Datenschutzinformation

(Zuletzt geändert: 12.10.26)

Diese Datenschutzinformation erläutert, wie personenbezogene Daten in der App Locio (nachfolgend „Website") durch die Locio GmbH verarbeitet werden. Die Locio GmbH verarbeitet ausschließlich solche Daten, die zur Bereitstellung und Sicherung der App erforderlich sind, und orientiert sich dabei am Grundsatz der Datenminimierung. „Personenbezogene Daten" sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (betroffene Person) beziehen, wie beispielsweise Name, Anschrift, Telefonnummer, Geburtsdatum, E-Mail-Adresse oder IP-Adresse. Informationen, die keiner bestimmten Person zugeordnet werden können, etwa aufgrund von Anonymisierung, gelten nicht als personenbezogene Daten.

1. Verantwortlicher

Nutzung im Rahmen Ihres Arbeitsverhältnisses

Wenn Sie die Locio App nutzen, weil Ihr Arbeitgeber Locio zur Abrechnung der Ladevorgänge Ihres Dienstfahrzeugs einsetzt, ist Ihr Arbeitgeber Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO. Locio verarbeitet die im Rahmen der App anfallenden Daten (z. B. Ladevorgänge, Zuordnung zu Ihrem Dienstfahrzeug, Abrechnungsinformationen) in diesem Fall als Auftragsverarbeiter nach Art. 28 DSGVO ausschließlich nach Weisung Ihres Arbeitgebers.

Für die unter 3.5 („Tracking und Analyse") genannten Verarbeitungen ist Locio eigener Verantwortung.

Eigenständige / private Nutzung der App

Wenn Sie die Locio App eigenständig aus dem jeweiligen App Store herunterladen und nutzen, ohne dass Ihr Arbeitgeber Locio offiziell eingeführt oder Sie zur Nutzung aufgefordert hat, ist Locio selbst Verantwortlicher für die Verarbeitung Ihrer personenbezogenen Daten.

In diesem Fall erbringen wir unsere Leistungen direkt Ihnen gegenüber (z. B. Erfassung und Auswertung Ihrer Ladevorgänge, Erstellung von Übersichten/Reports), die Verarbeitung erfolgt auf Grundlage des zwischen Ihnen und Locio bestehenden Nutzungsverhältnisses.

Locio GmbH
Sandstraße 3
80335 München
Deutschland
Tel.: 089 6931900 80
E-Mail: info(at)locio.de

Für Datenschutzanfragen oder zur Wahrnehmung Ihrer Betroffenenrechte wenden Sie sich bitte an datenschutz(at)locio.de.

2. Datenschutzbeauftragter

Zum Datenschutzbeauftragten hat Locio bestellt:

Kertos GmbH
Brienner Straße 41
80333 München

Deutschland
E-Mail: dsb(at)kertos.io

3. Datenverarbeitungen innerhalb der App

3.1 Bereitstellung und Nutzung der App

Beim Herunterladen der App werden die hierfür notwendigen Informationen an den App Store übertragen, insbesondere Nutzername, E-Mail-Adresse, Kundennummer, Zeitpunkt des Downloads, Zahlungsinformationen und die individuelle Gerätekennziffer. Der App Store erhebt zudem eigenständig verschiedene Daten und stellt Analyseergebnisse bereit. Auf diese Datenverarbeitung haben wir keinen Einfluss und sind hierfür nicht verantwortlich. Wir verarbeiten diese Daten nur, soweit dies für den Download der mobilen App auf Dein Endgerät erforderlich ist.

3.1.1 Amazon Web Services

Empfänger: Amazon Web Services EMEA SARL, 38 Avenue John F. Kennedy, L-1855 Luxembourg (Server-Infrastruktur)

Verarbeitete Daten:

- Nutzungsdaten (z.B. IP-Adresse, Datum und Uhrzeit der Anfrage)
- Gerätedaten (z.B. Gerätekennung, Betriebssystem)
- Kontaktdaten (z.B. E-Mail-Adresse, Handynummer)
- Netzwerkdaten (z.B. MAC-Adresse bei WLAN-Nutzung)
- Identifikationsdaten (z.B. eindeutige Geräte-Nummer IMEI, eindeutige Teilnehmernummer IMSI)
- App Store Daten (z.B. Nutzername, Kundennummer, Zahlungsinformationen)
- Technische Protokolldaten (z.B. Request- und Antwortdaten, Fehlermeldungen)

Rechtsgrundlage: Art. 6 Abs. 1 lit. b DSGVO, Art. 6 Abs. 1 lit. f DSGVO (Sicherstellung der Sicherheit und des Betriebs der App)

Speicherdauer: Für die Dauer der App-Nutzung und darüber hinaus entsprechend gesetzlicher Aufbewahrungsfristen

Weitere Informationen: https://aws.amazon.com/de/privacy/

3.1.2 Mobile Builds und Over-the-Air-Updates (Expo Application Services)

Zweck: Erstellung (Build) der mobilen App sowie Bereitstellung von Over-the-Air (OTA) Updates, damit App-Inhalte und Fehlerbehebungen ausgeliefert werden können, ohne dass ein erneuter Download über den App Store erforderlich ist

Empfänger: 650 Industries, Inc. („Expo"), 624 University Ave, Palo Alto, CA 94301, USA

Verarbeitete Daten:

- Technische Gerätedaten (z.B. Betriebssystem im Rahmen der Update-Anfrage)
- Zufällig generierte Geräte-Installations-ID (zur Erkennnung, welche Geräte ein Updaten angefragt haben – laut Anbieter nicht direkt identifizierend)
- IP-Adresse, Browsertyp/technische Verbindungsdaten

Rechtsgrundlage: Berechtigtes Interesse an Bereitstellung, Wartung und Aktualisierung der App (Art. 6 Abs. 1 lit. f DSGVO); ggf. Vertragserfüllung (Art. 6 Abs. 1 lit. b DSGVO)

Speicherdauer:

- EAS Build: 90 Tage
- EAS Update: Die Daten werden nur so lange gespeichert, wie dies für die Bereitstellung der Updates erforderlich ist (Angabe des Anbieters).

Drittlandtransfer: Übermittlung in die USA

Weitere Informationen: https://expo.dev/privacy

3.2 System Berechtigungen

Bestimmte Funktionen unserer App erfordern den Zugriff auf spezifische Schnittstellen und Daten Ihres Geräts. Je nach Betriebssystem ist hierfür Ihre ausdrückliche Einwilligung erforderlich. Nachfolgend erläutern wir, für welche Funktionen unsere App Berechtigungen anfordern kann (soweit relevant) und für welche Zwecke dies geschieht. Die Berechtigungen können Sie jederzeit in den Systemeinstellungen Ihres Geräts verwalten.

- Standortdienste / Standortdaten: Die Berechtigung zum Zugriff auf die Standortdienste Ihres Geräts ist erforderlich, damit die App auf den durch Ihr Gerät ermittelten Standort zugreifen kann. Wenn Sie den Zugriff nicht erlauben, ist eine standortbasierte Anzeige von Inhalten möglicherweise gar nicht oder nur eingeschränkt möglich.
- Benachrichtigungen/Push-Mitteilungen: Für die Nutzung von Push-Services ist eine Berechtigung erforderlich. Bei manchen Geräten ist diese standardmäßig für alle Apps aktiviert.
- Bluetooth: Die App benötigt Zugriff auf die Bluetooth-Schnittstelle Ihres Geräts, um eine Verbindung zu anderen Bluetooth-fähigen Geräten in Ihrer Umgebung herzustellen oder Daten auszutauschen.
- Zugriff auf gespeicherte Fotos: Für den Zugriff der App auf gespeicherte Fotos (Leserechte) oder zum Speichern von durch die App erzeugten Fotos (Schreibrechte) ist eine Zustimmung notwendig.
- Kamera: Die App benötigt eine Berechtigung zur Nutzung der Kamera Ihres Geräts, z. B., um Fotos aufzunehmen oder QR-Codes zu scannen. Ein Zugriff erfolgt ausschließlich, wenn Sie in der App die entsprechende Funktion auswählen.
- Mobile Daten (iOS) bzw. Zugriff auf alle Netzwerke und Netzwerkverbindungen (Android): Diese Berechtigungen ermöglichen es der App, Daten über die Internetverbindung Ihres Geräts zu übertragen. Dies kann z. B. erforderlich sein, wenn Eingaben aus der App an unsere Server gesendet werden, etwa bei einer Suche.
- Zugriff auf Gerätespeicher: Unsere App kann eine Berechtigung benötigen, um Dateien auf Ihrem Gerät zu speichern oder darauf zuzugreifen. Sowohl unter Android als auch iOS kann die App ausschließlich auf ihren eigenen app-spezifischen Speicherbereich zugreifen; ein Zugriff auf fremde Dateien oder den allgemeinen Gerätespeicher ist nicht möglich.

Widerruf: Sie können Ihre Einwilligung zur Datenverarbeitung im Rahmen der erteilten Berechtigungen jederzeit in den Einstellungen Ihres Smartphones widerrufen.

3.3 In-App-Support

Zweck: In-App-Support, Bereitstellung von Chat- und Supportfunktionen zur direkten Nutzerbetreuung innerhalb der App

Empfänger: Intercom R&D Unlimited Company, 124 St Stephen's Green, Dublin 2, DC02 C628, Irland

Verarbeitete Daten:

- Kontaktangaben (z. B. Name, E-Mail-Adresse)
- Supportanfragen und Chatinhalte (z. B. Nachrichtenverlauf, Tickets)
- Nutzungsdaten (z. B. Zeitpunkt und Häufigkeit der Supportnutzung)
- Technische Informationen (z. B. IP-Adresse, Gerätetyp)

Rechtsgrundlage: Berechtigtes Interesse an effizienter Nutzerbetreuung und Support (Art. 6 Abs. 1 lit. f DSGVO); falls Supportdaten für Vertragserfüllung erforderlich, Art. 6 Abs. 1 lit. b DSGVO

Speicherdauer: Support- und Kontaktdaten werden gelöscht, sobald sie für den jeweiligen Supportzweck nicht mehr benötigt werden oder auf Nutzeranfrage (Art. 17 DSGVO). Intercom löscht inaktive Workspace-Daten nach spätestens 13 Monaten, Chatverläufe nach 9 Monaten.

Weitere Informationen: https://www.intercom.com/legal/privacy

3.4 Zahlungsabwicklung (Hausstromrückerstattung)

Zweck: Abwicklung der Hausstromrückerstattung über einen lizenzierten Zahlungsdienstleister

Empfänger: Secupay AG, Goethestraße 6, 01896 Pulsnitz, Deutschland (BaFin-lizenziertes Zahlungsinstitut nach ZAG). Secupay ist eigenständiger Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO und verarbeitet die Daten im Rahmen eigener aufsichtsrechtlicher Pflichten.

Verarbeitete Daten:

- Empfängerdaten (Vor- und Nachname)
- Zahlungsdaten (IBAN, Auszahlungsbetrag)
- Transaktionsdaten (z. B. Zeitpunkt der Zahlung, Verwendungszweck/Referenz)

Rechtsgrundlage: Art. 6 Abs. 1 lit. b DSGVO (Vertragserfüllung); für die Verarbeitung durch Secupay zur Erfüllung aufsichts- geldwäsche- und handelsrechtlicher Pflichten Art. 6 Abs. 1 lit. C DSGVO.

Speicherdauer: Nach Auszahlung und Ablauf gesetzlicher Aufbewahrungsfristen; Secupay unterliegt eigenen Aufbewahrungspflichten nach GwG und HGB.

Weitere Informationen: https://secupay.com/datenschutz

3.5 Tracking und Analyse

Zur Verbesserung unseres Angebots und zur Analyse sowie Optimierung der App-Nutzung setzen wir verschiedene Tracking- und Analyse-Technologien ein. Hauptsächlich werden mobile Werbe-IDs wie der „Identifier for Advertisers" (IDFA) für Apple-Geräte und „Google Advertising ID" (GAID/AAID) für Android-Geräte verwendet. Diese IDs dienen der Geräteerkennung zu Analyse- und Werbezwecken. Zusätzlich integrieren wir SDKs von Drittanbietern (z. B. für Statistik, Werbung oder Fehlermeldungen), die gerätespezifische Informationen (z. B. Werbe-ID, Nutzungsverhalten, IP-Adresse sowie ggf. Standortdaten)

erfassen. Sofern diese Technologien nicht technisch unbedingt erforderlich sind, erfolgt ihre Nutzung ausschließlich auf Basis Ihrer vorherigen Einwilligung gemäß Art. 6 Abs. 1 lit. a DSGVO und § 25 Abs. 1 TDDDG. Sie können Ihre Einwilligung jederzeit in den Datenschutzeinstellungen der App oder in Ihren Geräteeinstellungen widerrufen.

3.5.1 PostHog (Analytics, Entry Tracking & Logging)

Zweck: Analyse des Nutzerverhaltens in der App zur Verbesserung von Bedienfreundlichkeit, Produktentwicklung, Fehlerbehebung und Marketingauswertung

Empfänger: PostHog, Inc., 2261 Market St., #4008, San Francisco, CA 94114, USA; Speicherung/Verarbeitung erfolgt auf Servern in der EU (Frankfurt, Deutschland)

Verarbeitete Daten:

- Nutzungsdaten (z. B. Klickpfade, Event-Tracking, Sessions, Feature-Flag-Nutzung)
- Session-Replay-Daten (Aufzeichnung von Bildschirminteraktionen)
- Fehler- und Protokolldaten (z.B. Stacktraces, Fehlermeldungen, Logs)
- Technische Informationen (z. B. Geräte-ID, Betriebssystem, Browsertyp)
- IP-Adresse (konfigurierbar verkürzt/anonymisiert)
- Individuelle Nutzer-ID oder Werbe-ID (z. B. IDFA/GAID, sofern verfügbar)

Rechtsgrundlage: Einwilligung gem. Art. 6 Abs. 1 lit. a DSGVO für Analytics/Session-Replay; berechtigtes Interesse an Qualitätssicherung und Fehlerbehebung gem. Art. 6 Abs. 1 lit. F DSGVO für Error Tracking/Logging

Speicherdauer:

- Logs: 14 Tage (Erhöhung auf 30 Tage geplant)
- Session Replay: 30 Tage
- Events und Error Tracking: 1 Jahr

Drittlandtransfer: Speicherung und Verarbeitung erfolgen in der EU (Frankfurt). Übermittlung zusätzlich über Teilnahme von PostHog am EU-U.S. Data Privacy Framework (Angemessenheitsbeschluss gem. Art. 45 DSGVO) abgesichert.

Weitere Informationen: https://posthog.com/privacy

3.5.2 Solarwinds

Zweck: IT-Monitoring, Fehlerdiagnose und Leistungsüberwachung von Netzwerken, Servern und Anwendungen zur Systemsicherheit und Optimierung der IT-Infrastruktur

Empfänger: SolarWinds Worldwide, LLC, 7171 Southwest Parkway, Bldg 400, Austin, TX 78735, USA

Verarbeitete Daten:

- System- und Netzwerkdaten (z. B. IP-Adressen, Hostnamen, Logs)
- Nutzungs- und Leistungsdaten (z. B. Antwortzeiten, Systemstatus)
- Administratorkonten und Zugriffsprotokolle (z. B. Nutzername, Anmeldezeitpunkte)
- Gegebenenfalls Kontaktinformationen technischer Ansprechpartner (z. B. Name, E-Mail-Adresse)

Rechtsgrundlage: Erfüllung des Lizenzvertrags und zur Wahrung der Sicherheit der IT-Systeme (Art. 6 Abs. 1 lit. b und f DSGVO)

Speicherdauer: Speicherung für die technisch erforderliche Dauer zum Monitoring und gemäß vertraglicher Vereinbarungen; Administrations- und Nutzungsdaten werden nach Zweckerfüllung oder auf Anfrage gelöscht

Drittlandtransfer: Übermittlung in die USA; Absicherung über das EU-U.S. Data Privacy Framework (Art. 45 DSGVO)

Weitere Informationen: https://www.solarwinds.com/legal/privacy

3.5.3 Amazon Cloud Watch

Zweck: Überwachung, Logging und Analyse von System- und Anwendungsmetriken zur Sicherstellung der Systemstabilität, Fehlerdiagnose und Optimierung der Infrastruktur

Empfänger: Amazon Web Services EMEA SARL, 38 Avenue John F. Kennedy, 1855 Luxemburg

Verarbeitete Daten:

- System- und Infrastrukturprotokolle (z. B. Applikations- und Server-Logs, Ereignisprotokolle)
- Betriebsdaten (z. B. Metriken, Statusinformationen zur Laufzeit, Ressourcenverbrauch)
- IP-Adressen (z. B. Kommunikationsprotokolle, Monitoring)
- Zugriffs- und Benutzerereignisse (z. B. Login-/Zugriffszeiten, Nutzeraktivitäten)

Rechtsgrundlage: Berechtigtes Interesse an Sicherheit, Stabilität und Fehlerprävention (Art. 6 Abs. 1 lit. f DSGVO); im Rahmen von Supportmaßnahmen oder Vertragserfüllung Art. 6 Abs. 1 lit. b DSGVO

Speicherdauer: Protokolldaten werden grundsätzlich bis zum Wegfall des Speicherzwecks aufbewahrt; standardmäßig erfolgt die Löschung nach Zweckfortfall oder spätestens nach Ablauf gesetzlicher Aufbewahrungsfristen

Drittlandtransfer: Übermittlung in die USA und andere Drittstaaten, Absicherung durch das EU-U.S. Data Privacy Framework (Art. 45 DSGVO)

Weitere Informationen: https://aws.amazon.com/de/cloudwatch/

4. Kontaktaufnahme

Wenn Sie uns per E-Mail kontaktieren, verarbeiten wir die von Ihnen angegebenen personenbezogenen Daten (z. B. Name, E-Mail-Adresse, Inhalt der Nachricht) ausschließlich zur Bearbeitung und Beantwortung Ihrer Anfrage. Rechtsgrundlage ist in der Regel unser berechtigtes Interesse an der Kommunikation mit Dir (Art. 6 Abs. 1 lit. f DSGVO) oder – sofern die Anfrage der Anbahnung oder Durchführung eines Vertrags dient – Art. 6 Abs. 1 lit. b DSGVO. Ihre Daten werden nur so lange gespeichert, wie dies zur Bearbeitung Ihrer Anfrage erforderlich ist. Eine Weitergabe an Dritte erfolgt nicht, es sei denn, wir sind gesetzlich dazu verpflichtet oder dies ist zur Bearbeitung Ihrer Anfrage unerlässlich.

5. Internationale Datenübermittlung

Wir verarbeiten Ihre Daten grundsätzlich innerhalb der EU und des EWR. Manche Dienstleister befinden sich jedoch in sog. "Drittländern". Die DSGVO stellt hierfür hohe Anforderungen. Alle Empfänger müssen diese erfüllen. Vor Übermittlung an einen Drittland-Dienstleister prüfen wir das Datenschutzniveau und wählen ausschließlich Anbieter mit nachweislich angemessenem Schutz aus. Jeder Dienstleister – auch außerhalb des EWR – hat mit uns einen Auftragsverarbeitungsvertrag geschlossen. Für Anbieter außerhalb des EWR gelten zusätzliche

Vorgaben: Nach Art. 44 ff. DSGVO dürfen Daten übermittelt werden, wenn mindestens eine der folgenden Bedingungen erfüllt ist:

- Die EU-Kommission hat ein angemessenes Datenschutzniveau festgestellt.
- Standardvertragsklauseln sind mit dem Empfänger vereinbart.
- Weitere geeignete Garantien gemäß Art. 46 DSGVO.
- In Ausnahmefällen greift eine der Ausnahmen nach Art. 49 DSGVO.

6. Empfänger von Daten

Eine Übermittlung der von uns erhobenen personenbezogenen Daten erfolgt grundsätzlich nur, wenn:

- Sie gemäß Art. 6 Abs. 1 lit. a DSGVO Ihre ausdrückliche Einwilligung erteilt haben,
- die Weitergabe gemäß Art. 6 Abs. 1 lit. f DSGVO zur Wahrung berechtigter Interessen oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist und kein Grund zur Annahme besteht, dass Ihre schutzwürdigen Interessen überwiegen,
- wir gesetzlich verpflichtet sind (Art. 6 Abs. 1 lit. c DSGVO) oder
- die Weitergabe gesetzlich zulässig und zur Vertragsdurchführung oder zur Durchführung vorvertraglicher Maßnahmen erforderlich ist (Art. 6 Abs. 1 lit. b DSGVO).

Mögliche Empfänger sind:

- Auftragsverarbeiter: Konzernunternehmen oder externe Dienstleister, z. B. im Bereich technische Infrastruktur, Verarbeitung, Wartung oder Zahlungsabwicklung. Diese dürfen Daten ausschließlich nach unseren Weisungen verwenden.
- Öffentliche Stellen: Behörden und Ämter, z. B. Finanzbehörden, Staatsanwaltschaften, Gerichte, sofern wir dazu verpflichtet sind oder berechtigte Interessen dies erfordern.

6. Datensicherheit und Schutzmaßnahmen

Wir stellen sicher, dass Ihre personenbezogenen Daten sicher und vertraulich bleiben. Zum Schutz vor Manipulation, Verlust oder Missbrauch setzen wir technische und organisatorische Maßnahmen ein, die regelmäßig überprüft und dem Stand der Technik angepasst werden.

Beachte bitte, dass andere Personen oder Institutionen auf dem Internet ggf. Datenschutzvorgaben missachten. Vor allem unverschlüsselte Daten (z. B. E-Mails) können von Dritten eingesehen werden. Darauf haben wir keinen Einfluss. Schützen Sie daher Ihre Daten durch Verschlüsselung oder vergleichbare Maßnahmen vor Missbrauch.

7. Datenspeicherung

Personenbezogene Daten werden gelöscht oder gesperrt, sobald der Zweck der Speicherung entfällt. Eine Speicherung kann darüber hinaus erfolgen, wenn dies durch europäische oder nationale Vorschriften vorgesehen ist. Daten werden außerdem gesperrt oder gelöscht, wenn eine gesetzliche Aufbewahrungsfrist abläuft, es sei denn, sie werden noch zur Vertragserfüllung benötigt.

8. Betroffenenrechte

Sie haben folgende Rechte bezüglich Ihrer personenbezogenen Daten:

- **Recht auf Auskunft:** Sie können erfahren, ob wir Ihre personenbezogenen Daten nutzen. Falls ja, haben Sie das Recht zu wissen, welche Daten das sind, warum wir sie nutzen, wer sie bekommt und wie lange wir sie aufbewahren.
- **Recht auf Berichtigung:** Sie können die unverzügliche Korrektur unrichtiger oder Vervollständigung unvollständiger Daten verlangen.
- **Recht auf Löschung:** Sie können die Löschung fordern, z. B. wenn Daten nicht mehr benötigt werden, Sie Ihre Einwilligung widerrufen oder die Nutzung unrechtmäßig war.
- **Recht auf Einschränkung der Verarbeitung:** Sie können in bestimmten Fällen die Sperrung verlangen.
- **Recht auf Datenübertragbarkeit:** Sie erhalten Ihre Daten in maschinenlesbarem Format.

Widerrufs- und Widerspruchsrecht: Sie können Ihre Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen. Die Rechtmäßigkeit der bisherigen Verarbeitung bleibt unberührt. Sie können der Nutzung Ihrer Daten für Werbezwecke jederzeit widersprechen; dies gilt auch für damit verbundenes Profiling.

Beschwerde: Sie können sich bei einer Aufsichtsbehörde beschweren, wenn Sie sich in Ihren Rechten verletzt sehen.

Änderungshistorie

Date	**Version**	Grund der Änderung
12.10.26	1.0	Erste Fassung der überarbeiteten Datenschutzhinweise im neuen Format
12.10.26	2.0	Aktualisierung der eingesetzten Dienste: Ablösung von Mixpanel und Sentry durch PostHog (Analytics/Error Tracking); Ergänzung von Expo Application Services (EAS) für Mobile Builds und OTA-Updates als Ersatz für AppZung

Privacy Policy

(Last modified: 12.10.26)

This Privacy Policy explains how personal data is processed in the Locio app (hereinafter "App") by Locio GmbH. Locio GmbH processes only such data as is necessary for the provision and security of the App, adhering to the principle of data minimization. "Personal data" means all information relating to an identified or identifiable natural person (data subject), such as name, address, telephone number, date of birth, email address, or IP address. Information that cannot be attributed to any specific person, for example due to anonymization, does not constitute personal data.

1. Controller

Use within the scope of your employment

If you use the Locio app because your employer uses Locio to process the charging transactions of your company vehicle, your employer is the controller within the meaning of Art. 4 No. 7 GDPR. In this case, Locio processes the data generated within the app (e.g. charging transactions, assignment to your company vehicle, billing information) as a processor pursuant to Art. 28 GDPR exclusively on your employer's instructions.

For the processing operations described under 3.5 ("Tracking and Analytics"), Locio acts as its own controller.

Independent / private use of the App

If you independently download and use the Locio app from the respective app store without your employer having officially introduced Locio or having asked you to use it, Locio itself is the controller for the processing of your personal data.

In this case, we provide our services directly to you (e.g. recording and evaluating your charging transactions, creating overviews/reports); processing is carried out on the basis of the user relationship existing between you and Locio.

Locio GmbH
Sandstraße 3
80335 Munich
Germany
Tel.: 089 6931900 80
Email: info(at)locio.de

For data protection inquiries or to exercise your data subject rights, please contact: datenschutz(at)locio.de.

2. Data Protection Officer

Locio has appointed the following as Data Protection Officer:

Kertos GmbH
Brienner Straße 41
80333 Munich

Germany
Email: dsb(at)kertos.io

3. Data Processing within the App

3.1 Provision and Use of the App

When downloading the app, the information required for this purpose is transmitted to the app store, in particular username, email address, customer number, time of download, payment information, and the individual device identifier. The app store also independently collects various data and provides analysis results. We have no influence over this data processing and are not responsible for it. We only process this data to the extent necessary for downloading the mobile app to your device.

3.1.1 Amazon Web Services

Recipient: Amazon Web Services EMEA SARL, 38 Avenue John F. Kennedy, L-1855 Luxembourg (Server infrastructure)

Data processed:

- Usage data (e.g. IP address, date and time of request)
- Device data (e.g. device identifier, operating system)
- Contact data (e.g. email address, mobile number)
- Network data (e.g. MAC address when using Wi-Fi)
- Identification data (e.g. unique device number IMEI, unique subscriber number IMSI)
- App Store data (e.g. username, customer number, payment information)
- Technical log data (e.g. request and response data, error messages)

Legal basis: Art. 6(1)(b) GDPR, Art. 6(1)(f) GDPR (ensuring the security and operation of the app)

Retention period: For the duration of app use and beyond in accordance with statutory retention periods

Further information: https://aws.amazon.com/privacy/

3.1.2 Mobile Builds and Over-the-Air-Updates (Expo Application Services)

Purpose: Building the mobile app and delivering over-the-air (OTA) updates, allowing app content and bug fixes to be delivered without requiring a new download from the App Store

Recipient: 650 Industries, Inc. ("Expo"), 624 University Ave, Palo Alto, CA 94301, USA

Data processed:

- Technical device data (e.g. operating systems as part of the update request)
- Randomly generated device install ID (used to determine which devices requested an update – not directly identifying per the provider)
- IP address, browser type / technical connection data

Legal basis: Legitimate interest in providing, maintaining, and updating the app (Art. 6(1)(f) GDPR); where applicable, performance of contract (Art. 6(1)(b) GDPR)

Retention period:

- EAS Build: 90 days
- EAS Update: The data is stored only for as long as necessary to provide the updates (as stated by the provider).

Third country transfer: Transfer to the USA

Further information: https://expo.dev/privacy

3.2 System Permissiones

Certain functions of our app require access to specific interfaces and data on your device. Depending on the operating system, your explicit consent may be required. Below we explain for which functions our app may request permissions (where relevant) and for what purposes. You can manage the permissions at any time in your device's system settings.

- Location services / location data: Permission to access your device's location services is required so that the app can access the location determined by your device. If you do not grant access, location-based display of content may not be possible at all or only to a limited extent.
- Notifications / push notifications: A permission is required to use push services. On some devices this is enabled by default for all apps.
- Bluetooth: The app requires access to your device's Bluetooth interface to connect to other Bluetooth-enabled devices in your vicinity or to exchange data.
- Access to stored photos: Consent is required for the app to access stored photos (read access) or to save photos generated by the app (write access).
- Camera: The app requires permission to use your device's camera, e.g. to take photos or scan QR codes. Access only occurs when you select the corresponding function within the app.
- Mobile data (iOS) / access to all networks and network connections (Android): These permissions allow the app to transmit data via your device's internet connection. This may be required, for example, when input from the app is sent to our servers, such as during a search.
- Access to device storage: Our app may require permission to save or access files on your device. Both on Android and iOS, the app can only access its own app-specific storage area; access to other files or the general device storage is not possible.

Withdrawal: You can withdraw your consent to data processing within the scope of the granted permissions at any time in your smartphone's settings.

3.3 In-App Support

Purpose: In-app support, provision of chat and support functions for direct user assistance within the app

Recipient: Intercom R&D Unlimited Company, 124 St Stephen's Green, Dublin 2, DC02 C628, Ireland

Data processed:

- Contact details (e.g. name, email address)
- Support requests and chat contents (e.g. message history, tickets)
- Usage data (e.g. time and frequency of support use)
- Technical information (e.g. IP address, device type)

Legal basis: Legitimate interest in efficient user support (Art. 6(1)(f) GDPR); if support data is required for performance of contract, Art. 6(1)(b) GDPR

Retention period: Support and contact data are deleted once no longer required for the respective support purpose or upon user request (Art. 17 GDPR). Intercom deletes inactive workspace data after a maximum of 13 months, chat histories after 9 months.

Further information: https://www.intercom.com/legal/privacy

3.4 Payment Processing (Home Electricity Reimbursement)

Purpose: Processing of the home electricity reimbursement via a licensed payment service provider

Recipient: Secupay AG, Goethestraße 6, 01896 Pulsnitz, Germany (BaFin-licensed payment institution pursuant to ZAG). Secupay is an independent controller within the meaning of Art. 4 No. 7 GDPR and processes the data in the context of its own regulatory obligations.

Data processed:

- Master data (e.g. name, address)
- Payment data (e.g. IBAN, transaction amount)
- Transaction data (e.g. timestamp, allocation to the charging session)

Legal basis: Art. 6(1)(b) GDPR (performance of contract)

Retention period: After payout and expiry of statutory retention periods; Secupay is subject to its own retention obligations under the German Anti-Money Laundering Act (GwG) and Commercial Code (HGB).

Further information: https://secupay.com/datenschutz

3.5 Tracking and Analytics

To improve our offering and to analyze and optimize app usage, we use various tracking and analytics technologies. Primarily, mobile advertising IDs are used, such as the "Identifier for Advertisers" (IDFA) for Apple devices and the "Google Advertising ID" (GAID/AAID) for Android devices. These IDs are used for device recognition for analytics and advertising purposes. We also integrate third-party SDKs (e.g. for statistics, advertising, or error reporting), which collect device-specific information (e.g. advertising ID, usage behavior, IP address, and where applicable location data). To the extent these technologies are not strictly technically necessary, their use is based exclusively on your prior consent pursuant to Art. 6(1)(a) GDPR and § 25(1) TDDDG. You can withdraw your consent at any time in the app's privacy settings or in your device settings.

3.5.1 PostHog (Analytics, Error Tracking & Logging)

Purpose: Analysis of user behavior in the app, error monitoring, session replay and logging to improve usability, product development, bug fixing and marketing evaluation

Recipient: PostHog, Inc., 2261 Market St., #4008, San Francisco, CA 94114, USA; storage/processing takes place on servers in the EU (Frankfurt, Germany)

Data processed:

- Usage data (e.g. click paths, event tracking, sessions, feature flag usage)
- Session replay data (recording of screen interactions)
- Error and log data (e.g. stack traces, error messages, logs)
- Technical information (e.g. device ID, operating system, browser type)
- IP address (configurable truncation/anonymization)
- Individual user ID or advertising ID (e.g. IDFA/GAID, where available)

Legal basis: Consent pursuant to Art. 6(1)(a) GDPR for analytics/session replay; legitimate interest in quality assurance and bug fixing pursuant to Art. 6(1) (f) GDPR for error tracking/logging

Retention period:

- Logs: 14 days (planned increase to 30 days)
- Sessions replay: 30 days
- Events and error tracking: 1 year

Third country transfer: Storage and processing take place on servers in the EU (Frankfurt, germany). Transfer is additionally safeguarded through PostHog's participation in the EU-U.S. Data Privacy Framework (adequacy decision pursuant to Art. 45 GDPR)

Further information: https://posthog.com/privacy

3.5.2 SolarWinds

Purpose: IT monitoring, fault diagnosis, and performance monitoring of networks, servers, and applications for system security and optimization of IT infrastructure

Recipient: SolarWinds Worldwide, LLC, 7171 Southwest Parkway, Bldg 400, Austin, TX 78735, USA

Data processed:

- System and network data (e.g. IP addresses, hostnames, logs)
- Usage and performance data (e.g. response times, system status)
- Administrator accounts and access logs (e.g. username, login times)
- Where applicable, contact information of technical contacts (e.g. name, email address)

Legal basis: Performance of the license agreement and to safeguard the security of IT systems (Art. 6(1)(b) and (f) GDPR)

Retention period: Stored for the technically required duration for monitoring and in accordance with contractual agreements; administration and usage data is deleted after the purpose is fulfilled or upon request

Third country transfer: Transfer to the USA; safeguarded via the EU-U.S. Data Privacy Framework (Art. 45 GDPR)

Further information: https://www.solarwinds.com/legal/privacy

3.5.3 Amazon CloudWatch

Purpose: Monitoring, logging, and analysis of system and application metrics to ensure system stability, fault diagnosis, and infrastructure optimization

Recipient: Amazon Web Services EMEA SARL, 38 Avenue John F. Kennedy, 1855 Luxembourg

Data processed:

- System and infrastructure logs (e.g. application and server logs, event logs)
- Operational data (e.g. metrics, runtime status information, resource consumption)
- IP addresses (e.g. communication logs, monitoring)
- Access and user events (e.g. login/access times, user activities)

Legal basis: Legitimate interest in security, stability, and fault prevention (Art. 6(1)(f) GDPR); in the context of support measures or performance of contract, Art. 6(1)(b) GDPR

Retention period: Log data is generally retained until the purpose for storage no longer applies; by default deletion occurs after the purpose ceases or at the latest upon expiry of statutory retention periods

Third country transfer: Transfer to the USA and other third countries, safeguarded by the EU-U.S. Data Privacy Framework (Art. 45 GDPR)

Further information: https://aws.amazon.com/cloudwatch/

4. Contact

If you contact us by email, we process the personal data you provide (e.g. name, email address, content of the message) exclusively for the purpose of processing and responding to your inquiry. The legal basis is generally our legitimate interest in communicating with you (Art. 6(1)(f) GDPR) or – if the inquiry relates to the initiation or performance of a contract – Art. 6(1)(b) GDPR. Your data will only be stored for as long as is necessary to process your inquiry. No disclosure to third parties takes place unless we are legally required to do so or this is essential for processing your inquiry.

5. International Data Transfers

We generally process your data within the EU and the EEA. However, some service providers are located in so-called "third countries". The GDPR sets high requirements for such transfers. All recipients must meet these requirements. Before transferring data to a third-country service provider, we review the level of data protection and exclusively select providers with demonstrably adequate protection. Each service provider – including those outside the EEA – has entered into a data processing agreement with us. Additional requirements apply to providers outside the EEA: Pursuant to Art. 44 et seq. GDPR, data may be transferred if at least one of the following conditions is met:

- The European Commission has determined an adequate level of data protection.

- Standard contractual clauses have been agreed with the recipient.
- Other appropriate safeguards pursuant to Art. 46 GDPR.
- In exceptional cases, one of the exceptions under Art. 49 GDPR applies.

6. Recipients of Data

Transfer of personal data collected by us generally only takes place if:

- You have given your explicit consent pursuant to Art. 6(1)(a) GDPR,
- Disclosure is necessary pursuant to Art. 6(1)(f) GDPR to protect legitimate interests or to assert, exercise, or defend legal claims and there is no reason to assume that your overriding interests in protection prevail,
- We are legally obligated to do so (Art. 6(1)(c) GDPR), or
- The disclosure is legally permissible and necessary for the performance of a contract or for the implementation of pre-contractual measures (Art. 6(1)(b) GDPR).

Possible recipients are:

Processors: Group companies or external service providers, e.g. in the areas of technical infrastructure, processing, maintenance, or payment processing. These may use data exclusively according to our instructions.

Public authorities: Authorities and offices, e.g. tax authorities, public prosecutors, courts, where we are obligated to do so or where legitimate interests require it.

7. Data Security and Protective Measures

We ensure that your personal data remains secure and confidential. To protect against manipulation, loss, or misuse, we implement technical and organizational measures that are regularly reviewed and adapted to the state of the art.

Please note that other persons or institutions on the internet may disregard data protection requirements. In particular, unencrypted data (e.g. emails) can be accessed by third parties. We have no influence over this. Therefore, protect your data from misuse through encryption or comparable measures.

8. Data Retention

Personal data is deleted or blocked as soon as the purpose of storage no longer applies. Storage may also take place if this is provided for by European or national regulations. Data is also blocked or deleted when a statutory retention period expires, unless it is still required for the performance of a contract.

9. Data Subject Rights

You have the following rights with regard to your personal data:

- **Right of access:** You can find out whether we use your personal data. If so, you have the right to know what data this is, why we use it, who receives it, and how long we retain it.
- **Right to rectification**: You can demand the immediate correction of inaccurate data or the completion of incomplete data.

- **Right to erasure**: You can demand deletion, e.g. if data is no longer required, you withdraw your consent, or the processing was unlawful.
- **Right to restriction of processing**: In certain cases, you can demand that processing be restricted.
- **Right to data portability**: You will receive your data in a machine-readable format.
- **Right of withdrawal and right to object**: You can withdraw your consent at any time with effect for the future. The lawfulness of processing carried out prior to withdrawal remains unaffected. You can object to the use of your data for advertising purposes at any time; this also applies to related profiling.
- **Right to lodge a complaint**: You can lodge a complaint with a supervisory authority if you believe your rights have been violated.

Change History

Date	Version	Reason for Change
23.09.2026	1.0	First version of the revised privacy policy in the new format
12.10.2026	2.0	Update of services used: replacement of Mixpanel and Sentry with PostHog (analytics/error tracking); addition of Expo Application Services (EAS) for mobile builds and OTA updates, replacing AppZung