Privacy Declaration: DeviceLab ApS

Effective Date: 19 April 2026

Version: 2.3

1. Introduction

This Privacy Declaration describes how **DeviceLab ApS** ("we", "us", or "our") handles personal data. As a specialised B2B provider of IoT hardware and software for the utility sector, we operate on the principle of "Privacy by Design". We minimise data collection to what is strictly necessary for professional business operations, financial management, and technical support.

2. Data Controller

DeviceLab ApS is the data controller for the personal data of our business contacts, website visitors, and professional partners.

- **Company:** DeviceLab ApS (CVR: 40220445)
- **Address:** Haraldsvej 60, 1., 8960 Randers SØ, Denmark
- **Privacy Lead:** Palle Haderslev
- **Contact:** info@devicelab.dk

3. Data Processing Activities

3.1 Software & Hardware (Payload Collector / Extractor)

Our software solutions are engineered to ensure client data sovereignty:

- **On-Premise Architecture:** All software is installed locally on the customer's infrastructure. DeviceLab ApS has no access to the customer's live data or server environment.
- **Encryption Key Management (Keystore):** Whilst our software features a secure keystore for meter encryption keys, these keys are stored locally within the customer's environment. **DeviceLab ApS does not have access to these keys**, and we cannot decrypt or view the meter data.
- **Remote Support:** In exceptional cases where technical support is requested, remote access may be granted by the customer. This access is strictly temporary and performed under customer supervision. No personal data is extracted or stored by DeviceLab during these sessions.

3.2 Sales, Marketing & Lead Generation

We process professional contact information to grow our B2B operations:

- **Lead Generation:** We engage specialised marketing sub-processors and tools, such as **Walego**, to identify potential B2B partners on LinkedIn. Initial correspondence occurs within the LinkedIn messaging system.
- **CRM & Correspondence:** If a lead progresses, professional contact details (name, title, company email) are transferred to our **Google Workspace** environment for further negotiation and project management.
- **Legal Basis:** This processing is based on our **Legitimate Interest** (GDPR Art. 6(1)(f)) and **Contractual Necessity** (GDPR Art. 6(1)(b)).

3.3 Financial & Administrative Management

We process personal data related to invoicing and contract management to comply with Danish law. This includes:

- Sharing relevant financial data with our outsourced accounting partner, **Valentin Regnskab**, for the purposes of bookkeeping, VAT reporting, and financial auditing.

4. Sub-processors & International Transfers

To provide our services, we use the following third-party providers. All transfers outside the EU/EEA are governed by the **EU-U.S. Data Privacy Framework** or the European Commission's **Standard Contractual Clauses (SCCs)**.

Provider / Partner	**Purpose**	**Location**
Google Cloud EMEA	Workspace (Email, Files, Meet)	EU/US
Carrd Inc.	Website Hosting	US

Matomo Cloud	Web Analytics	EU
Visma e-conomic	Accounting Platform	DK
Valentin Regnskab	Outsourced Financial & Bookkeeping Services	DK
Walego	LinkedIn Lead Generation & Marketing Support	EU
Signal Messenger	Encrypted internal & subcontractor comms	US (E2EE)
Technical Subcontractors	Engineering and consultancy services	EU/EEA

5. Data Retention

- **Financial Records:** We retain invoices and related contact data for **5 years** to comply with the *Danish Bookkeeping Act* (*Bogføringsloven*).
- **Marketing Leads:** Data from leads that do not result in a contract is deleted or anonymised after **2 years** of inactivity.
- **Technical Support:** Any temporary logs or credentials used during a support session are deleted immediately upon case resolution.

6. Security & Confidentiality

We implement rigorous technical and organisational measures, including:

- **Encrypted Communication:** We utilise end-to-end encrypted (E2EE) channels, such as **Signal**, for all internal coordination and communication with subcontractors (technical, financial, and marketing) to ensure project confidentiality.
- **Data Protection:** Use of **AES-256 encryption** for data at rest within our Google Workspace and **Two-Factor Authentication (2FA)** on all internal systems.
- **Access Control:** Strict internal policies regarding the handling of client-side remote access and the immediate revocation of support credentials.

7. Your Rights

Under the GDPR, you have the right to request **access**, **rectification**, or **erasure** of your personal data, and the right to **object** to our processing.

To exercise these rights, please contact **info@devicelab.dk**. You may also lodge a complaint with the Danish Data Protection Agency (**Datatilsynet**) at www.datatilsynet.dk.
