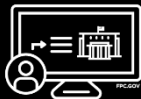


Nutzer können jederzeit ihre personenbezogenen Daten in ihrem Kunden-Konto einsehen und bearbeiten.

Es wird einfach vermittelt, wie Datenänderungen verfügbar gemacht und bearbeitet werden können.



ACCESS AND
AMENDMENT

ZUGANG UND ÄNDERUNG.

Einzelpersonen angemessenen Zugang zu personenbezogenen Daten und angemessene Möglichkeit zur Korrektur oder Änderung bieten.



ACCOUNTABILITY

Rollen und Berechtigungen innerhalb des Produkts unterstützen die Zuweisung und Überprüfung von Datenzugriffsrechten.

Datenschutzprüfungen werden regelmäßig durchgeführt und dokumentiert, in denen Verantwortlichkeiten klar definiert sind.

RECHENSCHAFTSPFLICHT.

Verantwortung für Einhaltung, Überwachung, Prüfung und Dokumentation geltender Datenschutzbestimmungen.

Rollen und Verantwortlichkeiten Mitarbeitender und Auftragnehmer für personenbezogene Daten klar definieren und entsprechende Schulungen anbieten.



AUTHORITY

Nutzer:innen werden vor der Nutzung des Produkts über die rechtliche Grundlage der Datenerhebung informiert.

Rollen für den Zugriff auf personenbezogene Daten werden durch Datenverarbeitungsverträge festgelegt und regeln u.a., welche Parteien Zugriff auf Daten haben.

BEFUGNIS.

Personenbezogene Daten nur dann erstellen, sammeln, verwenden, verarbeiten, speichern, aufbewahren, verbreiten oder offenlegen, wenn Befugnis dazu besteht und in entsprechender Mitteilung angegeben wird.





MINIMIZATION

Es werden nur Datenfelder im Produkt vorgegeben, die für den Zweck relevant sind, um die Erfassung unnötiger personenbezogener Daten zu vermeiden.

Mitarbeiter:innen dürfen nur personenbezogene Daten sammeln, die für ihre Aufgaben erforderlich sind und Daten, die nicht mehr benötigt werden, werden systematisch gelöscht.

MINIMIERUNG.

Nur solche personenbezogenen Daten erstellen, sammeln, verwenden, verarbeiten, speichern, aufbewahren, verbreiten oder offenlegen, die direkt relevant und notwendig sind, um einen gesetzlich genehmigten Zweck zu erfüllen, und nur so lange aufbewahren, wie es für die Erfüllung des Zwecks erforderlich ist.





QUALITY AND
INTEGRITY

Die Software informiert Nutzer:innen, welche ihrer personenbezogenen Daten für spezifische Zwecke verarbeitet werden, und gibt ihnen die Möglichkeit, diese zu bearbeiten.

Interne Richtlinien im Unternehmen stellen sicher, dass nur den Datenschutzrichtlinien entsprechende personenbezogene Daten verwendet werden.

QUALITÄT UND INTEGRITÄT.

Personenbezogene Daten mit solcher Genauigkeit, Relevanz, Aktualität und Vollständigkeit erstellen, erheben, verwenden, verarbeiten, speichern, pflegen, verbreiten oder offenlegen, wie es vernünftigerweise erforderlich ist, um die Fairness gegenüber dem Einzelnen zu gewährleisten.





**INDIVIDUAL
PARTICIPATION**

Benutzer:innen können spezifische Anfragen zur
Löschung ihrer personenbezogenen Daten über die
Plattform stellen und können ihre Zustimmung zur
Datennutzung einfach widerrufen.

Das Unternehmen stellt sicher, dass Anfragen zur
Korrektur- und Einsicht personenbezogener Daten auf
einfachem Weg schnell bearbeitet werden.

BETEILIGUNG DES EINZELNEN.

Den Einzelnen in den Prozess der Verwendung von personenbezogenen Daten einbeziehen und, wenn möglich, die Zustimmung des Einzelnen zur Erstellung, Erhebung, Verwendung, Verarbeitung, Speicherung, Pflege, Verbreitung oder Offenlegung von personenbezogenen Daten einholen. Verfahren zur Annahme und Bearbeitung von Beschwerden und Anfragen zum Datenschutz einrichten.





PURPOSE SPECIFICATION AND USE LIMITATION

Alle Datenverarbeitungszwecke werden transparent
im Benutzeroberfläche erklärt.

Personenbezogene Daten werden nur für den
ursprünglichen Zweck verwendet, der unter anderem
eine Weiterverarbeitung ohne Zustimmung verhindert.

ZWECKBESTIMMUNG UND NUTZUNGSBESCHRÄNKUNG.

Spezifischen Zweck, für den personenbezogene Daten gesammelt werden, mitteilen und nur für Zweck verwenden, verarbeiten, speichern, aufbewahren, verbreiten oder offenlegen, welcher in der Mitteilung erläutert wird oder der anderweitig rechtlich zulässig ist.





Das Produkt nutzt Verschlüsselung, sichere Passwörter, Zwei-Faktor-Authentifizierung und/oder regelmäßige Sicherheitsupdates.

Neben technischen Sicherheitsmaßnahmen wie Firewalls dürfen Mitarbeitender:innen nur über sichere, zugelassene Geräte auf personenbezogene Daten zugreifen.

SICHERHEIT.

Verwaltungstechnische, technische und physische Sicherheitsvorkehrungen zum Schutz von personenbezogenen Daten treffen, die dem Risiko und dem Ausmaß des Schadens entsprechen, der sich aus unbefugtem Zugriff, Nutzung, Änderung, Verlust, Zerstörung, Verbreitung oder Offenlegung ergeben würde.

Alle Informationen und ggf. Änderungen in der Erfassung und Nutzung von personenbezogenen Daten werden den Nutzenden deutlich angezeigt.

Datenschutzrichtlinien sind für alle Mitarbeitenden und Kund:innen verständlich und zugänglich.



TRC.GOV

TRANSPARENCY

TRANSPARENZ.

Informationspolitik und -praktiken in Bezug auf personenbezogene Daten transparent machen und klare und zugängliche Informationen über deren Erstellung, Erhebung, Verwendung, Verarbeitung, Speicherung, Pflege, Verbreitung und Offenlegung bereitstellen.