

Privacy Policy for iPwr

1. Introduction

iPwr B.V., Oude Middenweg 85, 2491AC Den Haag ("we", "us", "our") is committed to protecting your personal data and handling it transparently and securely. This privacy policy explains how we collect, use, and protect your data when you use the iPwr software platform. We process your personal data in accordance with the General Data Protection Regulation (GDPR) and other applicable data protection laws. Some personal data is necessary to ensure the correct functioning of our services and to comply with legal obligations. This policy also explains your rights regarding your personal data and how you can exercise them.

2. Data Controller

The data controller responsible for processing your personal data is:

iPwr B.V.
 Oude Middenweg 85
 2491 AC Den Haag
 The Netherlands
 Email: support@ipwr.nl

3. What Data Do We Collect?

We only collect data that is necessary for the proper functioning of the iPwr software platform and to meet our legal obligations. Depending on your use of our services, we may collect the following categories of personal data:

- (i) **Identification and Contact Information:** Name, email address, home address, phone number, username, and securely hashed passwords (not stored in plain text).
- (ii) **Household Information:** Information such as home size, number of occupants, heating system type, and historical energy usage.
- (iii) **Sensor Data from Connected Devices:** Data from smart meters, thermostats, or electric vehicles, including device model, operational status, and energy or battery measurements. Smart meter data is processed in accordance with the *Gedragcode Slim Netbeheer*.
- (iv) **Purchase Information:** Information provided during product or service purchases, including product selection and payment method.
- (v) **Communication Data:** Content you share with us via customer support or messaging features.
- (vi) **Technical Data:** Information such as operating system, device characteristics, session timestamps, usage history, and crash reports.

We do not collect special categories of personal data as defined in Article 9 GDPR (e.g. health, religion, political opinions).

4. Purposes and Legal Bases for Data Processing

We process your personal data only when there is a clear purpose and a valid legal basis under the General Data Protection Regulation (GDPR, Article 6). These purposes include the execution of a contract, compliance with legal obligations, our legitimate interests, or your explicit consent. Our legitimate interests may include improving the performance and reliability of our software platform and ensuring secure and user-friendly service delivery. Below is an overview of purposes, data categories, and legal bases:

Purpose of Processing	Categories of Data	Legal Basis
Creating and managing your account	Identification and Contact Information	Performance of a contract
Providing and optimizing our Services	Technical Data, Sensor Data	Performance of a contract; Legitimate interest

Purpose of Processing	Categories of Data	Legal Basis
Communication and customer support	Communication Data	Performance of a contract; Legitimate interest
Marketing and promotional activities	Identification and Contact Information	Consent; Legitimate interest
Compliance with legal obligations	All relevant categories	Legal obligation

5. Sharing Your Data

We only share your personal data with third parties when necessary to provide our services or when required by law. We ensure that all parties we work with comply with applicable data protection laws and maintain adequate technical and organizational safeguards.

We may share your personal data with:

- (i) **Service Providers and Partners:** We have a Data Processing Agreement in place with Nexxtlab, who acts as our data processor for the technical operation of the iPwr software platform. Nexxtlab may only use sub-processors with our prior consent and must inform us of any changes. All processors and sub-processors are contractually bound to comply with the GDPR and ensure data security.
- (ii) **Government Authorities:** When required to comply with legal obligations, such as responding to regulatory requests or law enforcement.
- (iii) **Other Third Parties:** With your explicit consent, or where legally permitted. This may include hosting providers, analytics platforms, or grid operators when necessary for service delivery or regulatory compliance.

We do not sell your personal data. Where applicable, we will provide you with the option to opt in or opt out of certain types of data sharing.

6. Data Processing Terms

This section summarizes key terms of the Data Processing Agreement (DPA) between iPwr (Controller) and Nexxtlab (Processor) for the technical operation of the iPwr software platform, in accordance with Article 28 GDPR.

The Processor shall process personal data only on documented instructions from the Controller, which may include written directives, APIs, or functional specifications. These instructions cover the scope, duration, purpose, data categories, data subjects, and any international data transfers. All personnel and approved sub-processors involved in data processing must maintain confidentiality. The Processor may not appoint sub-processors without the Controller’s prior written authorization. If general authorization is granted, the Processor must inform the Controller of any changes in advance, and the Controller may object.

The Processor shall implement appropriate technical and organizational security measures, including but not limited to encryption, access controls, system resilience, and regular testing, in accordance with Article 32 GDPR. Audit or compliance evidence must be provided upon request. The Processor must notify the Controller—typically within 24–48 hours—of any data breach or deviation from the Controller’s instructions, and provide all necessary information to support regulatory reporting.

The Processor shall assist the Controller with handling data subject requests, breach notifications, Data Protection Impact Assessments (DPIAs), and any required consultations with supervisory authorities.

Upon termination of the processing relationship, the Processor shall either return or securely delete all personal data (including backups), as instructed by the Controller, unless legal retention is required.

The Processor remains liable to the Controller for any acts of sub-processors. The Controller retains the right to audit the Processor and any sub-processors to verify compliance.

Any data transfers to countries outside the EU/EEA may only take place upon the Controller's documented instruction and must be protected by appropriate safeguards, such as Standard Contractual Clauses (SCCs).

7. Retention Periods

We retain your personal data for as long as necessary for the purposes for which it was collected, or as required by applicable law. Personal data is anonymized according to guidelines set by the European Data Protection Board (EDPB) and the Dutch Data Protection Authority (Autoriteit Persoonsgegevens).

Retention periods are as follows:

- (i) Contractual and billing information: up to 7 years, in line with tax regulations (Art. 52 AWR)
- (ii) Technical device data and usage logs: up to 2 years after contract termination
- (iii) Support communications: up to 3 years for quality monitoring and legal defense
- (iv) Marketing data (with consent): up to 12 months after last user interaction.

8. Your Rights

You have the following rights regarding your personal data:

- (i) **Right of Access:** You may request access to the personal data we hold about you.
- (ii) **Right to Rectification:** You may request the correction of inaccurate or incomplete data.
- (iii) **Right to Erasure:** You may request the deletion of your data under certain circumstances.
- (iv) **Right to Restrict Processing:** You may request a temporary restriction of processing in specific situations.
- (v) **Right to Data Portability:** You may request to receive your data or have it transferred to another controller.
- (vi) **Right to Object:** You may object to processing based on our legitimate interests or for direct marketing purposes.

You can submit a request by emailing privacy@ipwr.nl. We will respond within one month of receipt. If your request is complex, this period may be extended by up to two additional months, and we will notify you accordingly.

We may ask for additional information to verify your identity before processing your request. Please note that exercising certain rights (such as deletion or restriction) may affect our ability to deliver the iPwr software platform. If this is the case, we will inform you and discuss possible solutions.

You also have the right to lodge a complaint with your local supervisory authority, such as the **Dutch Data Protection Authority (Autoriteit Persoonsgegevens)**.

9. Changes to This Privacy Policy

We may update this privacy policy from time to time, for example, to add new features to the service or due to legal or regulatory reasons. For significant changes, we will notify you. We recommend reviewing this policy regularly.

10. Contact Information

If you have any questions about this privacy policy or the processing of your data, please contact our Data Protection Officer.