collla Verarbeitungsverzeichnis

Verzeichnis von Verarbeitungstätigkeiten nach Art. 30
EU-Datenschutz-Grundverordnung (DSGVO)

Das Produkt collla wird von der collla GmbH entwickelt und betrieben. Die collla GmbH kümmert sich um die gesetzlichen Anforderungen zum Datenschutz und darüber hinaus auch ganz allgemein um die Datensicherheit im Bezug auf collla. Datenschutz und Datensicherheit hat bei uns Priorität. Dieses Dokument erklärt, welche Daten wir speichern, zu welchem Zweck die Daten verwendet werden und welche technisch-organisatorischen Maßnahmen wir zur Sicherheit der Daten vorgesehen haben.

Stammdaten des Auftragverarbeiters

collla GmbH

Schottenfeldgasse 40/8
1070 Wien
Österreich

Datenschutzbeauftragte: Catherine Kupetzius, c.kupetzius@collla.com

Kategorien der Verarbeitung

collla ist eine Kommunikationsplattform für Unternehmen, Betriebsräte und deren Belegschaft. Die Plattform wird von den Betriebsräten administriert und bietet ihnen die Möglichkeit Inhalte einzutragen und so der Belegschaft zur Verfügung zu stellen. Die Plattform bietet außerdem verschiedene Möglichkeiten zur Kommunikation zwischen der Belegschaft und den Betriebsräten.

collla umfasst zwei Plattformen, das Admin Portal unter https://admin.collla.com sowie die “collla” App für mobile Geräte, die in allen gängigen App Stores verfügbar ist. Das Admin-Portal erlaubt den Betriebsräten die Administration der Inhalte. Die mobile “collla” App bietet den Mitarbeitern und den Betriebsräten Zugriff auf die zur Verfügung gestellten Inhalte. Der Login funktioniert überall mittels der Handynummer und einem auf die Handynummer versandten SMS Code.

Die gespeicherten Daten lassen sich grob in drei Kategorien teilen:

1. Daten, die für die Technik benötigt werden (z.B Handynummer für den Login oder Zuordnung zu Abteilungen, um Beiträge für diese Abteilung freizugeben)
2. Inhalte, die Betriebsräte und Benutzer teilen (z.B. Beiträge, Nachrichten)
3. Protokolle zur Interaktion, die zur Fehlerbehebung und zur Verbesserung der Funktionen genutzt werden.

Datenschutz hat für uns Priorität. Um diese oben genannten Funktionalitäten zu ermöglichen, speichern wir für die Technik in collla (oben Punkt 1.) daher nur folgende Daten:

4. Name des Benutzers
5. Handynummer des Benutzers

Sollen Inhalte Benutzern in bestimmten “Kategorien” freigegeben werden können, so werden diese “Kategorien” benötigt. Diese Kategorien “verstehen” wir nicht tiefer, es ist lediglich eine Möglichkeit für den Betriebsrat Inhalte nur dem interessierten Teil der Belegschaft freizugeben. In der Regel handelt sich es dabei um:

- Abteilung im Unternehmen
- Ist ÖGB Mitglied ja/nein

Benutzer können auch mittels E-Mail eingeladen werden, in dem Fall wird ebenfalls gespeichert:

- E-Mail Adresse des Benutzers

Um in sicherheitskritischen Prozessen wie bei dem Login eine hohe Sicherheit bieten zu können, werden in diesen Prozessen zusätzlich folgende Informationen protokolliert:

- IP Adresse und Uhrzeit

Um Mitarbeiterlisten zu importieren, wird in der Liste eine eindeutige Identifikation wie zum Beispiel eine Personalnummer oder eine Sozialversicherungsnummer benötigt. Diese Nummer wird ausschließlich beim Import direkt im Browser verwendet und wird nicht in unseren Services gespeichert. Da es sich hier teilweise um hoch sensible Daten handelt, lassen wir diese direkt im Browser durch eine geeignete Hash-Funktion (i.d.R SHA256 mit Seed) laufen. Das Ergebnis dieser Hash-Funktion ist nicht auf die Nummer zurückführbar und auch nicht mit anderen Systemen abgleichbar.

Betriebsräte und Mitarbeiter haben die Möglichkeit in collla Inhalte zu teilen (oben genannter Punkt 2.). Einige Beispiele dazu sind hier Beiträge, Kommentare und Direktnachrichten. Wir speichern diese Inhalte, um sie entsprechend zur Verfügung stellen zu können. Wir analysieren sie aber nicht oder ähnliches. Das sind einfach nur Inhalte von den Nutzern für die Nutzer. Die Verantwortung für diese und andere Inhalte liegt bei dem Betriebsrat bzw. den Administratoren des Accounts.

Unsere Services speichern Daten ausschließlich in der Europäischen Union. Um eine angenehme Benutzererfahrung sicherzustellen, werden die Daten teilweise zusätzlich auf den Endgeräten der Benutzer zwischengespeichert.

collla stellt die Plattform zur Verfügung und kümmert sich auf Wunsch der Administratoren um das Importieren von Daten und eventuelle Problemlösungen. Ausschließlich für diesen Zweck können bestimmte entsprechend geschulte Mitarbeiter auf die Daten zugreifen.

Übermittlung von personenbezogenen Daten in Drittländer

collla übermittelt keine personenbezogenen Daten in Drittländer.

Technisch-Organisatorische Maßnahmen

Datencenter auf höchstem Standard ISO/IEC 27001, ISO/IEC 27017 und ISO/IEC 27018 zertifiziert. Für die Büros und Mitarbeiter gelten mindestens folgende Regelungen:

Zutrittskontrolle:

- Sicherheitsschlösser
- Besucher in Begleitung durch Mitarbeiter
- Sorgfalt bei Auswahl Reinigungsdienste
- Videoüberwachung der Eingänge
- ISO/IEC 27001, ISO/IEC 27017 und ISO/IEC 27018 zerifiziertes Datencenter mit 6 Sicherheitsschichten

Zugangskontrolle:

- Login mit Benutzername + Passwort und zweitem Faktor
- Login mit biometrischen Daten
- Anti-Virus-Software
- Verschlüsselung von Computern, Notebooks und anderen mobilen Geräten
- BIOS Schutz (separates Passwort)
- Verwalten von Benutzerberechtigungen
- Zentrale Passwortvergabe
- Richtlinie „Sicheres Passwort“
- Anleitung „Manuelle Desktopsperre“

Zugriffskontrolle:

- Aktenschredder (mind. Stufe 3, cross cut)
- Physische Löschung von Datenträgern
- Einsatz Berechtigungskonzepte
- Minimale Anzahl an Administratoren
- Datenschutztresor
- Verwaltung Benutzerrechte durch Administratoren

Trennungskontrolle:

- Trennung von Produktiv- und Testumgebung
- Steuerung über Berechtigungskonzept

- Festlegung von Datenbankrechten

Pseudonymisierung:

- Im Falle der Pseudonymisierung: Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem und abgesicherten System (mögl. verschlüsselt)
- Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren / pseudonymisieren

Weitergabekontrolle:

- Bereitstellung über verschlüsselte Verbindungen wie sftp, https
- Sorgfalt bei Auswahl von TransportPersonal und Fahrzeugen

Eingangskontrolle:

- Technische Protokollierung der Eingabe, Änderung und Löschung von Daten
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden
- Klare Zuständigkeiten für Löschungen

Verfügbarkeitskontrolle:

- Feuer- und Rauchmeldeanlagen
- Serverraumüberwachung

Datenschutz-Maßnahmen:

- Interner Datenschutzbeauftragter
- Mitarbeiter geschult und auf Vertraulichkeit/Datengeheimnis verpflichtet
- Regelmäßige Sensibilisierung der Mitarbeiter mindestens jährlich

Incident-Reponse-Management:

- Intrusion Detection System (IDS)
- Intrusion Prevention System (IPS)
- Dokumentation von Sicherheitsvorfällen und Datenpannen

Datenschutzfreundliche Voreinstellungen:

- Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind

Auftragskontrolle:

- Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit
- Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis

- Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Vorliegen Bestellpflicht

Änderungen an diesem Dokument

Wir bemühen uns dieses Dokument immer aktuell zu halten und entsprechend für neue Funktionen anzupassen. Unsere Grundeinstellung wird aber immer die gleiche bleiben; wir schützen Ihre Daten, speichern nur was für den Betrieb notwendig ist und geben Ihrem Team die Möglichkeit Inhalte zu teilen und zu nutzen. Bitte beachten Sie dennoch, dass sich dieses Dokument von Zeit zu Zeit ändern kann. Sie können jederzeit eine aktuelle Version dieses Dokuments anfordern, schreiben Sie dazu einfach kurz an hallo@collla.com.