Wevo Energy (Acquired by SolarEdge) Data Processing Agreement

DATA PROCESSING AGREEMENT [Last Updated January 2026] This Data Processing Agreement ("DPA") is incorporated and forms an integral part of the Software as a Service Agreement and any Service Order (collectively "Agreement") executed by and between Wevo Energy LTD ("Wevo"), a wholly owned subsidiary of Solaredsge technologies, and the customer identified under the Service Order ("Customer"). Wevo and the Customer shall each be referred to as a "party" and collectively the "parties". All capitalized terms not defined herein shall have the meaning set forth in the Agreement. The parties have agreed to enter into this DPA to address the compliance obligations imposed upon Wevo and the Customer pursuant to the Data Protection Laws (as defined below). Therefore, this DPA sets forth the parties' responsibilities and obligations regarding the Processing of Users' Personal Data during the course of the engagement.

1. Definitions

1.1 "Adequate Country" is a country that received an adequacy decision from the European Commission.

1.2 "CCPA" means the California Consumer Privacy Act (Cal. Civ. Code §§ 1798.100 – 1798.199) of 2018, including as modified by the California Privacy Rights Act ("CPRA") as well as all regulations promulgated thereunder from time to time.

1.3 The terms “Controller”, “Processor”, “Data Subject”, “Processing” (and “Process“), “Personal Data”, “Personal Data Breach”, “Special Categories of Personal Data” and “Supervisory Authority”, shall all have the same meanings as ascribed to them in the EU Data Protection Law. The terms “Business”, “Business Purpose”, “Consumer”, “Service Provider”, “Contractor”, “Third Party Business”, “Sale”, “Sell” and “Share” shall have the same meaning as ascribed to them in the CCPA. ““Data Subject” shall also mean and refer to “Consumer”, as such term defined under the CCPA, “Personal Data” shall include “Personal Information” under this DPA.

1.4 “Data Protection Law” means any and all applicable privacy and data protection laws and regulations (including, where applicable, EU Data Protection Law, UK Data Protection Laws, Swiss Data Protection Laws and the CCPA) as may be amended or superseded from time to time.

1.5 “European Data Protection Law” means the (i) EU General Data Protection Regulation (Regulation 2016/679) (“GDPR”); (ii) Regulation 2018/1725; (iii) the EU e-Privacy Directive (Directive 2002/58/EC), as amended (e-Privacy Law); (iv) any national data protection laws made under, pursuant to, replacing, adopting or succeeding (i) and (ii) including the the Data Protection Act 2018 (DPA 2018), as amended, and the GDPR as it forms part of domestic law in the United Kingdom by virtue of section 3 of the European Union (Withdrawal) Act 2018 (“UK GDPR”), and the Swiss Federal Data Protection Act (dated June 19, 1992, as of March 1, 2019) (“FDPA”) as well as the Ordinance on the Federal Act on Data Protection (“FODP”); (v) any legislation replacing or updating any of the foregoing; and (vi) any judicial or administrative interpretation of any of the above, including any binding guidance, guidelines, codes of practice, approved codes of conduct or approved certification mechanisms issued by any relevant Supervisory Authority.

1.6 “Security Incident” means any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data. Any Personal Data Breach will comprise a Security Incident.

1.7 “Standard Contractual Clauses” mean, collectively and as applicable: (i) the standard contractual clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council adopted by the European Commission Decision 2021/914 of 4 June 2021, which may be found at: Standard Contractual Clauses; (ii) the UK “International Data Transfer Addendum to The European Commission Standard Contractual Clauses” available HERE as adopted, amended or updated by the UK Information Commissioner Office, Parliament or Secretary of State; and (iii) the applicable standard data protection clauses issued, approved or recognized by the Swiss Federal Data Protection and Information Commissioner.

2. Roles And Details of Processing

2.1 The parties agree and acknowledge that under the performance of their obligations set forth in the Agreement, and with respect to the Processing of Users’ Personal Data:

• With regards to: (i) Authorized Users' Personal Data; (ii) Users' Personal Data uploaded by the Authorized Users to the Platform; and (iii) End Users' Personal Data collected while using a Branded App (collectively "Customer Data") – Wevo is acting as a Processor and Service Provider and Customer is acting as a Controller and a Business.

• With regards to End Users' Personal Data collected while using a Wevo App – the parties shall act as independent co-controllers ("ICC") and each as a Business with regards to certain data sets as further detailed in Section 10. Personal Data Processed by Wevo in its role as an ICC shall be further referred to herein as "Wevo Data". Each party shall be individually and separately responsible for complying with the obligations that apply to such party under applicable Data Protection Law.

2.2 The subject matter and duration of the Processing carried out by the Processor on behalf of the Controller, the nature and purpose of the Processing, the type of Personal Data and categories of Data Subjects are described in Annex I attached hereto.

2.3 Where the CCPA applies to Wevo's Processing of Customer Data as a Service Provider, Wevo shall not:

(i) Sell or Share the Customer Data; (ii) retain, use or disclose the Customer Data for any purpose other than for a Business purpose specified in the Agreement; (iii) combine the Customer Data with other Personal Information that it receives from, or on behalf of, another customer, or collects from its own interaction with California residents (other than, when applicable, Customer's Users using the Wevo App), expect as otherwise permitted by the CCPA; (iv) Wevo permits Customer to monitor its compliance subject to Section 8 in the DPA “Audit Rights”; (v) Wevo agrees to notify the Customer if Wevo makes a determination that it can no longer meet its obligations under this DPA or the CCPA;

(vi) Wevo shall provide assistance as Customer may reasonably request, in connection with any obligation by Customer to respond to requests for exercising the rights of a Consumer under the CCPA. In addition, Wevo acknowledges and confirms that it does not receive or Process any Customer Data as consideration for any Services that Wevo provides to Customer under the Agreement.

3. Representations and Warranties

3.1 Wevo represents and warrants that it shall Process Customer Data, on behalf of the Customer (subject to Article 28 of the GDPR), solely for the purpose of providing the Service, all in accordance with Customer’s written instructions under the Agreement and this DPA. Notwithstanding the above, in the event Wevo is required under applicable laws, including Data Protection Law, to Process Customer Data other than as instructed by Customer, Wevo shall make its best efforts to inform the Customer of such requirement prior to Processing such Customer Data, unless prohibited under applicable law.

3.2 Wevo shall provide reasonable cooperation and assistance to the Customer in ensuring compliance with its obligation to carry out data protection impact assessments with respect to the Processing of its Customer Data and to consult with the Supervisory Authority (as applicable).

3.3 Where applicable, Wevo shall assist the Customer in ensuring that Customer Data Processed is accurate and up to date, by informing the Customer if it becomes aware of the fact that the Customer Data it is processing is inaccurate or has become outdated. Wevo shall take reasonable steps to ensure: (i) the reliability of its staff and any other person acting under its supervision who may come into contact with, or otherwise have access to and Process Customer Data; (ii) that persons authorized to process the Customer Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality; and (iii) that such personnel are aware of their responsibilities under this DPA and any applicable Data Protection Laws.

4. Data Subjects Rights and Request

4.1 It is agreed that where Wevo receives a request from a Data Subject or an applicable authority in respect of Customer Data, where applicable, Wevo will direct the Data Subject or the applicable authority to the Customer in order to enable the Customer to respond directly to the Data Subject’s or the applicable authority’s request, unless otherwise required under applicable laws. Parties shall provide each other with commercially reasonable cooperation and assistance in relation to the handling of a Data Subject’s or applicable authority’s request, to the extent permitted under Data Protection Law.

5. Sub-Processing

5.1 The Customer acknowledges and agrees that Wevo may transfer Customer Data to and otherwise interact with third party data Processors (“Sub-Processor”).

5.2 Where the European Data Protection Laws apply – the Customer hereby authorizes Wevo to engage and appoint such Sub-Processors as listed in Annex II, to Process Customer Data, as well as permits each Sub-Processor to appoint a Sub-Processor on its behalf. Where Wevo may engage an additional or replace an existing Sub-Processors to process Customer Data, subject to the provision of a ten (10) days prior notice of its intention to do so to the Customer. In case the Customer has not objected to the adding or replacing of a Sub-Processor within the aforesaid prior notice period, such Sub-Processor shall be considered approved by the Customer. In the event the Customer objects to the adding or replacing of a Sub-Processor, where such objection can be made solely on reasonably grounds related to non-compliance with Data Protection Laws, Wevo may, under Wevo' sole discretion, suggest the engagement of a different Sub-Processor, or otherwise terminate the Agreement.

5.3 Wevo shall, where it engages any Sub-Processor, impose, through a legally binding contract, data protection obligations similar to those set out in this DPA. Wevo shall remain responsible to the Customer for the performance of the Sub-Processor's obligations in accordance with this DPA.

6. Technical and Organizational Measures

6.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context, and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, and without prejudice to any other security standards agreed upon by the parties, Wevo shall implement and will maintain appropriate physical, technical and organizational measures to protect the Customer Data as required under Data Protection Laws.

7. Security Incident

7.1 Wevo will notify the Customer upon becoming aware of a confirmed Security Incident involving the Customer Data in Wevo's possession or control. Wevo's notification regarding or response to a Security Incident shall not be construed as an acknowledgment by Wevo of any fault or liability with respect to the Security Incident.

7.2 Wevo will: (i) take necessary steps to remediate, minimize any effects of and investigate any Security Incident and to identify its cause; (ii) co-operate with the Customer and provide the Customer with such reasonable assistance and information as it may reasonably require in connection with the containment, investigation, remediation or mitigation of the Security Incident; and (iii) reasonably co- operate with the Customer and assist Customer with its obligation to notify the affected individuals in the case of a Security Incident.

8. Audit Rights

8.1 Wevo shall maintain records of the Processing activities of any Customer Data carried out under this DPA and shall make such records available to the Customer and applicable supervisory authorities upon written request. Such records provided shall be considered Wevo' Confidential Information and shall be subject to confidentiality obligations.

8.2 In the event the records and documentation provided subject to Section 8.1 above are not sufficient, Wevo shall make available, solely upon prior reasonable written notice and no more than once per year, to a reputable auditor nominated by the Customer, information necessary to reasonably demonstrate compliance with this DPA in Wevo's role as a Processor, and shall allow for audits, including inspections, by such reputable auditor solely in relation to the Processing of the Customer Data (provided that the Customer shall not be entitled to access any of Wevo's systems)("Audit") in accordance with the terms and conditions hereunder. The auditor shall be subject to the terms of this DPA and standard confidentiality obligations (including towards third parties). Wevo may object to an auditor appointed by the Customer in the event Wevo reasonably believes the auditor is not suitably qualified or independent, is a competitor of Wevo or otherwise unsuitable ("Objection Notice"). The Customer will appoint a different auditor or conduct the Audit itself upon its receipt of an Objection Notice from Wevo. Customer shall bear all expenses related to the Audit and shall (and ensure that each of its auditors shall), avoid causing any damage, injury or disruption to Wevo' premises, equipment, personnel and business while its personnel are on those premises in the course of such Audit. Any and all conclusions of such Audit shall be confidential and reported back to Wevo immediately.

9. Cross Border Personal Data Transfers

9.1 Where the GDPR, UK GDPR or the Swiss FADP is applicable, if the Processing of Personal Data by Wevo in its role as a Processor to a Sub-Processor includes transfer of Personal Data to a third country outside the European Economic Area ("EEA"), the UK and Switzerland that is not an Adequate Country, such transfer shall only occur if an appropriate safeguard approved by the applicable Data Protection Law (the GDPR (Article 46), UK GDPR (Article 46) or Swiss FADP (as applicable)) for the lawful transfer of Personal Data under is in place.

10. Independent Co-Controllers

10.1 When parties are ICC: (i) It is hereby clarified that in no event will the parties Process the data as joint controllers. Each party shall be individually and separately responsible for complying with the obligations that apply to it, in accordance with the Data Protection Laws; (ii) If a party receives a request from a Data Subject or an applicable authority in respect to Personal Data processed by the parties as ICC, it will notify the other party of such request, and where applicable, direct the Data Subject or the applicable authority to the other party; (iii) Each party shall notify the other party upon becoming aware of any Security Incident involving the Personal Data Processed by it as ICC.

11. Term, Termination and Conflict

11.1 This DPA shall be effective as of the Effective Date (as defined in the agreement) and shall remain in force until the Agreement terminates. Wevo shall be entitled to terminate this DPA or terminate the Processing of Customer Data in the event that Processing of Customer Data under the Customer’s instructions or this DPA infringe applicable legal requirements. Following the termination of this DPA, Wevo shall, at the choice of the Customer, delete all Customer Data processed on behalf of the Customer and certify to the Customer that it has done so, or, return all

Customer Data to the Customer and delete existing copies, unless applicable law or regulatory requirements requires that Wevo continue to store Customer Data.

11.2 In the event of a conflict between the terms and conditions of this DPA and the Agreement, this DPA shall prevail. For the avoidance of doubt, in the event Standard Contractual Clauses have been executed between the parties, the terms of the Standard Contractual Clauses shall prevail over those of this DPA. Except as set forth herein, all of the terms and conditions of the Terms shall remain in full force and effect. ANNEX I – DETAILS OF PROCESSING This Annex includes certain details of the Processing of Customer Data as required by Article 28(3) GDPR. Categories of Data Subjects: Authorized Users and Users, as defined under the Agreement. Categories of Personal Data processed: Credentials; contact information; authentication and security credentials; online identifiers; address and parking space; payment information; Charger's usage information. Special Categories of Personal Data: None. Nature of the processing: Collection, storage, organization, communication, transfer, host and other uses in performance of the Services as set out in the Agreement. Purpose(s) of Processing: To provide the Service. Retention Period: For as long as is necessary to provide the Service by Wevo; provided there is no legal obligation to retain the Personal Data past termination or unless otherwise requested by the Customer. Process Frequency: Continuous basis ANNEX II – LIST OF SUB-PROCESSORS Name Servers Address Description of the processing Amazon Web Services (AWS) EU hosting and storage Intercom, inc. EU/US Cloud based customer support and messaging. Coralogix Ltd EU Analytics Pipedrive EU/US CRM sales tool Stripe EU/US Payment processing Grow EU Payment processing Retell AI US AI support agent

ANNEX I – DETAILS OF PROCESSING

This Annex includes certain details of the Processing of Customer Data as required by Article 28(3) GDPR.

Categories of Data Subjects:

Authorized Users and Users, as defined under the Agreement.

Categories of Personal Data processed:

Credentials; contact information; authentication and security credentials; online identifiers; address and parking space; payment information; Charger's usage information.

Special Categories of Personal Data:

None.

Nature of the processing:

Collection, storage, organization, communication, transfer, host and other uses in performance of the Services as set out in the Agreement.

Purpose(s) of Processing:

To provide the Service.

Retention Period:

For as long as is necessary to provide the Service by Wevo; provided there is no legal obligation to retain the Personal Data past termination or unless otherwise requested by the Customer.

Process Frequency:

Continuous basis

ANNEX II – LIST OF SUB-PROCESSORS

Name	**Servers Address**	**Description of the processing**
Amazon Web Services (AWS)	EU	hosting and storage
Intercom, inc.	EU/US	Cloud based customer support and messaging.
Coralogix Ltd	EU	Analytics
Pipedrive	EU/US	CRM sales tool
Stripe	EU/US	Payment processing

Grow	EU	Payment processing
Retell AI	US	AI support agent

ANNEX III: TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

Last Updated: December 2025

This Annex forms part of the Data Processing Agreement (“DPA”) between Wevo Energy Ltd. (“Processor”) and the Customer (“Controller”).

1. CERTIFICATIONS AND COMPLIANCE FRAMEWORK

1.1 Information Security Management

Wevo Energy maintains an Information Security Management System (ISMS) certified to the following international standards:

Certification	**Scope**	**Certification Body**
ISO/IEC 27001	Information Security Management System	SII (Standards Institution of Israel)
ISO/IEC 27017	Cloud Security Controls	SII (Standards Institution of Israel)
ISO/IEC 27018	Protection of PII in Public Clouds	SII (Standards Institution of Israel)

Certificates are available upon request and are subject to annual surveillance audits and triennial recertification.

---

2. TECHNICAL MEASURES

2.1 Encryption

Measure	Implementation
Data at Rest	AES-256 encryption for all stored Personal Data
Data in Transit	TLS 1.2 or higher for all data transmissions
Key Management	Encryption keys managed through AWS KMS with automatic rotation
Database Encryption	Transparent Data Encryption (TDE) enabled on all production databases

2.2 Access Control

Measure	Implementation
Authentication	Multi-factor authentication (MFA) required for all administrative access
Authorization	Role-based access control (RBAC) with principle of least privilege
Password Policy	Minimum 12 characters, complexity requirements, 90-day rotation
Session Management	Automatic session timeout after 15 minutes of inactivity
Privileged Access	Just-in-time privileged access for administrative functions
Access Reviews	Quarterly access reviews for all systems containing Personal Data

2.3 Network Security

Measure	Implementation
Firewalls	Web Application Firewall (WAF) and network firewalls (AWS security groups) with default-deny policies
Segmentation	Network segmentation between production, development, and corporate environments
Intrusion Detection	IDS/IPS monitoring with 24/7 alerting (AWS GuardDuty)
DDoS Protection	AWS Shield and CloudFront for DDoS mitigation
VPN	Encrypted VPN required for all remote administrative access

2.4 Application Security

Measure	Implementation
Secure Development	Secure Software Development Lifecycle (SSDLC) practices
Code Reviews	Mandatory peer code reviews before production deployment
Vulnerability Scanning	Automated vulnerability scanning in CI/CD pipeline
Penetration Testing	Annual third-party penetration testing
Dependency Mgmt	Automated scanning for vulnerable dependencies

2.5 Infrastructure Security

Measure	**Implementation**
Cloud Provider	Amazon Web Services (AWS) EU Region (Frankfurt)
Hardening	CIS Benchmark hardening standards applied
Patch Management	Critical patches applied within 72 hours; routine patches within 30 days
Logging	Centralized logging with minimum 12-month retention
Monitoring	Real-time security monitoring via Coralogix SIEM (AWS Ireland)

2.6 Security Assessments

Measure	**Implementation**
Internal Audits	Annual internal ISMS audits
Vulnerability Assessments	Quarterly vulnerability assessments
Penetration Testing	Annual penetration testing by qualified third parties
Third-Party Audits	Annual ISO 27001/27017/27018 surveillance audits
SOC 2 Report	SOC 2 Type II report available upon request under NDA

3. ORGANIZATIONAL MEASURES

3.1 Information Security Governance

Measure	Implementation
Security Leadership	Designated Chief Security Officer (CSO)
ISMS Framework	Documented ISMS policies and procedures aligned with ISO 27001
Risk Management	Annual risk assessments with documented risk treatment plans
Policy Review	Annual review and update of all security policies

3.2 Personnel Security

Measure	Implementation
Confidentiality	NDAs and confidentiality clauses in all employment contracts
Security Training	Mandatory annual security awareness training
Specialized Training	Role-specific security training for technical personnel
Termination Procedures	Immediate access revocation upon termination; exit procedures documented

3.3 Physical Security

Measure	Implementation
Data Center Security	AWS data centers with SOC 2 Type II certification
Physical Access	Badge access, visitor logging, CCTV monitoring at office locations
Clean Desk Policy	Enforced clean desk policy for all personnel
Media Disposal	Secure destruction of media containing Personal Data

4. DATA MANAGEMENT

4.1 Data Segregation

Personal Data is logically segregated by customer using:

- Unique tenant identifiers
- Application-level access controls

4.2 Data Backup and Recovery

Measure	**Implementation**
Backup Frequency	Daily automated backups with point-in-time recovery
Backup Encryption	All backups encrypted at rest using AES-256
Backup Testing	Quarterly backup restoration testing
Geographic Redundancy	Backups replicated across multiple AWS Availability Zones
Retention	Backup retention per contractual requirements (minimum 30 days)

4.3 Data Deletion

Upon termination of the Agreement or upon Controller’s request:

- Personal Data is deleted within 30 days.
- Deletion is confirmed via written certification.
- Backups are purged according to retention schedule (maximum 90 days).

5. CONTACT INFORMATION

Data Protection Officer:

SolarEdge Technologies Ltd.

Email: DPO@solaredge.com

Security Inquiries:

Wevo Energy Ltd.

Email: info@wevo.energy

This Annex is subject to periodic review and update. The Processor shall notify the Controller of any material changes to the security measures described herein.