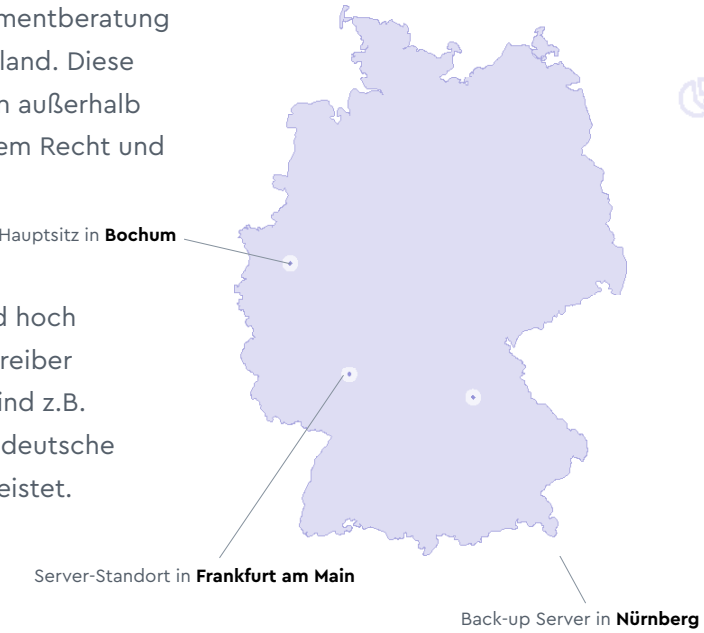
FAQ
Datenschutz & Datensicherheit

Unser Standort

Wo sitzt ihr?

factro ist ein Produkt der Schuchert Managementberatung GmbH & Co KG. mit Sitz in Bochum, Deutschland. Diese hat keine Gesellschafter oder Abhängigkeiten außerhalb von Deutschland und unterliegt nur deutschem Recht und Gerichtsbarkeit.



factro wird ausschließlich in zertifizierten und hoch gesicherten Rechenzentren namenhafter Betreiber in Deutschland gehostet: Server-Standorte sind z.B. Frankfurt am Main und Nürnberg. Damit sind deutsche Datenschutzstandards durchgängig gewährleistet.

Datenschutzkonformität

Ist factro Datenschutz-konform?

Für factro gilt die volle EU-DSGVO-Konformität sowie das deutsche Bundesdatenschutzgesetz (BDSG-neu). Dies wurde von unabhängigen Stellen geprüft und testiert.

Transparenz und Einwilligung (Art. 12–14 DS-GVO):

Bei der Registrierung klären wir Dich über die Erhebung Deiner Daten auf und setzen das Douple-Opt-in-Verfahren ein. Dies gilt auch, wenn Du Dritte zur Mitarbeit in Deine Cloud einlädst.

Auskunft (Art. 15 DS-GVO):

Du und die von Dir eingeladenen Mitarbeitenden können die personenbezogenen Daten aus eigenen factro Kontos jederzeit einsehen.

Berichtigung (Art. 16 DS-GVO):

Korrigiere Deine Daten selbstständig und jederzeit.

Vergessenwerden (Art. 17 DS-GVO):

Als Eigentümer einer factro Cloud kannst Du sowohl die Cloud als auch Deinen Account selbstständig zur Löschung durch einen automatisierten Prozess vormerken. Personenbezogene Stammdaten von Mitarbeitenden können auf Anfrage der betroffenen Person per Knopfdruck anonymisiert werden.

Einschränkung der Verarbeitung (Art. 18 DS-GVO):

Schränke die Verarbeitung Deiner Daten selbstständig ein, z.B. durch Opt-Out aus Mailing-Listen oder durch die Deaktivierung von Benachrichtigungs-E-Mails.

Übertragbarkeit (Art 20. DS-GVO):

Exportiere die von uns zu Deinem Account erfassten personenbezogenen Dateien jederzeit in einem allgemeinen maschinenlesbaren Format für Dich selbst oder zur Übergabe an einen anderen Verarbeiter.

Sind factro und sein (Daten-) Standort zertifizert?

factro wird am **Standort Bochum** entwickelt und getestet. Die Entwicklung orientiert sich an anwendbaren Normen, ist aber nicht eigens zertifiziert. Der Produktiv- und Backup-Betrieb von factro sowie die Datenhaltung erfolgen ausschließlich in **deutschen Rechenzentren**, die fortlaufend nach ISO 27001 und weiteren anwendebaren Normen zertifiziert sind.

Gibt es ein Sicherheitskonzept für factro?

Dauerhafte Informationssicherheit gemäß DSGVO: factro hat ein Informationssicherheitsmanagementsystem (ISMS) eingeführt, mit dem Vorgehensweisen und Regeln zur Wahrung einer dauerhaften und nachvollziehbaren Informationssicherheit und zur Einhaltung der Vorgaben der DSGVO gewährleistet werden.

Wie wird die Infomationssicherheit (per ISMS) von factro gewährleistet?

Maßnahmen:
Es werden alle notwendigen technischen und organisatorischen Maßnahmen (TOM) zur Sicherung und zum angemessenen Schutz der Kundendaten getroffen. Diese sind in Anlage 2 zur AVV genannt.

Drittanbieter:
Es wird vetraglich sichergestellt, dass alle Dienstleister und Auftragsverarbeiter, an die Nutzerdaten übertragen werden, das Schutzniveau ebenfalls einhalten.

Mitarbeitende:
Es wird organisatorisch und vertraglich sichergestellt, dass factro Mitarbeitende angemessen/vertraulich mit persönlichen Kundendaten umgehen.

Verstöße und Sicherheitslücken:
Die entsprechenden Aufsichtsbehörden sowie betroffene Nutzer im Falle von Verstößen und Sicherheitslücken werden unverzüglich kontaktiert.

Mandantentrennung:

Die Mandantentrennung erfolgt bei den factro Standardprodukten durch Softwarelogik, indem bei allen Lese- und Schreiboperationen die Account- und Mandanten-ID mitgeführt, authentifiziert und autorisiert werden muss. Bei factro Enterprise-Produkten mit Managed Private Cloud erfolgt die Mandantentrennug physisch durch separate Hardware pro Kunde.

Privacy-by-Default / Privacy-by-Design:

Die factro Produktentwicklung achtet auf datenschutzfreundliche Voreinstellungen (Privacy-by-Default) und sog. eingebauten, d.h. intuitiven Datenschutz (Privacy-by-Design).

Datenschutzbeauftragte:
factro hat – unabhängig von einer diesbezüglich geltenden Verpflichtung – einen Datenschutzbeauftragten bestellt, der Regelungen zur Verarbeitung von personenbezogenen Daten überwacht und bei Fragen zur Verfügung steht.

Gibt es eine Auftragsverarbeitungsvereinbarung (AVV)?

Gemäß Art. 28 DSGVO wird eine Auftragsvereinbarung (AVV) auf Anfrage von Lizenznehmern der kostenplfichtigen Tarife angeboten, wenn deren Verarbeitungstätigkeiten dies erfordern.

Auftragsverarbeitung durch Dritte

Gibt factro personenbezogene Daten weiter?

Die vertraglichen Leistungen und Funktionen von factro werden z.T. unter Inanspruchnahme von Leistungen Dritter erbracht, die als Unterauftragnehmer zu diesem Zweck ggf. auch personenbezogene Daten der Benutzer verarbeiten müssen. Diese werden in Anlage 1 AVV aufgelistet.

Sind beteiligte Unterauftragnehmer auf den Datenschutz verpflichtet?

Gemäß Art. 28 DSGVO wurden Auftragsdatenverarbeitungsverträge mit allen Service Providern und Unterauftragsverarbeitern geschlossen, die im Kontext der Bereitstellung von factro beauftragt sind.

Das Schutzniveau der geschlossenen Auftragsverarbeitungsverträge entspricht mindestens demjenigen, das den Lizenznehmern als Auftraggeber von factro angeboten wird.

Notfallprozeduren

Gibt es für factro Notfallpläne?

Es sind Prozesse zum Handling von Fehlfunktionen und Beeinträchtigungen der Verfügbarkeit etabliert, die auch bedarfsweise Information an Benutzer beinhalten. Die Information erfolgt per E-Mail oder innerhalb der Plattform.

Wie hoch ist die garantierte Verfügbarkeit von factro?

Die garantierte Verfügbarkeit von factro beträgt 95% im Jahresmittel. Die effektive Verfügbarkeit von factro im zurückliegenden Jahreszeitraum betrug über 99%.

Kann eine höhere Verfügbarkeit vertraglich vereinbart werden?

Auf Anfrage kann eine höhere Verfügbarkeit kalkuliert und vertraglich vereinbart werden.

Gibt es geplante Ausfallzeiten?

Geplante Ausfallzeiten, z.B. für Updates und Wartungsarbeiten, werden möglichst in die Abend- und Nachtstunden gelegt. Bei einer längeren erwartbaren Beeinträchtigung der Benutzer erfolgt vorab eine Ankündigung per E-Mail.

Datenschutzrichtlinien

Gibt es für factro eine Datenschutzrichtlinie?

Die factro Datenschutzrichtlinie ist mitgeltender Vertragsbestandteil des Lizenzvertrags und informiert jeden Benutzer darüber, welche personenbezogenen Daten bei der Registrierung eines factro Accounts wie erfasst, gespeichert und verarbeitet werden:
https://www.factro.de/datenschutzerklaerung-factro/

VVT

Gibt es für factro ein Verzeichnis der Verarbeitungstätigkeiten (VVT)?

Ein Verzeichnis der Verarbeitungstätigkeiten liegt – unabhängig von einer Verpflichtung zur Führung eines solchen – für diejenigen personenbezogenen Daten vor, die factro zur Registrierung, Lizensierung und Bereitstellung der vertraglich vereinbarten Leistung erhebt.

Führt factro ein VTT für den Lizenznehmer?

Für diejenigen personenbezogenen Daten, die der Lizenznehmer und seine Anwender bei der Benutzung von factro erheben, obliegt die Beurteilung der Notwendigkeit und die Führung eines VVT dem Lizenznehmer als verantwortliche Stelle i.S.d. DSGVO.

AVV/Vertraulichkeitserklärung

Gibt es eine Auftragsverarbeitungsvereinbarung (AVV)?

Gemäß Art. 28 DSGVO wird eine solche Anfrage Lizenznehmern der kostenpflichtigen Tarife angeboten, wenn deren Verarbeitungstätigkeiten dies erfordern.

Die aktuelle Version kann unter **sales@factro.de** angefragt werden.
Individuelle Vereinbarungen von Auftraggebern können in den Standardtarifen nicht abgeschlossen werden.

Gibt es für factro eine Vertraulichkeitserklärung?

factro bietet schon vor Vertragsabschluss eine standardisierte Vertraulichkeitsvereinbarung für Interessenten an, die uns zur Bewertung der Eignung für ihren Use-Case vertrauliche Daten und Fakten offenlegen möchten. Individuelle Vertraulichkeitsvereinbarungen werden nicht angeboten oder abgeschlossen.

Rechenzentren

Absicherung/Zugangskontrollen: s. Anlage 1 AVV – Technisch-organisatorische Maßnahmen. Die Notfallprozeduren der Data Center sind Bestandteil ihres jeweils zertifizierten Sicherheitskonzeptes.

Die beauftragten Data Center entsprechen TIER 2 oder höher.

Für alle Data Center, in denen factro gehostet wird oder Backups gelagert werden, liegen mindestens **gültige Zertifikate** gem. ISO/IEC 27001 und ISO/IEC 9001 vor. Eine Zertifizierung nach DIN EN 50600 ist keine notwendige Voraussetzung für das Hosting von factro und wird auch nicht angestrebt.

factro wird ausschließlich in zertifizierten und hoch gesicherten Rechenzentren namenhafter Betreiber in Deutschland gehostet:
Server-Standorte befinden sich z.B. in **Frankfurt am Main** und in **Nürnberg**.

Backup-Konzept/GEO-Redundanz

Backup Schema:
Backups von Benutzer-Uploads und Datenbank-Sicherungen erfolgen 1x täglich zu Offload-Zeiten.

Geplante Backups sind in der regulären Lizenzgebühr enthalten.
Backups werden geo-redundant innerhalb der EU gespeichert.
Weitere Informationen zum Back-Up-Konzept sind dem entsprechenden Handout zu entnehmen.

Wie lange werden die Daten im Backup aufbewahrt?

Vorhalte Schema:

letzte 4 Wochen: tagesgenau
bis zu 3 Monaten: wochengenau
bis zu 6 Monaten: monatsgenau
bis zu 1 Jahr: quartalsgenau

Werden die Backup getrennt von den Produktivsystemen aufbewahrt?

Die automatischen Datensicherungen erfolgen auf separierten Systemen an anderen Standorten innerhalb der EU, auf die vom Produktivsystem aus kein Zugriff besteht.

Kann ich meine Daten aus einem Backup wiederherstellen?

Backups sind für Benutzer nicht zugänglich oder exportierbar. Sie dienen der Wiederherstellung des Gesamtsystems nach einem Ausfall. Die Wiederherstellung von Individualdaten nach Bedienfehler ist im Einzelfall als Dienstleistung nach Aufwand zu bewerten und wird nicht garantiert.

Kann ich eigene Backups herstellen?

Lizenznehmer können eigene Abzüge ihrer strukturierten Daten über die offene REST API von factro anfertigen.

Es besteht ein aktives Monitoring aller für die Verfügbarkeit und Performance relevanten Parameter, damit frühzeitig auf Engpässe und Störungen reagiert werden kann. Das Load Balancing zur Verteilung der Rechenlasten gewährleistet auch die Failover für die Applikationsserver.

Datenverschlüsselung

Die Datenbank- und Storage-seitige Ablage (in-rest) erfolgt nach Mandanten (factro Clouds) software-logisch getrennt. Bei jedem Speicher- und Lesevorgang wird die Mandant-ID zwingend mitgeführt und die Identität und Autorisierung des anfordernden Benutzers geprüft.

So wird sichergestellt, dass nur berechtigte Benutzer mit gültiger Anmeldesitzung auf die jeweils für sie freigegebenen Daten ihres Mandanten zugreifen können.

Die Speicherung erfolgt innerhalb des Mandanten unverschlüsselt, um dort globale Funktionen wie die Volltextsuche zu ermöglichen.

Benutzerdaten werden zwischen dem Browser des Benutzers und dem factro Server verschlüsselt transportiert (in-transit).

Die Verschlüsselung über HTTPS erfolgt nach dem TLS1.3-Standard mit Fallback auf TLS1.2.

Datensicherheitsstandards

Stand: 08.11.2024

Softwaretechnik

1. Web-basierte Saas-Applikation, nicht anfällig für Endgeräte-Viren
2. Modulare Architektur mit moderner Web Technik im BackEnd (nginx, node. js, PostgreSQL, Redis, ElasticSearch)
3. Einsatz von redundant ausgelegten Micro-Services (Containerisierung) für minimierte Wartungsfenster, automatisches Failo-over und Load Balancing
4. Standard-Browser[1] und native iOS-/Android-App als User Clients
5. Geschützer Datentransport mit SSL Verschlüsselung (TLS 1.3, SHA-256 mit RSA 4096)
6. Integrierter Schutz gegen Angriffe per XSS / SQL-Injection
7. 24/7 Software Monitoring aller relevanten Metriken

[1]Aktuelle Versionen von Google Chrome, Mozilla Firefox, Apple Safari, Opera, Microsoft Edge

Systemtechnik

1. Gekapselte VMs auf Debian-/Ubuntu-Basis mit Long Term Support als Docker Hosts
2. SSD-Storage mit 2N bzw. N+1 Auslegung für produktive Systeme
3. Attachment File Space nach S3 Standard, logisch separiert pro factro Cloud
4. Internes VLAN zwischen den VMs
5. Datensicherung auf geografisch separierte Systeme über DB-Dumps und Volume-Snapshots

Serverstandort: Interxion Data Center Campus FRA-1, **Frankfurt/Main**

Zertifiziert nach ISO/IEC 27001, ISO 22301, ISO 9001, ISO 14001, ISO 50001 und PCI DSS

Direkte Anbindung an DE-CIX

24/7 bewacht und gemonitort

Betrieb nach ITILv3

Dual Carrier Connect mit 40 Gbit/s Glasfaser-Backbones

DSGVO

Stand: November 2024

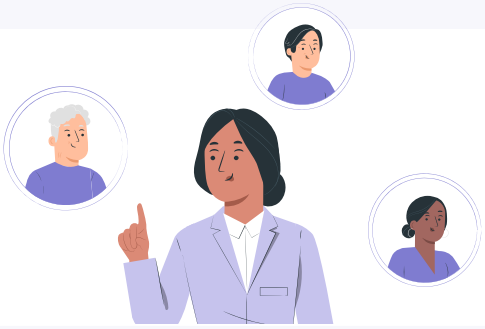
factro® unterstützt die DSGVO und die Betroffenenrechte gem. Art. 12 – 22 DSGVO bei der Erhebung von personenbezogenen Daten wie folgt:

1. Transparenz und Einwilligung

Art. 12–14 DSGVO

a. Bei der Erhebung personenbezogener Daten im Zuge der Registrierung und Buchung einer eigenen factro® Cloud wird die betroffene Person über den Zweck, den Umfang und die Rechtsgrundlagen der Erhebung sowie die Möglichkeit und Folgen des Widerrufs aufgeklärt und willigt aktiv in die Verarbeitung ein.

b. Für personenbezogene Daten, die im Rahmen der Einladung zur Mitarbeit in einer anderen factro® Cloud von einem verantwortlichen Dritten erfasst wurden, unterstützt factro® den Verantwortlichen bei der Ausübung seiner Aufklärungspflichten und Einholung der aktiven Einwilligung durch ein Double-Op-In-Verfahren.



2. Auskunftsrecht

Art. 15 DSGVO

a. Die betroffene Person hat die Möglichkeit, die sie betreffenden personenbezogenen Daten, die im Zuge der Registrierung und Buchung einer eigenen factro® Cloud erhoben wurden, regelmäßig online in ihrem factro® Account bzw. in der Lizenzverwaltung einzusehen.

b. Für personenbezogene Daten, die im Rahmen der Einladung zur Mitarbeit in einer anderen factro® Cloud von einem verantwortlichen Dritten erfasst wurden, unterstützt factro® den Verantwortlichen funktional bei der Ausübung seiner Informationspflichten unter Beachtung der für ihn eingestellten Rechte.

3. Recht auf Berechtigung

Art. 16 DSGVO

a. Die betroffene Person hat die Möglichkeit, die sie betreffenden personenbezogenen Daten, die im Zuge der Registrierung und Buchung einer eigenen factro® Cloud erhoben wurden, regelmäßig online in ihrem factro® Account bzw. in der Lizenzverwaltung einzusehen und dort bei Bedarf selbstständig zu korrigieren.

b. Für personenbezogene Daten, die im Rahmen der Einladung zur Mitarbeit in einer anderen factro® Cloud von einem verantwortlichen Dritten erfasst wurden, unterstützt factro® den Verantwortlichen funktional bei der Ausübung seiner Korrekturpflichten unter Beachtung der für ihn eingestellten Rechte.

4. Recht auf Vergessenwerden

Art. 17 DSGVO

a. Die betroffene Person hat das Recht, dass die sie betreffenden personenbezogenen Daten, die im Zuge der Registrierung und Buchung einer eigenen factro® Cloud erhoben wurden, nach Beendigung des Vertrags auf Anfrage oder nach Widerspruch gegen die Verarbeitung gelöscht werden, wo dem keine berechtigten Gründe oder höherwertigen Rechtspflichten des Verantwortlichen entgegenstehen. Dazu bietet factro® ein standartisiertes Verfahren zur Löschung des Accounts an.

b. Für personenbezogene Daten, die im Rahmen der Einladung zur Mitarbeit in einer anderen factro® Cloud von einem verantwortlichen Dritten erfasst wurden, stellt factro® dem Verantwortlichen unter der Beachtung der für ihn eingestellten Rechte ein Verfahren zur datenschutzkonformen Anonymisierung der Stammdaten der betroffenen Person zur Verfügung.

5. Recht auf Einschränkung der Verarbeitung

Art. 18 DSGVO

a. Die betroffene Person hat das Recht, die Nutzung der sie betreffenden personenbezogenen Daten, die im Zuge einer Registrierung und Buchung einer eigenen factro® Cloud erhoben wurden, auf Verlangen einzuschränken, wo dem keine berechtigten Gründe oder höherwertigen Rechtspflichten des Verantwortlichen entgegenstehen. Dazu bietet factro® der betroffenden Person z.B. die Möglichkeit eines selbstständigen OptOuts aus Mailing-Listen und der Deaktivierung der Benachrichtigungs-eMails.

b. Für personenbezogene Daten, die im Rahmen der Einladung zur Mitarbeit in einer anderen factro® Cloud von einem verantwortlichen Dritten erfasst wurden, stellt factro® dem berechtigten Verantwortlichen die Option der Deaktivierung von Benutzern zur Verfügung.

6. Recht auf Übertragbarkeit

Art. 20 DSGVO

a. Die betroffene Person hat das Recht, dass die sie betreffenden personenbezogenen Daten, die im Zuge einer Registrierung und Buchung einer eigenen factro® Cloud erhoben wurden, nach Beendigung des Vetrags oder nach Widerspruch gegen die Verarbeitung auf Anfrage in einem allgemeinen maschinenlesbaren Format an sie selbst oder einen anderen Verarbeiter übergeben werden. Dazu existiert ein standardisierter Prozess zum Export und Transfer der Daten im CSV-Format.

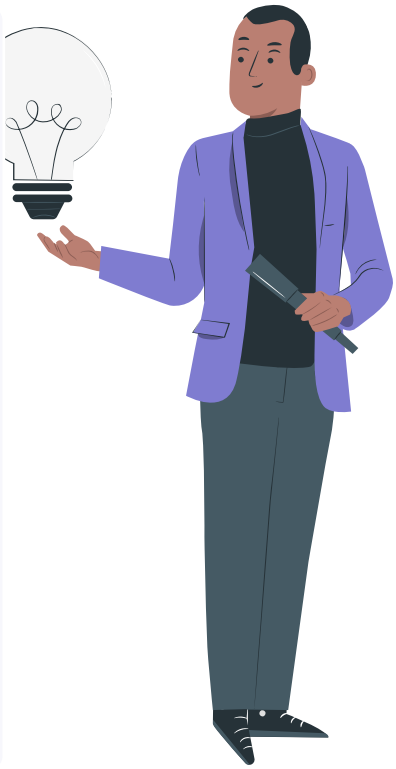
b. Für personenbezogene Daten, die im Rahmen der Einladung zur Mitarbeit in einer anderen factro® Cloud von einem verantwortlichen Dritten erfasst wurden, stellt factro® dem berechtigten Verantwortlichen die Option eines Exports von Benutzerstammdaten im CVS-Format zur Verfügung.

7. Recht auf Widerspruch gegen Direktwerbung und Profiling

Art. 21–22 DSGVO

a. Die betroffene Person hat das Recht, dass die sie betreffenden personenbezogenen Daten, die im Zuge der Registrierung und Buchung einer eigenen factro® Cloud erhoben wurden, nach Beendigung des Vetrags oder nach Widerspruch gegen die Verarbeitung auf Anfrage in einem allgemeinen maschinenlsebaren Format an sie selbst oder einen anderen Verarbeiter übergeben werden. Dazu existiert ein standardisierter Prozess zum Export und Transfer der Daten im CSV-Format.

b. Für personenbezogene Daten, die im Rahmen der Einladung zur Mitarbeit in einer anderen factro® Cloud von einem verantwortlichen Dritten erfasst wurden, stellt factro® dem berechtigten Verantwortlichen die Option eines Exportes von Benutzerstammdaten im CSV-Format zur Verfügung.



Schuchert Managementberatung GmbH & Co. KG
Geschäftsbereich factro®
Kirchharpener Str. 46
D-44805 Bochum
E-Mail: info@factro.de
Internet: www.factro.de
Support: +49 234–89155–55