

PRIVACY POLICY

Cutters AI Platform — Powered by Lifiot UG (haftungsbeschränkt)

Effective Date: April 14, 2026 | Version 2.0 | English Version

AT A GLANCE

Who: Lifiot UG (haftungsbeschränkt), Luisenstr. 7, 78048 Villingen-Schwenningen, Germany — acts as data controller for account, billing, and marketing data, and as data processor for customer IoT and uploaded-file data.

What: Account details, IoT telemetry, GPS location, platform usage data, uploaded files, and marketing consent.

Why: To deliver the Cutters AI platform, manage subscriptions, monitor IoT-connected assets on behalf of customers, and send marketing communications where consented.

Your rights: Access, rectification, erasure, portability, restriction, objection, and the right to complain to the LfDI Baden-Württemberg.

Contact: info@lifiot.com — Full details in Sections 1–18 below.

Note on language: This document is provided in English and German. For customers domiciled in Germany, Austria, or Switzerland (DACH region), the German version below is the authoritative version. For all other customers, the English version governs. In case of conflict between the two versions, the German version prevails for DACH customers.

1. Identity of the Data Controller

The data controller responsible for the processing of your personal data in connection with the Cutters AI platform is:

Lifiot UG (haftungsbeschränkt)

Luisenstr. 7, 78048 Villingen-Schwenningen, Germany

HRB 728690, Amtsgericht Freiburg im Breisgau

USt-IdNr.: DE361451350

Email: info@lifiot.com

Website: www.lifiot.com

DPO NOTE: Lifiot UG (haftungsbeschränkt) is currently assessing its obligation to appoint a Data Protection Officer pursuant to GDPR Art. 37 and BDSG §38 as its processing activities scale. The mandatory threshold under BDSG §38(1) (20+ employees regularly processing personal data) is not currently met. We will appoint a DPO as required by law as customer volume grows. For all data protection enquiries in the interim, please contact: info@lifiot.com

2. Scope of This Privacy Policy

This Privacy Policy explains how Lifiot UG (haftungsbeschränkt) ("we", "us", "our") processes personal data in connection with the Cutters AI software-as-a-service platform and all associated IoT device integrations (collectively, the "Platform"). It covers:

- Sections 3–5: Data processing when you visit and use the Platform
- Section 6: Data processing in the context of the B2B customer relationship
- Section 7: IoT device data — including the controller/processor framework
- Section 8: Employee and operator data linked to assets
- Section 9: File and document uploads
- Section 10: Marketing communications
- Section 11: Sub-processors and data recipients
- Sections 12–17: Your rights, retention, security, and legal bases

This Policy does not establish contractual rights or obligations. For the contractual relationship governing use of the Platform, please refer to our Terms of Service.

***ROLES OVERVIEW:** Lifiot UG (haftungsbeschränkt) acts as DATA CONTROLLER for: website and platform access data, account and identity data, billing and contract data, customer analytics, and marketing communications. Lifiot acts as DATA PROCESSOR for: customer-managed IoT device telemetry, employee/operator assignment data, and files uploaded by customers — all processed solely on the customer's instructions under a Data Processing Agreement (DPA). This distinction is explained further in Sections 7, 8, and 9.*

3. What Is Personal Data?

Personal data is any information relating to an identified or identifiable natural person (e.g. name, email address, IP address, location data, device identifiers). This Policy applies to all personal data we process, regardless of the medium or format in which it is held.

4. Categories of Personal Data We Collect

4.1 Account and Identity Data

When you register and use the Platform as a business customer, we collect:

- Full name, job title, and professional email address of account administrators and platform users.
- Company name, registered address, business license number, and VAT identification number.
- Login credentials (passwords stored exclusively in hashed, salted form — never in plain text).
- Billing contact details and correspondence records.

4.2 Platform Usage and Technical Data

We automatically collect technical data when the Platform is accessed:

- IP address, browser type and version, operating system, and device type.
- Pages visited, features used, session duration, and interaction events within the application.

- Error logs and performance diagnostics used to maintain and improve the Platform.

Provision requirement — account and identity data: Providing this data is a contractual requirement. Without name, email, and company details, we cannot create your account or manage your subscription. There is no legal obligation to provide this data, but without it use of the Platform is not possible.

Legal basis: Art. 6(1)(f) GDPR — Art. 6(1)(b) GDPR (contract performance) for core technical data necessary to deliver the Platform service (IP address, session data, page routing). Art. 6(1)(f) GDPR — our legitimate interests of detecting and preventing unauthorised access, cyberattacks, and service disruption for log files, error diagnostics, and performance analytics.

4.3 IoT Device and Equipment Telemetry Data

When IoT-enabled assets ("Connected Devices") are registered to the Platform, the following machine-generated data is collected. Connected Devices may include, but are not limited to, power tools, heavy construction equipment (e.g. excavators, drilling rigs), vehicles, site machinery, and any other asset to which an IoT sensor or beacon has been attached by the customer:

- Device identifiers, hardware serial numbers, firmware versions, and connection status.
- Sensor telemetry and operational data generated by Connected Devices, which may include performance metrics, equipment status readings, and usage data, the specific parameters of which depend on the type and configuration of the Connected Device.
- GPS coordinates and location data of Connected Devices during active operational sessions.
- Operational timestamps, session durations, utilization hours, and equipment run cycles.
- Fault codes, maintenance alerts, and predictive maintenance indicators.

Provision requirement — platform usage and technical data: This data is collected automatically when you use the Platform. Providing it is technically necessary for the service to function. You are not separately asked to supply it; however, use of the Platform implies this collection occurs.

Legal basis: Art. 6(1)(b) GDPR (performance of contract) for core telemetry; Art. 6(1)(a) GDPR (consent) for optional device-level access subject to TDDG §25 requirements.

4.4 Location and GPS Data

GPS location data is collected from Connected Devices during active job sessions for asset tracking and project management. Mobile app location data is collected only where the user has explicitly granted location permissions. Mobile users may disable location tracking at any time in device settings without affecting core Platform functionality.

Provision requirement — IoT telemetry: Providing IoT telemetry data is contractually required to use the equipment monitoring features of the Platform. Without it, asset tracking, predictive maintenance, and related features cannot be delivered. Use of the Platform for project management only remains possible without connecting IoT devices.

Legal basis: Art. 6(1)(b) GDPR for device GPS; Art. 6(1)(a) GDPR (consent) for mobile app location.

Provision requirement — location and GPS data: Device GPS data is contractually required when using Connected Devices with the Platform. Mobile app location is entirely voluntary — you may deny or revoke location permissions at any time in your device settings without affecting core Platform access.

4.5 File and Document Uploads

The Platform allows customers to upload files including documents, photographs, and PDFs. Uploaded files are stored on our infrastructure and may contain personal data depending on their content. Customers are responsible for ensuring any personal data in uploaded files is processed lawfully.

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

Provision requirement — file uploads: Uploading files is entirely voluntary. You are not required to upload documents, photographs, or PDFs to use the Platform. If you upload files containing personal data, you do so as Data Controller and bear sole responsibility for that data.

5. Data Processing When Visiting the Platform

5.1 Display of the Platform

To display the Platform, we process: URL of requested function, IP address, and browser details. Standard access logs are retained for up to 12 months for security purposes.

Legal basis: Art. 6(1)(f) GDPR — our legitimate interest in ensuring the security of the Platform against unauthorised access, manipulation, and service disruption.

5.2 Cookies and Tracking Technologies

We use strictly necessary cookies for session management and authentication only. No advertising or cross-site tracking cookies are used. We do not currently use analytics cookies. If we introduce analytics cookies in future, we will update this Policy and obtain your prior consent before doing so. Any such cookies will be manageable via the cookie settings panel in the Platform.

6. Data Processing in the Customer Business Relationship

6.1 Initiation and Management of the Business Relationship

We process contact persons' data (name, professional email, job title, phone number) for managing the customer relationship.

Legal basis: Art. 6(1)(b) GDPR (contract performance); Art. 6(1)(f) GDPR — our legitimate interest in managing and developing the B2B customer relationship, communicating effectively with customer contacts, and maintaining business continuity. Retention: duration of contract + 3 years, or 5 years from last contact for prospects.

6.2 Customer Analytics

We process basic customer data for internal business analysis to understand and improve our services.

Legal basis: Art. 6(1)(f) GDPR — our legitimate interest in understanding our customer base, identifying patterns in service adoption, and making informed product development decisions. Retention: 5 years from last contact.

6.3 Invoicing and Accounting

We process billing details for invoicing and financial record-keeping using our internal CRM — no third-party CRM receives your data.

Legal basis: Art. 6(1)(c) GDPR (legal obligation). Retention: 10 years (§ 257 HGB, § 147 AO).

6.4 Automated Decision-Making

No decision producing legal effects is made solely on the basis of automated processing within the meaning of Art. 22 GDPR. AI-generated insights are informational only and do not constitute automated decisions under Art. 22 GDPR.

7. IoT Data — Controller and Processor Framework

7.1 Who Is the Data Controller for IoT Data?

The customer (diamond contractor, OEM supplier, or other business) connecting equipment to the Platform is the Data Controller. Lifiot UG (haftungsbeschränkt) acts as Data Processor, processing IoT data solely on the customer's instructions under a GDPR Art. 28 Data Processing Agreement (DPA).

7.2 Customer Obligations as Data Controller

Customers are responsible for: having a valid legal basis for IoT telemetry collection; informing their employees about equipment monitoring (see Section 8); complying with applicable data protection laws in their jurisdiction; and only registering devices they have the right to monitor.

7.3 EU Data Act — User Rights Over Equipment Data

The EU Data Act (Regulation (EU) 2023/2854, applicable from 12 September 2025) grants users of Connected Devices rights over the data their equipment generates, including rights of access, portability, and third-party sharing on fair terms. Full details of these rights and our obligations under the EU Data Act are set out in our Terms of Service. For EU Data Act requests: info@lifiot.com.

7.4 TDDDG — IoT Device Access (Germany)

Where Germany's TDDDG (Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz, formerly TTDSG, renamed 14 May 2024) applies, access to device-stored data requires explicit consent (provided during device onboarding) or a recognized legal exemption. Consent can be managed in Platform account settings at any time.

8. Employee and Operator Data Linked to Assets

Where a customer optionally assigns an employee or operator to a specific asset in the Platform, the associated telemetry and GPS data constitutes personal data. Lifiot UG (haftungsbeschränkt) processes this data as Data Processor on the customer's instructions. In accordance with GDPR Article 14 (data not obtained directly from the data subject): where Lifiot receives personal data about employees or operators that was not provided directly by those individuals, the source of that data is the customer organisation (the employer or contracting entity) using the Platform. The categories of data received from this source may

include: name, employee identifier, job role, and any other fields populated by the customer when making an asset assignment.

IMPORTANT FOR CUSTOMERS: *Before assigning employees to assets, you must ensure your employees have received appropriate notice about equipment monitoring, consistent with your obligations as an employer under GDPR and applicable national employment law (e.g. Betriebsvereinbarung in Germany).*

9. File and Document Upload Processing

- Files are stored on AWS infrastructure within the EEA (Frankfurt or Ireland).
- We do not analyse or extract personal data from uploaded files beyond what is necessary for storage and retrieval.
- Customers are the Data Controller for personal data in uploaded files.
- Upon termination, files are available for export for 90 days, then permanently deleted.

10. Marketing Communications

With your explicit consent (Art. 6(1)(a) GDPR), we send marketing emails about Platform features and updates. You may withdraw consent at any time by clicking the unsubscribe link or contacting info@lifiot.com. Marketing emails are sent directly from our own accounts — no third-party email platform receives your data. Provision requirement — marketing communications: Providing consent for marketing emails is entirely voluntary. Refusing or withdrawing consent has no consequences for your Platform access or subscription.

11. Sub-Processors and Data Recipients

11.1 Sub-Processor Table

Recipient	Purpose	Data categories	Legal basis	Country	Transfer basis
Amazon Web Services EMEA SARL	Cloud infrastructure & file storage	All Platform data incl. IoT telemetry, GPS, files	Art. 6(1)(b) GDPR	Germany / Ireland (EEA)	EEA — no transfer mechanism required
Lifiot UG internal CRM	Customer relationship management	Name, email, company, subscription data	Art. 6(1)(b)/(f) GDPR	Germany (EEA)	EEA — no transfer mechanism required
Stripe, Inc.	Online payment processing	Name, email, billing address, payment data	Art. 6(1)(b) GDPR	USA	EU-US Data Privacy Framework + SCCs Art. 46(2)(c) GDPR

The sub-processors listed above reflect our current engagements. As our platform evolves, sub-processors may be added, replaced, or removed. We maintain an up-to-date list of sub-processors and will notify customers of material changes with reasonable advance notice, during which customers may raise legitimate objections. The current list is always available at www.lifiot.com/subprocessors.

11.2 Legal Disclosures

We may disclose personal data where required by applicable law or binding court order. We implement measures to resist non-EEA governmental access to non-personal data without a valid EU legal basis.

11.3 Aggregated Data

Fully anonymized, aggregated industry statistics may be used for product development. This data cannot be traced back to any individual customer.

12. International Data Transfers

Platform data is primarily hosted on AWS infrastructure within the EEA (Frankfurt, Germany or Dublin, Ireland). We have selected EEA-based regions as our primary hosting environment to minimise third-country transfers. Where incidental access to platform data from third countries occurs — for example, in the context of technical support, development, or security operations — we ensure appropriate safeguards are in place, including Standard Contractual Clauses (SCCs) pursuant to Art. 46(2)(c) GDPR. The primary identified third-country transfer is payment processing via Stripe, Inc. (USA), governed by the EU-US Data Privacy Framework and SCCs.

13. Data Retention Periods

Data category	Retention period	Purpose	Legal basis
Account and user data	Contract duration + 3 years	Legal compliance, disputes	§ 195 BGB
IoT telemetry and GPS data	Contract duration + 90 days	Customer export period	Contract performance
Uploaded files	Contract duration + 90 days	Customer export period	Contract performance
Platform access logs	12 months	Security incident detection	Legitimate interest
Billing and invoice records	10 years	German commercial/tax law	§ 257 HGB, § 147 AO
Marketing consent records	Until withdrawn + 3 years	Proof of consent	Art. 7(1) GDPR
Legal claims data	Up to 30 years	Assertion/defense of claims	Art. 6(1)(f) GDPR

14. Your Rights Under GDPR

You have the right to lodge a complaint with a supervisory authority at any time, in particular in the EU member state of your habitual residence, place of work, or place of the alleged infringement. To exercise any of your other rights, contact info@lifiot.com. We will respond within 30 days.

- Right of Access (Art. 15 GDPR): Obtain a copy of personal data we hold about you.
- Right to Rectification (Art. 16 GDPR): Request correction of inaccurate data.
- Right to Erasure (Art. 17 GDPR): Request deletion subject to legal retention obligations.
- Right to Restriction (Art. 18 GDPR): Request restricted processing in specific circumstances.
- Right to Data Portability (Art. 20 GDPR): Receive your data in machine-readable format (JSON or CSV).
- Right to Object (Art. 21 GDPR): Object to processing based on legitimate interests.
- Right to Withdraw Consent (Art. 7(3) GDPR): Withdraw consent at any time without affecting prior processing.
- Right re Automated Decisions (Art. 22 GDPR): Not to be subject to solely automated decisions with legal effects. We make no such decisions.

Competent supervisory authority:

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg (LfDI BW)

Lautenschlagerstraße 20, 70173 Stuttgart — www.baden-wuerttemberg.datenschutz.de

15. Data Security

- AES-256 encryption at rest and TLS 1.3 in transit on AWS infrastructure.
- Role-based access controls (RBAC) restricting data access to authorised personnel.
- Regular security assessments, vulnerability scanning, and penetration testing.
- Documented incident response procedures: personal data breaches are assessed and handled in accordance with GDPR Art. 33, including notification to the LfDI BW where legally required.
- AWS infrastructure: SOC 2 Type II, ISO/IEC 27001, ISO/IEC 27017 certified.

16. Processing for Legal Claims

We process personal data for asserting, exercising, or defending legal claims on the basis of Art. 6(1)(f) GDPR — our legitimate interest in enforcing contractual rights, defending against unfounded claims, and complying with court orders and regulatory requirements. Data may be retained for up to 30 years following the end of the business relationship where legally necessary.

17. Changes to This Privacy Policy

We will provide at least 30 days' notice of material changes via email or in-Platform notification. The current version is always available at www.lifiot.com/privacy.

18. Contact

Lifiot UG (haftungsbeschränkt)

Luisenstr. 7, 78048 Villingen-Schwenningen, Germany

HRB 728690 | USt-IdNr.: DE361451350

Email: info@lifiot.com | Website: www.lifiot.com/privacy

Supervisory authority: LfDI Baden-Württemberg — www.baden-wuerttemberg.datenschutz.de

DATENSCHUTZERKLÄRUNG

Cutters AI Plattform — Betrieben von Lifiot UG (haftungsbeschränkt)

Gültig ab: 14. April 2026 | Version 2.0 | Deutsche Fassung (maßgeblich für DACH)

AUF EINEN BLICK

Wer: Lifiot UG (haftungsbeschränkt), Luisenstr. 7, 78048 Villingen-Schwenningen — handelt als Verantwortlicher für Konto-, Rechnungs- und Marketingdaten sowie als Auftragsverarbeiter für IoT- und hochgeladene Kundendaten.

Was: Kontodaten, IoT-Telemetrie, GPS-Standort, Plattformnutzungsdaten, hochgeladene Dateien und Marketingeinwilligungen.

Warum: Zur Bereitstellung der Cutters AI Plattform, Verwaltung von Abonnements, IoT-Geräteüberwachung im Auftrag von Kunden sowie zum Versand von Marketingkommunikation mit Einwilligung.

Ihre Rechte: Auskunft, Berichtigung, Löschung, Datenübertragbarkeit, Einschränkung, Widerspruch sowie das Recht zur Beschwerde beim LfDI Baden-Württemberg.

Kontakt: info@lifiot.com — Vollständige Einzelheiten in den Abschnitten 1–18 unten.

Hinweis zur Sprache: Dieses Dokument wird auf Englisch und Deutsch bereitgestellt. Für Kunden mit Sitz in Deutschland, Österreich oder der Schweiz (DACH-Region) ist die deutsche Fassung die maßgebliche Version. Im Falle von Widersprüchen zwischen den beiden Sprachversionen gilt für DACH-Kunden die deutsche Fassung.

1. Verantwortlicher

Verantwortlicher im Sinne der Datenschutz-Grundverordnung (DSGVO) und des Bundesdatenschutzgesetzes (BDSG) für die Verarbeitung Ihrer personenbezogenen Daten im Zusammenhang mit der Cutters AI Plattform ist:

Lifiot UG (haftungsbeschränkt)

Luisenstr. 7, 78048 Villingen-Schwenningen, Deutschland

HRB 728690, Amtsgericht Freiburg im Breisgau

USt-IdNr.: DE361451350

E-Mail: info@lifiot.com

Website: www.lifiot.com

HINWEIS ZUM DATENSCHUTZBEAUFTRAGTEN: Die Lifiot UG (haftungsbeschränkt) prüft derzeit, ob gemäß Art. 37 DSGVO und § 38 BDSG eine Pflicht zur Bestellung eines Datenschutzbeauftragten besteht. Der Schwellenwert des § 38 Abs. 1 BDSG (mindestens 20 ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigte

Personen) ist derzeit nicht erreicht. Sobald dies gesetzlich erforderlich ist, wird ein Datenschutzbeauftragter bestellt. Für alle datenschutzbezogenen Anfragen wenden Sie sich bitte an: info@lifiot.com

2. Geltungsbereich dieser Datenschutzerklärung

Diese Datenschutzerklärung erläutert, wie die Lifiot UG (haftungsbeschränkt) ("wir", "uns", "unser") personenbezogene Daten im Zusammenhang mit der Cutters AI Software-as-a-Service-Plattform und allen zugehörigen IoT-Geräteintegrationen (zusammen die "Plattform") verarbeitet. Sie umfasst:

- Abschnitte 3–5: Datenverarbeitung beim Besuch und der Nutzung der Plattform
- Abschnitt 6: Datenverarbeitung im Rahmen der B2B-Kundenbeziehung
- Abschnitt 7: IoT-Gerätedaten — einschließlich des Verantwortlichen/Auftragsverarbeiter-Rahmens
- Abschnitt 8: Mitarbeiter- und Bediener-Daten in Verbindung mit Geräten
- Abschnitt 9: Datei- und Dokumenten-Uploads
- Abschnitt 10: Marketingkommunikation
- Abschnitt 11: Auftragsverarbeiter und Datenempfänger
- Abschnitte 12–17: Ihre Rechte, Speicherfristen, Sicherheit und Rechtsgrundlagen

Diese Erklärung begründet keine vertraglichen Rechte oder Pflichten. Für das Vertragsverhältnis zur Nutzung der Plattform verweisen wir auf unsere Allgemeinen Geschäftsbedingungen.

***ROLLENÜBERSICHT:** Die Lifiot UG (haftungsbeschränkt) handelt als VERANTWORTLICHER für: Website- und Plattformzugriffsdaten, Konto- und Identifikationsdaten, Rechnungs- und Vertragsdaten, Kundenanalysen und Marketingkommunikation. Lifiot handelt als AUFTRAGSVERARBEITER für: vom Kunden verwaltete IoT-Geräte telemetrie, Mitarbeiter- und Bediener-Zuweisungsdaten sowie vom Kunden hochgeladene Dateien — all diese werden ausschließlich auf Weisung des Kunden im Rahmen eines Auftragsverarbeitungsvertrags (AVV) verarbeitet. Diese Unterscheidung wird in den Abschnitten 7, 8 und 9 näher erläutert.*

3. Was sind personenbezogene Daten?

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (z. B. Name, E-Mail-Adresse, IP-Adresse, Standortdaten, Gerätekennungen). Diese Erklärung gilt für alle personenbezogenen Daten, die wir verarbeiten, unabhängig vom Medium oder Format.

4. Kategorien der von uns verarbeiteten personenbezogenen Daten

4.1 Konto- und Identifikationsdaten

Bei der Registrierung und Nutzung der Plattform als Geschäftskunde erheben wir:

- Vollständiger Name, Berufsbezeichnung und berufliche E-Mail-Adresse von Kontoadministratoren und Plattformnutzern.
- Firmenname, eingetragene Adresse, Gewerbeschein-Nummer und Umsatzsteuer-Identifikationsnummer.
- Anmeldedaten (Passwörter werden ausschließlich in gehashter, gesalzener Form gespeichert — niemals im Klartext).
- Rechnungskontaktdaten und Korrespondenzunterlagen.

4.2 Plattformnutzungs- und technische Daten

Beim Zugriff auf die Plattform erheben wir automatisch technische Daten:

- IP-Adresse, Browsertyp und -version, Betriebssystem und Gerätetyp.
- Besuchte Seiten, genutzte Funktionen, Sitzungsdauer und Interaktionsereignisse innerhalb der Anwendung.
- Fehlerprotokolle und Leistungsdiagnosen zur Wartung und Verbesserung der Plattform.

Angabepflicht — Konto- und Identifikationsdaten: Die Angabe dieser Daten ist vertraglich erforderlich. Ohne Name, E-Mail-Adresse und Unternehmensdaten können wir kein Konto erstellen oder Ihr Abonnement verwalten. Es besteht keine gesetzliche Pflicht zur Angabe, jedoch ist ohne diese Daten eine Nutzung der Plattform nicht möglich.

Rechtsgrundlage: Art. 6 Abs. 1 lit. f DSGVO — Art. 6 Abs. 1 lit. b DSGVO (Vertragserfüllung) für technische Kerndaten, die zur Erbringung der Plattformleistung erforderlich sind (IP-Adresse, Sitzungsdaten, Seitenweiterleitung). Art. 6 Abs. 1 lit. f DSGVO — unsere berechtigten Interessen an der Erkennung und Verhinderung von unbefugtem Zugriff, Cyberangriffen und Dienstunterbrechungen für Protokolldateien, Fehlerdiagnosen und Leistungsanalysen.

4.3 IoT-Gerätedaten und Anlagentelemetrie

Wenn IoT-fähige Anlagen ("Verbundene Geräte") auf der Plattform registriert werden, werden folgende maschinengenerierte Daten erhoben. Verbundene Geräte können unter anderem Elektrowerkzeuge, schwere Baumaschinen (z. B. Bagger, Bohrgeräte), Fahrzeuge, Baustellenmaschinen sowie sonstige Anlagen umfassen, an denen der Kunde einen IoT-Sensor oder Beacon angebracht hat:

- Gerätekennungen, Hardware-Seriennummern, Firmware-Versionen und Verbindungsstatus.
- Sensortelemetrie und Betriebsdaten der Verbundenen Geräte, einschließlich Leistungskennzahlen, Gerätestatus und Nutzungsdaten, wobei die konkreten Parameter vom Typ und der Konfiguration des jeweiligen Verbundenen Geräts abhängen.
- GPS-Koordinaten und Standortdaten der Verbundenen Geräte während aktiver Betriebssitzungen.
- Betriebszeitstempel, Sitzungsdauern, Betriebsstunden und Gerätebetriebszyklen.
- Fehlercodes, Wartungsalarme und Indikatoren für vorausschauende Wartung.

Angabepflicht — Plattformnutzungs- und technische Daten: Diese Daten werden automatisch bei der Nutzung der Plattform erhoben. Die Erhebung ist technisch notwendig für den Betrieb des Dienstes. Sie werden nicht gesondert zur Angabe aufgefordert; die Nutzung der Plattform setzt diese Erhebung jedoch voraus.

Rechtsgrundlage: Art. 6 Abs. 1 lit. b DSGVO (Vertragserfüllung) für die Kerntelemetrie; Art. 6 Abs. 1 lit. a DSGVO (Einwilligung) für optionalen Gerätezugriff gemäß § 25 TDDDG.

4.4 Standort- und GPS-Daten

GPS-Standortdaten werden von Verbundenen Geräten während aktiver Arbeitssitzungen zur Anlagenverfolgung und Projektverwaltung erhoben. Standortdaten aus mobilen Apps werden nur erhoben, wenn der Nutzer ausdrücklich die Standortberechtigung erteilt hat. Mobilnutzer können die Standortverfolgung jederzeit in den Geräteeinstellungen deaktivieren.

Angabepflicht — IoT-Telemetrie: Die Bereitstellung von IoT-Telemetriedaten ist vertraglich erforderlich, um die Geräteüberwachungsfunktionen der Plattform zu nutzen. Ohne diese Daten können Anlagenverfolgung, vorausschauende Wartung und verwandte Funktionen nicht erbracht werden. Eine Nutzung der Plattform ausschließlich für das Projektmanagement ist ohne Anschluss von IoT-Geräten weiterhin möglich.

Rechtsgrundlage: Art. 6 Abs. 1 lit. b DSGVO für Geräte-GPS; Art. 6 Abs. 1 lit. a DSGVO (Einwilligung) für mobilen App-Standort.

Angabepflicht — Standort- und GPS-Daten: Die Erhebung von Geräte-GPS-Daten ist vertraglich erforderlich, wenn Verbundene Geräte mit der Plattform genutzt werden. Der Standort in der mobilen App ist vollständig freiwillig — Sie können Standortberechtigungen jederzeit in den Geräteeinstellungen verweigern oder widerrufen, ohne dass der Kernzugang zur Plattform beeinträchtigt wird.

4.5 Datei- und Dokumenten-Uploads

Die Plattform ermöglicht Kunden das Hochladen von Dateien, darunter Dokumente, Fotos und PDFs. Hochgeladene Dateien werden auf unserer Infrastruktur gespeichert und können je nach Inhalt personenbezogene Daten enthalten. Kunden sind dafür verantwortlich, dass personenbezogene Daten in hochgeladenen Dateien rechtmäßig verarbeitet werden.

Rechtsgrundlage: Art. 6 Abs. 1 lit. b DSGVO (Vertragserfüllung).

Angabepflicht — Datei-Uploads: Das Hochladen von Dateien ist vollständig freiwillig. Sie sind nicht verpflichtet, Dokumente, Fotos oder PDFs hochzuladen, um die Plattform zu nutzen. Wenn Sie Dateien mit personenbezogenen Daten hochladen, handeln Sie als Verantwortlicher und tragen die alleinige Verantwortung für diese Daten.

5. Datenverarbeitung beim Besuch der Plattform

5.1 Darstellung der Plattform

Zur Darstellung der Plattform verarbeiten wir: URL der aufgerufenen Funktion, IP-Adresse und Browserdetails. Standard-Zugangsprotokolle werden bis zu 12 Monate lang für Sicherheitszwecke aufbewahrt.

Rechtsgrundlage: Art. 6 Abs. 1 lit. f DSGVO — unser berechtigtes Interesse an der Sicherheit der Plattform gegen unbefugten Zugriff, Manipulation und Dienstunterbrechungen.

5.2 Cookies und Tracking-Technologien

Wir verwenden ausschließlich technisch notwendige Cookies für die Sitzungsverwaltung und Authentifizierung. Es werden keine Werbe- oder seitenübergreifenden Tracking-Cookies eingesetzt. Wir verwenden derzeit keine Analyse-Cookies. Sollten wir in Zukunft Analyse-Cookies einführen, werden wir diese Richtlinie aktualisieren und vorab Ihre Einwilligung einholen. Solche Cookies können über das Cookie-Einstellungsfeld in der Plattform verwaltet werden.

6. Datenverarbeitung in der Kundengeschäftsbeziehung

6.1 Anbahnung und Verwaltung der Geschäftsbeziehung

Wir verarbeiten Daten von Kontaktpersonen (Name, berufliche E-Mail, Berufsbezeichnung, Telefonnummer) zur Verwaltung der Kundenbeziehung.

Rechtsgrundlage: Art. 6 Abs. 1 lit. b DSGVO (Vertragserfüllung); Art. 6 Abs. 1 lit. f DSGVO — unser berechtigtes Interesse an der Pflege und Entwicklung der B2B-Kundenbeziehung, der effektiven Kommunikation mit Kundenkontakten und der Sicherstellung der Geschäftskontinuität. Speicherdauer: Vertragsdauer + 3 Jahre, bzw. 5 Jahre ab letztem Kontakt für Interessenten.

6.2 Kundenanalyse

Wir verarbeiten grundlegende Kundendaten für interne Geschäftsanalysen zur Verbesserung unserer Dienstleistungen.

Rechtsgrundlage: Art. 6 Abs. 1 lit. f DSGVO — unser berechtigtes Interesse daran, unseren Kundenstamm zu verstehen, Muster bei der Dienstleistungsnutzung zu erkennen und fundierte Produktentwicklungsentscheidungen zu treffen. Speicherdauer: 5 Jahre ab letztem Kontakt.

6.3 Rechnungsstellung und Buchhaltung

Wir verarbeiten Rechnungsdaten für die Rechnungsstellung und Buchführung in unserem internen CRM-System — kein Drittanbieter-CRM erhält Ihre Daten.

Rechtsgrundlage: Art. 6 Abs. 1 lit. c DSGVO (gesetzliche Verpflichtung). Speicherdauer: 10 Jahre (§ 257 HGB, § 147 AO).

6.4 Automatisierte Entscheidungsfindung

Es wird keine Entscheidung, die rechtliche Wirkung entfaltet oder Sie in ähnlicher Weise erheblich beeinträchtigt, ausschließlich auf Basis automatisierter Verarbeitung im Sinne von Art. 22 DSGVO getroffen. KI-generierte Einblicke dienen ausschließlich der Information und stellen keine automatisierten Entscheidungen im Sinne von Art. 22 DSGVO dar.

7. IoT-Daten — Verantwortlicher und Auftragsverarbeiter

7.1 Wer ist für IoT-Daten verantwortlich?

Der Kunde (Auftragnehmer, OEM-Lieferant oder sonstiger Gewerbetreibender), der Anlagen auf der Plattform verbindet, ist der Verantwortliche. Die Lifiot UG (haftungsbeschränkt) handelt als Auftragsverarbeiter und verarbeitet IoT-Daten ausschließlich auf Weisung des Kunden im Rahmen eines Auftragsverarbeitungsvertrags (AVV) gemäß Art. 28 DSGVO.

7.2 Pflichten des Kunden als Verantwortlicher

Kunden sind verantwortlich für: das Vorliegen einer Rechtsgrundlage für die IoT-Telemetrieerhebung; die Unterrichtung ihrer Mitarbeiter über die Geräteüberwachung (siehe Abschnitt 8); die Einhaltung des anwendbaren Datenschutzrechts; sowie die ausschließliche Registrierung von Geräten, für die ein Überwachungsrecht besteht.

7.3 EU-Datengesetz — Nutzerrechte an Gerätedaten

Das EU-Datengesetz (Verordnung (EU) 2023/2854, anwendbar ab 12. September 2025) gewährt Nutzern Verbundener Geräte Rechte an den von ihren Anlagen generierten Daten, einschließlich Zugangs-, Portabilitäts- und Weitergaberechte zu fairen Bedingungen. Die vollständigen Einzelheiten dieser Rechte und unserer Pflichten gemäß dem EU-Datengesetz sind in unseren Allgemeinen Geschäftsbedingungen dargelegt. Für Anfragen zum EU-Datengesetz: info@lifiot.com.

7.4 TDDDG — IoT-Gerätezugriff

Soweit das Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG, ehemals TTDSG, umbenannt am 14. Mai 2024) Anwendung findet, bedarf der Zugriff auf geräteseitig gespeicherte Daten gemäß § 25 TDDDG einer ausdrücklichen Einwilligung (erteilt während der Gerätekonfiguration bei der Inbetriebnahme) oder einer anerkannten gesetzlichen Ausnahme. Die Einwilligung kann jederzeit in den Kontoeinstellungen der Plattform verwaltet werden.

8. Mitarbeiter- und Bediener-Daten in Verbindung mit Geräten

Wenn ein Kunde optional einen Mitarbeiter oder Bediener einem bestimmten Gerät auf der Plattform zuordnet, stellen die damit verbundenen Telemetrie- und GPS-Daten personenbezogene Daten dar. Die Lifiot UG (haftungsbeschränkt) verarbeitet diese Daten als Auftragsverarbeiter auf Weisung des Kunden. Gemäß Art. 14 DSGVO (nicht direkt von der betroffenen Person erhobene Daten): Soweit Lifiot personenbezogene Daten über Mitarbeiter oder Bediener erhält, die nicht direkt von diesen Personen bereitgestellt wurden, ist die Quelle dieser Daten die Kundenorganisation (der Arbeitgeber oder Auftraggeber), der die Plattform nutzt. Die aus dieser Quelle erhaltenen Datenkategorien können umfassen: Name, Mitarbeiterkennung, Berufsbezeichnung sowie sonstige vom Kunden bei der Gerätezuweisung eingetragene Felder.

***WICHTIGER HINWEIS FÜR KUNDEN:** Vor der Zuordnung von Mitarbeitern zu Geräten müssen Sie sicherstellen, dass Ihre Mitarbeiter entsprechend über die Geräteüberwachung informiert wurden. Dies hat im Einklang mit Ihren Arbeitgeberpflichten gemäß DSGVO und dem anwendbaren nationalen Arbeitsrecht zu erfolgen (z. B. durch eine Betriebsvereinbarung gemäß § 87 Abs. 1 Nr. 6 BetrVG).*

9. Datei- und Dokumenten-Upload-Verarbeitung

- Dateien werden auf AWS-Infrastruktur innerhalb des EWR (Frankfurt oder Irland) gespeichert.
- Wir analysieren oder extrahieren keine personenbezogenen Daten aus hochgeladenen Dateien, soweit dies nicht für den Speicher- und Abrufdienst notwendig ist.
- Kunden sind Verantwortliche für personenbezogene Daten in hochgeladenen Dateien.
- Nach Vertragsende stehen Dateien 90 Tage zum Export zur Verfügung, danach werden sie dauerhaft gelöscht.

10. Marketingkommunikation

Mit Ihrer ausdrücklichen Einwilligung (Art. 6 Abs. 1 lit. a DSGVO) senden wir Ihnen Marketing-E-Mails zu Plattformfunktionen und Updates. Sie können Ihre Einwilligung jederzeit durch Klicken auf den Abmelde-Link oder durch Kontaktaufnahme unter info@lifiot.com widerrufen. Marketing-E-Mails werden direkt von unseren eigenen Konten versendet — kein Drittanbieter-E-Mail-Dienst erhält Ihre Daten. Angabepflicht — Marketingkommunikation: Die Erteilung der Einwilligung für Marketing-E-Mails ist vollständig freiwillig. Die Verweigerung oder der Widerruf der Einwilligung hat keine Auswirkungen auf Ihren Plattformzugang oder Ihr Abonnement.

11. Auftragsverarbeiter und Datenempfänger

11.1 Liste der Auftragsverarbeiter

Empfänger	Zweck	Datenkategorien	Rechtsgrundlage	Land	Übermittlungsgru
Amazon Web Services EMEA SARL	Cloud-Infrastruktur & Dateispeicherung	Alle Plattformdaten inkl. IoT-Telemetrie, GPS, Dateien	Art. 6 Abs. 1 lit. b DSGVO	Deutschland / Irland (EWR)	EWR — kein Übermittlungsmech erforderlich
Internes CRM Lifiot UG	Kundenbeziehungsmanagement	Name, E-Mail, Unternehmen, Abonnementdaten	Art. 6 Abs. 1 lit. b/f DSGVO	Deutschland (EWR)	EWR — kein Übermittlungsmech erforderlich
Stripe, Inc.	Online-Zahlungsabwicklung	Name, E-Mail, Rechnungsadresse, Zahlungsdaten	Art. 6 Abs. 1 lit. b DSGVO	USA	EU-US Data Privacy Framework + SCC Abs. 2 lit. c DSGVO

Die oben aufgeführten Auftragsverarbeiter geben unsere aktuellen Engagements wieder. Im Zuge der Weiterentwicklung unserer Plattform können Auftragsverarbeiter hinzugefügt, ersetzt oder entfernt werden. Wir pflegen eine stets aktuelle Liste der Auftragsverarbeiter und benachrichtigen Kunden mit angemessener Vorankündigung über wesentliche Änderungen, während derer Kunden berechnigte Einwände erheben können. Die aktuelle Liste ist stets abrufbar unter www.lifiot.com/subprocessors.

11.2 Gesetzlich vorgeschriebene Offenlegungen

Wir können personenbezogene Daten offenlegen, soweit dies durch geltendes Recht oder eine verbindliche gerichtliche Anordnung vorgeschrieben ist. Wir haben Maßnahmen ergriffen, um den Zugriff von Behörden außerhalb des EWR auf nicht-personenbezogene Daten ohne gültige EU-Rechtsgrundlage zu verhindern.

11.3 Aggregierte Daten

Vollständig anonymisierte, aggregierte Branchenstatistiken können für die Produktentwicklung verwendet werden. Diese Daten lassen keinen Rückschluss auf einzelne Kunden zu.

12. Internationale Datenübermittlungen

Plattformdaten werden vorrangig auf AWS-Infrastruktur innerhalb des EWR (Frankfurt, Deutschland oder Dublin, Irland) gehostet. Wir haben EWR-basierte Regionen als primäre Hosting-Umgebung gewählt, um Drittlandsübermittlungen zu minimieren. Soweit ein gelegentlicher Zugriff auf Plattformdaten aus Drittländern erfolgt — beispielsweise im Rahmen von technischem Support, Entwicklung oder Sicherheitsoperationen — stellen wir geeignete Garantien sicher, einschließlich Standardvertragsklauseln (SCC) gemäß Art. 46 Abs. 2 lit. c DSGVO. Die primär identifizierte Drittlandsübermittlung ist die Zahlungsabwicklung über Stripe, Inc. (USA), geregelt durch das EU-US-Datenschutzrahmenwerk und SCC.

13. Speicherfristen

Datenkategorie	Speicherfrist	Zweck	Rechtsgrundlage
Konto- und Nutzerdaten	Vertragsdauer + 3 Jahre	Rechtliche Compliance, Streitigkeiten	§ 195 BGB
IoT-Telemetrie und GPS-Daten	Vertragsdauer + 90 Tage	Export-Zeitraum nach Kündigung	Vertragserfüllung
Hochgeladene Dateien	Vertragsdauer + 90 Tage	Export-Zeitraum nach Kündigung	Vertragserfüllung
Plattform-Zugriffsprotokolle	12 Monate	Erkennung von Sicherheitsvorfällen	Berechtigtes Interesse
Rechnungs- und Buchungsunterlagen	10 Jahre	Deutsches Handels-/Steuerrecht	§ 257 HGB, § 147 AO
Nachweise über Marketingeinwilligungen	Bis Widerruf + 3 Jahre	Einwilligungsnachweis	Art. 7 Abs. 1 DSGVO
Daten für Rechtsansprüche	Bis zu 30 Jahre	Geltendmachung/Abwehr von Ansprüchen	Art. 6 Abs. 1 lit. f DSGVO

14. Ihre Rechte nach der DSGVO

Sie haben jederzeit das Recht, eine Beschwerde bei einer Aufsichtsbehörde einzulegen, insbesondere in dem EU-Mitgliedstaat Ihres gewöhnlichen Aufenthaltsorts, Ihres Arbeitsplatzes oder des Orts des mutmaßlichen Verstoßes. Zur Ausübung Ihrer sonstigen Rechte wenden Sie sich bitte an info@lifiot.com. Wir werden innerhalb von 30 Tagen antworten.

- **Auskunftsrecht (Art. 15 DSGVO):** Erhalt einer Kopie der über Sie gespeicherten personenbezogenen Daten.
- **Recht auf Berichtigung (Art. 16 DSGVO):** Korrektur unrichtiger oder unvollständiger Daten.
- **Recht auf Löschung (Art. 17 DSGVO):** Löschung von Daten vorbehaltlich gesetzlicher Aufbewahrungspflichten.
- **Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO):** Einschränkung der Verarbeitung unter bestimmten Voraussetzungen.
- **Recht auf Datenübertragbarkeit (Art. 20 DSGVO):** Erhalt Ihrer Daten in maschinenlesbarem Format (JSON oder CSV).

- Widerspruchsrecht (Art. 21 DSGVO): Widerspruch gegen Verarbeitung auf Basis berechtigter Interessen.
- Recht auf Widerruf der Einwilligung (Art. 7 Abs. 3 DSGVO): Widerruf jederzeit ohne Auswirkung auf die Rechtmäßigkeit vorheriger Verarbeitung.
- Recht bezüglich automatisierter Entscheidungen (Art. 22 DSGVO): Kein Recht auf ausschließlich automatisierte Entscheidungen mit rechtlicher Wirkung — wir treffen solche Entscheidungen nicht.

Zuständige Aufsichtsbehörde:

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg (LfDI BW)

Lautenschlagerstraße 20, 70173 Stuttgart — www.baden-wuerttemberg.datenschutz.de

15. Datensicherheit

- AES-256-Verschlüsselung der gespeicherten Daten und TLS 1.3 für Daten bei der Übertragung auf AWS-Infrastruktur.
- Rollenbasierte Zugriffskontrollen (RBAC) zur Beschränkung des Datenzugriffs auf autorisiertes Personal.
- Regelmäßige Sicherheitsbewertungen, Schwachstellenscans und Penetrationstests.
- Dokumentierte Verfahren zur Behandlung von Vorfällen: Datenschutzverletzungen werden gemäß Art. 33 DSGVO bewertet und behandelt, einschließlich der Meldung an den LfDI BW, soweit gesetzlich vorgeschrieben.
- AWS-Infrastruktur: SOC 2 Typ II, ISO/IEC 27001, ISO/IEC 27017 zertifiziert.

16. Verarbeitung zur Geltendmachung von Rechtsansprüchen

Wir verarbeiten personenbezogene Daten zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen auf Basis von Art. 6 Abs. 1 lit. f DSGVO — unser berechtigtes Interesse an der Durchsetzung vertraglicher Rechte, der Abwehr unbegründeter Ansprüche sowie der Einhaltung gerichtlicher und behördlicher Anforderungen. Daten können bis zu 30 Jahre nach Beendigung der Geschäftsbeziehung aufbewahrt werden, soweit gesetzlich erforderlich.

17. Änderungen dieser Datenschutzerklärung

Wir werden Sie über wesentliche Änderungen mindestens 30 Tage im Voraus per E-Mail oder Plattform-Benachrichtigung informieren. Die aktuelle Version ist stets abrufbar unter www.lifiot.com/privacy.

18. Kontakt

Lifiot UG (haftungsbeschränkt)

Luisenstr. 7, 78048 Villingen-Schwenningen, Deutschland

HRB 728690 | USt-IdNr.: DE361451350

E-Mail: info@lifiot.com | Website: www.lifiot.com/privacy

Aufsichtsbehörde: LfDI Baden-Württemberg — www.baden-wuerttemberg.datenschutz.de