ausgeschlossen.

- Einsatz von Intrusion-Detection-Systemen
  CrowdSec wird als Angriffserkennungs- und Reaktionskomponente vor Produktivsystem und Kundenportal eingesetzt. Auffällige Zugriffsmuster werden anhand aktueller Szenarien erkannt, protokolliert und gesperrt. Relevante Muster erzeugen automatisch eine Meldung mit Protokollen an datenschutz@hallo-it.de. Regeln, Ausnahmen, Fehlalarme und die Funktionsfähigkeit der Erkennung werden überwacht.

- Berechtigungs-/ Authentifizierungskonzepte mit auf Nötigste beschränkten Zugriffsregulierungen
  TARIS verwendet ein hierarchisches Rollen- und Berechtigungskonzept für Plattform-, Partner-, Kunden-Admins und Kunden-Mitarbeiter. Zugriffe sind auf den jeweiligen Plattform-, Partner- und Kundenbereich

sowie die erforderlichen Funktionen begrenzt. Plattform- und Partner-Admins können sich zusätzlich nur von freigegebenen IP-Adressen anmelden. Konten werden durch Admins derselben oder einer höheren Ebene verwaltet; administrative Änderungen werden protokolliert.

- Stets aktuelle Softwareversionen
  Betriebssysteme, Container, Bibliotheken, Anwendungen, Traffic-Proxy, Firewall und CrowdSec unterliegen einem geregelten Patch- und Schwachstellenmanagement. Kritische aktiv ausgenutzte oder internetexponierte Schwachstellen werden unverzüglich, grundsätzlich binnen 24 Stunden, behoben oder kompensiert. Hohe, mittlere und niedrige Risiken werden innerhalb abgestufter Fristen bearbeitet; Abweichungen werden risikobasiert dokumentiert.

Weitergabekontrolle

- Festlegung und Dokumentation der Empfänger
  Für TARIS ist folgende Empfänger- und Unterauftragnehmerkette festgelegt: Hallo-IT GmbH betreibt die redundante VM-Infrastruktur; die zugrunde liegenden Host-Server werden bei Hetzner angemietet. Google Cloud Speech-to-Text verarbeitet den eingehenden Audiostream live innerhalb der EU und liefert die Echtzeit-Transkription zurück. Erkannter Text, System-Prompt und laufendes Gesprächstranskript werden durch die OpenAI API auf Microsoft-Azure-Servern innerhalb der EU Data Zone verarbeitet. ElevenLabs erzeugt aus der Textantwort live die TARIS-Sprachausgabe. Kundenbezogene E-Mail-Empfänger und angebundene Telefonie-, Kalender-, CRM- oder Weiterleitungssysteme werden je Auftrag festgelegt. Nach den vereinbarten Bedingungen erfolgt kein KI-Training. Für die OpenAI-/Azure-Verarbeitung und ElevenLabs besteht trotz vereinbarter EU Data Residency und Zero Data Retention eine mögliche Speicherung zur Betrugs- oder Missbrauchsprävention von bis zu 30 Tagen.

- Verschlüsselung von Datenträgern und Verbindungen
  Virtuelle Festplatten der VMs werden auf den physischen Datenträgern verschlüsselt gespeichert. HTTP- und WebSocket-Verbindungen sind über HTTPS abgesichert. Die Verbindung zum VoIP-Carrier erfolgt verschlüsselt. Partner-API-, Wartungs- und Administrationsverbindungen sind zusätzlich auf vorab freigegebene IP-Adressen beschränkt.

- Dedizierte Weitergabeberechtigungen
  Weitergaben erfolgen ausschließlich an dokumentierte, für den jeweiligen Zweck autorisierte Empfänger. Plattform-, Partner-, Kunden-Admins und Kunden-Mitarbeiter erhalten nur die ihrer Rolle und Mandantenzuordnung entsprechenden Zugriffs- und Weitergaberechte. Kundenbezogene E-Mail-Empfänger sowie Telefonie-, Kalender-, CRM- und Weiterleitungssysteme werden je Auftrag festgelegt. Exporte, Empfänger- und Berechtigungsänderungen werden protokolliert.

Eingabekontrolle

- Protokollierung von Dateneingaben-, Änderungen und Löschungen
  Sämtliche Dateneingaben, Änderungen und Löschungen durch Benutzer und Administratoren werden mit individuellem Konto, Rolle, Zeitpunkt, betroffenem Mandanten, Aktion, Objekt und Ergebnis protokolliert. Die Aktionsprotokolle werden sechs Monate aufbewahrt und anschließend automatisch gelöscht. Protokolle sind zugriffsbeschränkt und gegen unbefugte Veränderung zu schützen; Geheimnisse und unnötige Gesprächsinhalte werden nicht protokolliert.

- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
  Rechte zur Eingabe, Änderung, Löschung, zum Export und zur Verwaltung von Speicherfristen werden rollenbasiert vergeben. Plattform-Admins verwalten Plattform- und untergeordnete Bereiche; Partner-Admins nur zugeordnete Whitelabel-Kunden; Kunden-Admins und Kunden-Mitarbeiter nur den eigenen Kundenbereich. Rechteprüfungen erfolgen serverseitig. Konten- und Rollenänderungen werden vollständig protokolliert.

Auftragskontrolle

- Auswahl von Auftragnehmern unter Sorgfaltsgesichtspunkten
  Vor dem Einsatz von Auftragsverarbeitern und Unterauftragnehmern werden Zweck, Datenarten, Verarbeitungsorte, technische und organisatorische Maßnahmen, Unterauftragnehmerkette, Lösch- und Rückgaberegeln, Zusagen zu Datennutzung und KI-Training, Verfügbarkeit sowie Meldewege geprüft und dokumentiert. Dies gilt insbesondere für Hallo-IT GmbH, Hetzner, Google Cloud Speech-to-Text, OpenAI auf Microsoft Azure und ElevenLabs sowie für auftragsabhängig angebundene Telefonie-, E-Mail-, Kalender- und CRM-Dienste.

- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
  Nach Ende des Auftrags werden personenbezogene Daten nach Wahl und Weisung des Verantwortlichen zurückgegeben oder sicher gelöscht, soweit keine gesetzliche Aufbewahrungspflicht entgegensteht. Die Verpflichtung umfasst produktive Daten, Sicherungskopien und Unterauftragnehmer im Rahmen der technisch vorgesehenen Löschzyklen. Für TARIS werden Kundeninhalte nach Ablauf der kundenseitig festgelegten Frist, spätestens nach sechs Monaten, automatisiert gelöscht; erforderliche Rückgabe- oder Exportmöglichkeiten und Löschbestätigungen werden dokumentiert.

- Kontrolle der Einhaltung bei Auftragnehmern
  Die eingesetzten Auftragsverarbeiter werden mindestens jährlich sowie anlassbezogen bei wesentlichen Änderungen oder Sicherheitsvorfällen überprüft. Gegenstand der Prüfung sind insbesondere AV-Vertrag, TOM, Nachweise und Prüfberichte, Verarbeitungsregionen, Unterauftragnehmer, Löschfristen, Sicherheitsvorfälle und vereinbarte Datennutzungsbeschränkungen. Für Hetzner werden die einschlägigen ISO-27001- und BSI-C5-Nachweise innerhalb ihres ausgewiesenen Geltungsbereichs berücksichtigt. Feststellungen und erforderliche Maßnahmen werden dokumentiert und nachverfolgt.

- Schriftliche Festlegung der Weisungen
  Personenbezogene Daten werden durch Auftragsverarbeiter ausschließlich auf Grundlage dokumentierter Weisungen und der abgeschlossenen Vereinbarungen nach Art. 28 DSGVO verarbeitet. Weisungen und Änderungen werden nachvollziehbar dokumentiert. Erkennt ein Auftragsverarbeiter eine möglicherweise rechtswidrige Weisung oder eine Abweichung, wird die Verarbeitung soweit erforderlich ausgesetzt und an die zuständige Stelle sowie den Datenschutzbeauftragten eskaliert.

Verfügbarkeitskontrolle / Integrität

- Unterbrechungsfreie Stromversorgung und Überspannungsschutz
  Die Stromversorgung der bei Hetzner betriebenen Rechenzentrumsinfrastruktur wird durch die vom Rechenzentrumsbetreiber vorgesehenen redundanten Versorgungswege, unterbrechungsfreie Stromversorgung, Überspannungsschutz und Notstromverfahren abgesichert. DUSOFFICE prüft diese Maßnahmen im Rahmen der Dienstleisterkontrolle anhand der vertraglichen Unterlagen und verfügbaren Prüf- beziehungsweise Zertifizierungsnachweise innerhalb ihres jeweiligen Geltungsbereichs.

- Durchführung von Belastbarkeitstests
  Mindestens quartalsweise werden Lasttests mit einer großen Zahl paralleler automatisierter Anrufe durchgeführt; Ergebnisse werden intern dokumentiert und für die Weiterentwicklung und Optimierung künftiger Softwareversionen genutzt. Ebenfalls mindestens quartalsweise werden die Dauer eines Neustarts aller Dienste bis zur vollständigen Betriebsbereitschaft sowie eine vollständige Wiederherstellung aus einem Backup bis zum Datenstand des Vortags ermittelt und dokumentiert. Ein automatisches Failover zu einem anderen Provider-Endpunkt wird geprüft und ist geplant.

- Zusätzliche Sicherungskopien mit Lagerung an besonders geschützten Orten
  Sicherungskopien werden verschlüsselt und vom laufenden Produktivbetrieb zugriffstechnisch getrennt auf Hetzner Storage aufbewahrt. Zugriffe sind auf berechtigte Administratoren mit verwalteten SSH-Schlüsseln beschränkt und werden überwacht. Aufbewahrungsfristen werden automatisiert durchgesetzt; die Ausgestaltung schützt die Sicherungen insbesondere vor unberechtigter Veränderung und den Auswirkungen eines Angriffs auf die Produktivsysteme.

- Ständig kontrolliertes Backup- und Recoverykonzept
  Von den virtuellen Maschinen und Datenbanken werden täglich verschlüsselte Sicherungen erstellt und für 30 Tage auf Hetzner Storage aufbewahrt. Der administrative Zugriff erfolgt ausschließlich mit verwalteten SSH-Schlüsseln. Wiederherstellungstests werden quartalsweise und zusätzlich nach Änderungen am Sicherungsverfahren durchgeführt; Ergebnisse, Abweichungen und Korrekturmaßnahmen werden dokumentiert.

- Notfallkonzept
  Für TARIS gilt ein dokumentiertes Notfall- und Wiederanlaufkonzept mit System- und Abhängigkeitsinventar, Verantwortlichkeiten, Melde- und Eskalationswegen, Wiederanlaufreihenfolge sowie festgelegten Wiederanlauf- und Datenverlustzielen. Die redundante Verteilung der VMs auf mehrere Host-Server, die Abhängigkeiten zu externen Sprach- und KI-Diensten sowie betriebliche Ausweich- und manuelle Übergabeverfahren werden berücksichtigt. Das Konzept wird mindestens jährlich und nach wesentlichen Änderungen überprüft.

- Sicherstellung einer funktionsfähigen Klimatisierung
  Klimatisierung, Temperatur- und Umgebungsüberwachung sowie Brandfrüherkennung und Löschtechnik der Host-Server liegen in der Verantwortung des Hetzner-Rechenzentrums. DUSOFFICE berücksichtigt und überprüft die Maßnahmen im Rahmen der Auswahl und regelmäßigen Kontrolle des Unterauftragnehmers anhand vertraglicher Angaben und geeigneter Nachweise innerhalb ihres ausgewiesenen Geltungsbereichs.

Gewährleistung des Zweckbindungs-/Trennungsgebotes

- Trennung von Produktiv- und Testsystem
  Entwicklungs-, Test- und Produktivumgebung werden in getrennten Hosting-Umgebungen mit getrennten Datenbanken betrieben. Zugriffsrechte, Zugangsdaten, Schlüssel und Schnittstellenkonfigurationen werden je Umgebung getrennt verwaltet. Produktivdaten werden grundsätzlich nicht für Entwicklung oder Tests verwendet; erforderliche Ausnahmefälle bedürfen dokumentierter Freigabe und vorheriger wirksamer Anonymisierung oder mindestens geeigneter Pseudonymisierung.

- Logische Mandantentrennung (Software)
  Bei größeren Anrufvolumina und entsprechender Mindestabnahmevereinbarung kann eine eigene TARIS-Instanz ausschließlich für den jeweiligen Kunden bereitgestellt werden. In diesem Fall befinden sich nur dessen Daten auf der ausschließlich dieser VM zugeordneten verschlüsselten virtuellen Festplatte. Eine allgemeine Trennung über separat verschlüsselte Datenbanken je Kunde bleibt geplant.