Technische und Organisatorische Maßnahmen (TOM)

Alle Funktionen von campflow wurden von Anfang an mit Datenschutz im Blick entwickelt (privacy by design). Darüber hinaus setzt das Tool an verschiedenen Stellen durch sinnvolle Voreinstellungen Impulse für eine datenschutzkonforme Nutzung (privacy by default).

Datenminimierung

Features, die Nutzer:innen bei der Umsetzung unterstützen

- Frühestmögliche Löschung von personenbezogenen Daten bei Wegfall des Verarbeitungszweckes, z.B. Vernichtung einzelner, nicht mehr benötigter Datenfelder bei stornierten Teilnehmenden
- Standardmäßig werden in Anmeldeformularen keine sensiblen Datenkategorien erfasst. Diese müssen aktiv hinzufügt werden (privacy by default)
- Im Listenexport müssen die zu exportierenden Datenfelder aktiv ausgewählt werden. Es wird damit gefördert, nur das Mindestmaß der für den jeweiligen Zweck benötigten Daten zu exportieren, falls möglich sogar in anonymisierter Form.

Unsere internen Maßnahmen

- Nur das Mindestmaß der erforderlichen Stammdaten wird bei erstmaliger Registrierung erfasst. So erfolgt beispielsweise die Eingabe der Rechnungsadresse erst bei Abschluss eines Abos.
- Möglichkeiten zur selbstständigen Löschung und Berichtigung von Datenbeständen direkt durch Nutzer:innen, ohne Kontakt zu und ohne Einflussnahme durch Mitarbeitende.
- Automatische und umfassende Löschroutinen bei Löschung von personenbezogenen Daten nach einem festgelegten Löschkonzept

Verfügbarkeit

Features, die Nutzer:innen bei der Umsetzung unterstützen

- Vertraglich garantierte Verfügbarkeit des Tools
- Transparente Kommunikation des Bearbeitungsstandes von Störungen und Wartungsarbeiten via Status-Page unter https://status.campflow.de

Unsere internen Maßnahmen

- Verfügbarkeit der Serverinfrastruktur wird durch den Dienstleister Hetzner gewährleistet und ist vertraglich verankert.
- Die Rechenzentren von Hetzner sind nach ISO/IEC 27001:2013 zertifiziert. Die von der Hetzner Online GmbH getroffenen technischen und organisatorischen Maßnahmen finden Sie unter https://go.campflow.de/tom-hetzner.
- Laufendes Monitoring der Produktivsysteme via Application Performance Monitoring (APM) und Uptime Tracking
- Automatische Benachrichtigung der Mitarbeitenden bei Störungen (ständige Health Checks, Crash Reporting)
- Stichprobenartige sowie vorfallsbasierte Kontrolle der Log-Dateien
- Zusätzliche, tägliche Offsite-Datenbank-Backups mit automatisiertem Wiederherstellungsprozess
- Umfassende Backups vor Wartungsmaßnahmen
- Vollständige, regelmäßige Backup der Konfiguration

- Wiederherstellung der Verarbeitungstätigkeit wird durch dokumentierte bzw. automatisierte Konfigurationsabläufe unterstützt und beschleunigt
- Vertretungsregelung für abwesende Mitarbeitende

Integrität

Features, die Nutzer:innen bei der Umsetzung unterstützen

- Bei Registrierung abgeschlossener Auftragsverarbeitungsvertrag (AVV) regelt die Datenverarbeitungstätigkeit
- Personenbezogenen Daten können nur durch autorisierte Nutzer:innen aus einem begrenzten Personenkreis bearbeitet werden
- Einfache Löschbarkeit bzw. Korrigierbarkeit falscher Daten über das Datenschutz-Center
- Bestätigungsmodals vor allen destruktiven Aktionen, um unbeabsichtigten Datenverlust auszuschließen

Unsere internen Maßnahmen

- Regelmäßige Software-Updates
- Virenschutz der berechtigten Endgeräte
- Einsatz eines zeitlich begrenzten Verfahrens zur Authentifizierung zugreifender Nutzer:innen und Gerätschaften (u.a. JSON Web Tokens, regelmäßiger Token Refresh über zentralen Dienst)
- Vollständige Prüfung des Ist-Zustandes der Software mittels automatisierter Tests (Unit Tests, Integration Tests, End-to-End Tests)
- Prozess zur zeitnahen Benachrichtigung und Prüfung von Ausnahmen in der Datenverarbeitung (Crash Reporting, Error Logging)
- Einsatz von Prüfsummen bei der Verarbeitung und Archivierung von Belegen
- Sorgfältige Auswahl der Auftragnehmer (Zertifizierung, Standort, etc.)
- Umfang der Verarbeitung personenbezogener Daten durch Auftragsverarbeiter mittels eindeutiger Vertragsgestaltung geregelt (insbesondere AVV nach Vorschrift der DSGVO)
- Auftragnehmer werden vor Aufnahme der Datenverarbeitung nach Vorschriften der DSGVO auf die Einhaltung der erforderlichen technischen und organisatorischen Maßnahmen überprüft
- Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus bei längerer Zusammenarbeit
- Sicherstellung der Löschung/Vernichtung von Daten nach Beendigung des Auftrags

Vertraulichkeit

Features, die Nutzer:innen bei der Umsetzung unterstützen

- Zugang zu personenbezogenen Daten erfolgt nur durch autorisierte Nutzer:innen aus einem begrenzten Personenkreis
- Vermeidung von nicht geschützten Datenträgern (z.B. Papier) durch Einsatz von campflow
- 2-Faktor-Authentifizierung via TOTP-Einmalcodes konfigurierbar
- Deaktivieren der 2-Faktor-Authentifizierung nur mittels Bestätigungslink an E-Mail; keine Änderung der E-Mail während aktivierter 2-Faktor-Authentifizierung
- Passwort-Mindestlänge von 8 Zeichen sowie Mindestanforderungen an Komplexität (mind. eine Zahl sowie Groß- und Kleinbuchstaben)

Unsere internen Maßnahmen

- Bereitstellung von Daten ausschließlich über 256 bit TLS-verschlüsselter Verbindungen wie sftp, https etc.
- Schutz gegen Brute-Force-Attacken der Login-Seiten (Rate Limiting)
- Begrenzte Gültigkeit von Bestätigungslinks im Registrierungsverfahren
- Verpflichtung der Mitarbeitenden zur Vertraulichkeit (NDA / Vertraulichkeitserklärung)
- Clean Desk Policy
- Anzahl der Administratoren auf das Notwendigste reduziert
- Regelungen und Kontrollen für Fernzugriff durch Support: Protokollierung des Zugriffs unter Angabe einer Begründung durch Support-Personal, regelmäßige Revision aller protokollierten Zugriffe durch Mitarbeitende durch die Geschäftsleitung
- Technische Verpflichtung zur Einrichtung von 2-Faktor-Authentifizierung für alle Mitarbeitenden, sofern präferiert mittels Hardware-Sicherheitsschlüssel
- Technische Maßnahmen zur Umsetzung der unternehmensweiten Passwortrichtlinien: Randomisierte Erstellung und Aufbewahrung via Passwort-Manager sowie regelmäßiger Abgleich zur Vermeidung von geleakten oder mehrfach verwendeten Passwörtern
- Ein Berechtigungskonzept nach dem “Need-to-Know-Prinzip” ist im Einsatz. Alle intern genutzten Applikationen und Datenbanken sehen eine differenzierte Einräumung von Berechtigungen vor.
- Strikte räumliche Trennung von Arbeitsplätzen und Servern
- Schutz gegen unberechtigte interne und externe Zugriffe durch eine Firewall
- Keine direkte, externe Zugriffsmöglichkeit auf den Datenbankserver durch Abschottung in privates Netzwerk
- Sicherung aller digitaler Datenträger (Laptops, etc.) durch ein starkes Passwort
- Zugriff auf Produktivsysteme nur via SSH-Schlüssel (Secure Shell)
- Einsatz von Festplattenverschlüsselung aller Endgeräte, die über Zugriffsschlüssel der Produktiv-Systeme verfügen
- Trennung in Entwicklungs-, Test- und Produktivsysteme
- Zutrittskontrolle zu den Rechenzentren: Die von der Hetzner Online GmbH getroffenen technischen und organisatorischen Maßnahmen finden Sie unter https://go.campflow.de/tom-hetzner

Nichtverkettung

Features, die Nutzer:innen bei der Umsetzung unterstützen

- Nichtverkettung von personenbezogenen Daten (z.B. keine Zusammenführung von Teilnehmendendaten aufgrund identischer Datenfelder)

Unsere internen Maßnahmen

- Pseudonymisierte Erfassung von Fehlerprotokollen
- Einsatz von zweckspezifischen Pseudonymen bei der Verarbeitung von Kontobewegungsdaten

Transparenz

Features, die Nutzer:innen bei der Umsetzung unterstützen

- Vollständige Zusammenstellung aller Teilnehmendendaten einer betroffenen Person als übersichtliches PDF im Datenschutz-Center, um dem Recht auf Auskunft unverzüglich nachkommen zu können

Unsere internen Maßnahmen

- Dokumentation der Verträge mit externen Dienstleistern und Dritten, von denen Daten erhoben bzw. an die Daten übermittelt werden (z.B. AVV mit Hostinganbietern)
- Zeitnahe Benachrichtigung von Betroffenen bei Datenpannen oder bei Weiterverarbeitung zu einem anderen Zweck
- Dokumentation der durchgeführten automatischen Tests
- Versionierung sowie Protokollierung von Zugriffen und Änderungen des Source Codes sowie der Datenbankbackups
- Lückenlose Protokollierung von Fernzugriffen durch Support
- Berücksichtigung der Auskunftsrechte von Betroffenen im Auswertungskonzept

Intervenierbarkeit

Features, die Nutzer:innen bei der Umsetzung unterstützen

- Möglichkeit des Ausschlusses einzelner Personen beim Versand von Rundmails
- Manuelle Eingriffs- und Korrekturmöglichkeiten bei automatischen Vorgängen in der Buchhaltung, z.B. Korrektur automatischer Zuordnungen oder manuelle Anpassung des automatisch hinterlegten Wechselkurses

Unsere internen Maßnahmen

- Zentrale Kontaktmöglichkeit für Betroffene, siehe Datenschutzerklärung unter https://go.campflow.de/datenschutz-app
- Möglichkeit der manuellen Unterbrechung automatisch angestoßener Löschprozesse, z.B. als Reaktion auf eine erfolgte Vorankündigung per Mail