DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") addresses the processing and transfer of Personal Data of individual Data Subjects under Data Protection Laws, in connection with the Services provided by Direct Energy Partners, Inc. located at 19109 W. Catawba Ave, Ste 200, Cornelius, NC 28031, acting on its own behalf and, to the extent required under Data Protection Laws, on behalf of each Customer Affiliate having rights to use the Services and which have not signed an order form or equivalent directly with DEP for the Services ("**Customer**"), pursuant to the relevant services agreement you have executed with DEP ("**Services Agreement**").

Article 1. Definitions

Affiliate	means an entity that owns or controls, is owned or controlled by or is under common control or ownership with a Party, where the control is defined as direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.
Data Protection Laws	means any laws and regulations governing the privacy and security of personally identifiable information and applicable to the processing of Personal Data under the Services Agreement, including the following to the extent applicable to Personal Data: a) the General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 ("**GDPR**"); b) the Data Protection Act 2018 and any laws implementing the GDPR; c) the GDPR, as it forms part of the law of England and Wales, Scotland and Northern Ireland (i.e., the "**UK GDPR**") as provided in the Data Protection Act 2018, and/or any corresponding or equivalent national laws or regulations; d) the California Consumer Privacy Act of 2018 (Cal. Civ. Code §§ 1798.100 *et seq.*) ("**CCPA**"), and as may be amended, supplemented, or otherwise modified from time to time, including by virtue of the California Privacy Rights Act ("**CPRA**"); e) the laws of any country or other jurisdiction (including, without limitation, Switzerland and the United States and its states) that may apply to the Services; and f) any laws replacing, amending, extending, re-enacting or consolidating any of the enumerated laws above from time to time.
Data Subject	means the identified or identifiable person to whom the Personal Data relates.

Data Subject Request	means a request made by a Data Subject to exercise any rights of Data Subjects under applicable Data Protection Laws.
Personal Data	means all personally identifiable information applicable Data Protection Laws treat as "personal data" (or equivalent term, including without limitation, "personal information, personally identifiable information" and "nonpublic personal information") and where such data is customer data.
Personal Data Breach	means any breach of the Security Standards resulting in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, any Personal Data.
Standard Contractual Clauses ("SCCs")	means, the clauses included in European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 as currently stated at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj.
Sub-processor	means another processor engaged by DEP for carrying out processing activities in respect of the Personal Data.
Supervisory Authority	means any local, national or multinational, department, official, parliament, public or statutory person or any government or professional body, regulatory or supervisory authority, board or other body responsible for administering applicable Data Protection Laws.
Supervisory Authority Correspondence	means any correspondence or communication (whether written or verbal) from a Supervisory Authority in relation to the control or processing of the Personal Data.
Terms used but not defined in this DPA (e.g., "processing", "controller", "processor", "business" , "service provider") shall have the same meaning as set forth in Article 4 of the GDPR or other applicable Data Protection Laws.	

Article 2. <u>Roles</u>

1. For purposes of this DPA, Customer and DEP agree that Customer is the controller (or "business" as that term is defined by the CCPA) of Personal Data and DEP is a processor of Personal Data (or "service provider" as set forth in the CCPA).

Article 3. <u>Scope of Personal Data Processing</u>

1. The collection, processing and/or use of Personal Data may relate to the categories of data presented in **Annex A** to this DPA.

Article 4. Data Processing Instructions

1. DEP shall:

   a) process the Personal Data (i) based on written instructions from Customer, as further specified in this DPA, (ii) where required to do so under applicable Data Protection Laws to which DEP is subject (iii) resulting from processing initiated by Users in their use of the Services, and (iv) pursuant to other documented reasonable instructions of Customer where such instructions are consistent with the terms of the Services Agreement;

   b) delete any Personal Data pursuant to DEP's standard data deletion processes upon expiration or termination of the Services Agreement except for (i) secure back-ups deleted in the ordinary course of business according to an established data retention policy, and (ii) retention as required by Data Protection Laws;

   c) make available to Customer information reasonably necessary to demonstrate compliance with this DPA and Data Protection Laws; and

   d) inform Customer if, in DEP's opinion, any written instruction from Customer violates applicable Data Protection Laws, provided that DEP shall have no obligation to independently inspect or verify Customer's use or processing of Personal Data.

Article 5. Customer Obligations.

1. Customer shall comply with all Data Protection Laws and the terms of this DPA. For the avoidance of doubt, Customer's processing instructions to DEP for the processing of Personal Data must comply with all applicable Data Protection Laws.

2. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired the Personal Data, including providing any required notices to, and obtaining any necessary consent from, Data Subjects, employees or contractors. Customer acknowledges and agrees that DEP shall not be liable for the processing of any Personal Data in which Customer failed to obtain consent from the relevant Data Subject to process such Personal Data. Should Customer learn that it has provided Personal Data under the DPA that may not be shared pursuant to a consent or data privacy notice, Customer shall promptly delete such Personal Data and notify DEP in writing at info@directenergypartners.com without unreasonable delay.

Article 6. Sub-processing

1. Subject to the terms of this Article 6, Customer consents to DEP engaging Sub-processors for the processing of Personal Data. Excluding any DEP Affiliates that will act as additional processors, DEP shall provide notice of any additional Sub-processor(s) it intends to engage in the processing of Personal Data for review by Customer before authorizing such Sub-processor to Process Personal Data. Customer may object to a new Sub-processor by providing written notice to DEP within five days after receipt of DEP's notice. DEP will use reasonable efforts to either make available to Customer a change in the Service or recommend a commercially reasonable change to Customer's configuration and/or use of the Services to

avoid the processing of Personal Data by such objected to new Sub-processor. If DEP cannot make available such change within a reasonable period of time, not to exceed 60 days, Customer may, upon written notice to DEP, terminate the applicable subscriptions for the Services to which the new Sub-processor is applicable as set forth in the applicable Order Form.

2. Where DEP engages a Sub-processor for carrying out processing activities as part of the Services, DEP shall ensure its agreement with such Sub-processor shall contain, in substance, data protection obligations no less protective than those set out in this DPA with regard to the nature of processing by such Sub-processor.

3. DEP remains responsible at all times for compliance with this DPA as applicable. Where the Sub-processor fails to fulfill its obligations under any written DPA, DEP shall remain liable to Customer for the performance of the Sub-processor's obligations.

Article 7. <u>Onward and International Data Transfers</u>

1. In the event Personal Data is transferred out of Europe and to a country which does not ensure an adequate level of data protection within the meaning of the applicable Data Protection Laws, the Standard Contractual Clauses shall apply to such transfers and can be directly enforced by the parties to the extent such transfers are subject to the Data Protection Laws, subject to the following with regard to Module Two:

    a) the option under clause 7 shall not apply,

    b) for purposes of clause 8.1(a), the instructions by Customer to process Personal Data are set out in this DPA,

    c) for purposes of clause 8.5 and 16(d), the parties agree that certification of deletion of Personal Data shall be provided by DEP to Customer only upon Customer's written request,

    d) for purposes of clause 8.6(a), Customer is solely responsible for independently determining whether the technical and organizational measures set forth in the Security Standards meet Customer's requirements and agrees that the security measures and policies implemented and maintained provide a level of security appropriate to the risk with respect to Customer's Personal Data,

    e) for purposes of clause 8.6(c), Personal Data Breaches will be handled in accordance with the DPA,

    f) for purposes of clause 8.9, audits shall be carried out pursuant to the DPA,

    g) Option 2 under clause 9 shall apply. For purposes of clause 9(a), DEP has Customer's general authorization to engage Sub-processors pursuant to the terms of the DPA, and DEP shall notify Customer of additions to its Sub-processors per the terms of the DPA,

h) the optional language under clause 11 shall not apply and for purposes of clause 11, Data Subject Requests shall be addressed pursuant to the terms of the DPA, and

i) DEP's liability under clause 12(b) shall be limited to any damage caused by DEP's processing of Personal Data not in compliance with its obligations under Data Protection Laws specifically directed to Processors, or where DEP has Processed outside of or in contradiction to lawful instructions of Customer.

j) for purposes of clause 17, the governing law shall be as set forth in the Services Agreement. To the extent the governing law set forth in the Services Agreement is not of a European country, the Standard Contractual Clauses shall be governed by the laws of the Belgium.

k) for purposes of clause 18, the venue and jurisdiction shall be as set forth in the Services Agreement. To the extent the venue and jurisdiction set forth in the Services Agreement is not of a European country, the venue and exclusive jurisdiction to resolve any dispute or lawsuit shall be the courts of the England.

2. Where a transfer is made from the UK under the Standard Contractual Clauses (as modified pursuant to Article 7(1) of this DPA), and where such transfer is governed by the Data Protection Laws of the UK, the Mandatory Clauses of the International Data Transfer Addendum ("Addendum") to the EU Commission Standard Contractual Clauses issued by the UK's Information Commissioner's Office ("ICO") shall apply. Information required for Tables 1-3 of Part One of the Addendum is set out in Annex A of this DPA, as applicable. For purposes of Table 4 of Part One of the Addendum, "neither Party" may end this Addendum when the Addendum changes.

Article 8. Assistance with Data Subject Requests

DEP shall, to the extent legally permitted, promptly notify Customer upon receipt of a Data Subject Request. DEP shall not respond to a Data Subject Request itself, except for the purpose of redirecting the Data Subject to Customer to allow Customer to respond accordingly. DEP shall, to the extent Customer in its use of the Services does not have the ability to address a Data Subject Request, comply with reasonable requests to assist with Customer's response to Data Subjects where permitted and required by applicable Data Protection Law.

Article 9. Technical and Organizational Controls and Security

DEP shall maintain the technical and organizational controls and security measures for the protection of Personal Data as set forth in the Security Standards in Annex B.

Article 10. Personal Data Breach

1. DEP shall notify Customer without unreasonable delay after becoming aware of a Personal Data Breach relating to Personal Data. Such notification shall at least:

a) describe the nature of the Personal Data Breach including, where possible, the categories and approximate number of Data Subjects applicable to Customer concerned

and the categories and approximate number of Personal Data records applicable to Customer;

b) provide the name and contact details of the data protection officer or other contact where more information can be obtained; and

c) describe the measures taken or proposed to be taken to address the Personal Data Breach including, where appropriate, measures to mitigate its possible adverse effects.

2. DEP shall make reasonable efforts to identify the cause of the Personal Data Breach and take reasonable steps to remediate the cause as DEP deems necessary to the extent remediation is within DEP's reasonable control.

Article 11. DPIA; Records of Processing Activities

If a data protection impact assessment is required pursuant to Data Protection Laws, DEP shall cooperate and provide reasonable assistance to Customer as needed to fulfil Customer's obligation under Data Protection Laws and related to its use of the Services, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to DEP.

Article 12. Audit right

1. Customer may carry out audits of DEP's processing of Personal Data as required by Data Protection Laws, subject to Customer:

   a) giving DEP at least three (3) weeks' prior written notice of such audit being required by Data Protection Laws and/or the applicable Supervisory Authority, during which time the parties shall mutually agree on the scope, timing and duration of the audit, taking into account the nature and complexity of the Services,

   b) ensuring that all information obtained or generated by Customer or its auditor(s) in connection with such audits is kept strictly confidential save for disclosure to a Supervisory Authority or as otherwise required by Data Protection Laws,

   c) ensuring that such audit is undertaken during normal business hours, with minimal disruption to DEP's business, Sub-processors' business, or the business of other clients of DEP,

   d) providing, at no charge to DEP, a full copy of all findings of the audit, and

   e) paying DEP's reasonable costs for assisting with the provision of information and allowing for and contributing to the audits.

2. Customer may use a third-party auditor with DEP's written consent, which shall not be unreasonably withheld. Prior to any third-party audit, such auditor shall be required to execute an appropriate confidentiality agreement with DEP.

3. After conducting an audit under this Article 12 or after receiving an audit report from DEP, Customer must notify DEP, in writing, of the specific manner, if any, in which DEP does not comply with any of the security, confidentiality, or data protection obligations in this DPA or Data Protection Laws, if applicable. Any such information will be deemed confidential information of DEP.

Article 13. Counterparts, Modification, Supplementation, and Term

1. Should any provisions of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part DEP had never been contained herein.

2. Customer or DEP may modify or supplement this DPA by mutual agreement, (i) if required to do so by a Supervisory Authority or other government or regulatory entity, (ii) if necessary to comply with Data Protection Laws, (iii) to implement Standard Contractual Clauses, (iv) to adhere to an approved code of conduct or certification mechanism approved or certified pursuant to Articles 40 and 42 of the GDPR or similar provisions in applicable Data Protection Laws, or (v) to comply with any request or requirement imposed by an applicable third-party data controller.

3. Without prejudice to this DPA, either Party may from time to time provide additional information and detail about how it will execute this DPA in its product-specific technical, privacy, or policy documentation.

4. This DPA shall expire upon the later of (a) the termination of the Services Agreement; (b) cessation of any processing of Personal Data by DEP on behalf of Customer pursuant to the provision of the Services or (c) delivery of written notice of termination of the Services Agreement from one Party to the other.

DEP	**CUSTOMER**
Name:	Name:
Title:	Title:
Signature:	Signature:
Date:	Date:

ANNEX A TO DATA PROCESSING AGREEMENT

Details of Personal Data Processing

List of Parties
Data exporter: Customer as identified in the DPA.

Name: Customer as identified in the DPA.
Address: See Customer address stated in the DPA.
Contact person's name, position and contact details:
Activities relevant to the data transferred under these clauses: Performance of the Services pursuant to the Services Agreement and DPA.
Role: Controller as identified in the DPA.

Data importer: DEP as identified in the DPA.
Name: DEP as identified in the DPA.
Address: See DEP address stated in the DPA.
Activities relevant to the data transferred under these clauses: Performance of the Services pursuant to the Services Agreement and DPA.
Role: Processor as identified in the DPA.

Purpose(s) of Processing
Personal Data will be processed in accordance with the Services Agreement and the DPA.

Nature of Processing Operations
The nature of the processing activities is as described in the Services Agreement and this DPA.

Categories of Personal Data Transferred
Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include but is not limited to the following: first and last name, email address, mailing address, telephone number, and company affiliation.

Categories of Data Subjects to Whom the Personal Data Is Transferred
Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include but is not limited to the following:

Frequency of the Transfer
Continuous basis depending on Customer's use of the Services.

Duration of Processing
For the duration of the Services Agreement unless otherwise agreed to by the parties.

Sub-processor Transfers
Sub-processors will process Personal Data as set forth in the DPA.
Identities of Sub-processors, their location and processing activities are provided as set forth in the DPA.

Competent Supervisory Authority
If Customer is established in an EEA Member state, the supervisory authority with responsibility for ensuring compliance by the data exporter with GDPR as regards to the data transfer shall act as competent supervisory authority.

If Customer is not established in an EEA Member State but falls within the territorial scope of application of GDPR in accordance with Article 3(2) and has appointed a representative pursuant to Article 27(1) of GDPR, the supervisory authority of the EEA member state in which the representative sits within the meaning of Article 27(1) of GDPR is established shall act as competent supervisory authority.

Where Customer is not established in an EU Member State but falls within the territorial scope of application of GDPR in accordance with its Article 3(2) a competent supervisory authority in Belgium shall be selected.

Where Customer is established in the United Kingdom or falls within the territorial scope of application of the Data Protection Laws of the United Kingdom, the ICO shall act as competent supervisory authority.

Where Customer is established in Switzerland or falls within the territorial scope of application of the Data Protection Laws of Switzerland, the Swiss Federal Data Protection and Information Commissioner shall act as competent supervisory authority insofar as the relevant data transfer is governed by the Data Protection Laws of Switzerland.

Technical and Organizational Measures

The technical and organizational measures maintained by DEP are as set forth in the DPA.

ANNEX B TO DATA PROCESSING AGREEMENT

Direct Energy Partners' Technical and Organizational Measures

Direct Energy Partners maintains commercially reasonable and risk-based administrative, technical, and physical safeguards to protect the confidentiality, integrity, and availability of Personal Data. The following provides a high-level summary of those safeguards. This is not intended to be an exhaustive list, as Direct Energy Partners continually improves its security position in response to changes in business and emerging threats.

- **Change Management**: DIRECT ENERGY PARTNERS maintains logs that document all changes to the information technology operating environment, such as the addition of a server, modifying of code/configurations, or any and all changes affecting production equipment.

- **Encryption**: DIRECT ENERGY PARTNERS encrypts all Personal Data, both at rest and in transit. All DIRECT ENERGY PARTNERS backups utilize full Advanced Encryption System ("AES").

- **Information Security Program**: DIRECT ENERGY PARTNERS maintains a comprehensive written information security program including administrative, technical, and physical safeguards to protect Personal Data.

- **Multi-Factor Authentication**: DIRECT ENERGY PARTNERS enforces multi-factor authentication for all users with administrative privileges or elevated accounts.

- **Password Management**: All DIRECT ENERGY PARTNERS users are required to use strong passwords and change those passwords on a regular basis. In addition, all passwords for administrative accounts are maintained in a key vault with multi-factor authentication in place.

- **Patch Management**: DIRECT ENERGY PARTNERS maintains and pushes critical security updates for all equipment immediately upon Direct Energy Partners release.

- **Physical Safeguards**: All DIRECT ENERGY PARTNERS locations and data centers employ a full-time security guard, and maintains an access control system with clearance badges. In addition, DIRECT ENERGY PARTNERS has established security areas with restriction of access paths.

- **Risk Assessment & Penetration Testing**: DIRECT ENERGY PARTNERS performs annual information security risk assessments with penetration testing, as well as quarterly phishing campaigns.

- **Scanning**: DIRECT ENERGY PARTNERS performs vulnerability scans of all devices connected to its network by executing real-time anti-virus scans and malware scans, as well as full-time use of intrusion detection and penetration systems. DIRECT ENERGY PARTNERS also scans all emails for potentially malicious content and provides DIRECT ENERGY PARTNERS users the ability to report and quarantine as desired.

- **Training & Awareness**: DIRECT ENERGY PARTNERS mandates its employees complete regularly scheduled security and incident response training provided by its trusted third party Direct Energy Partners, and maintains an ongoing awareness progress to keep employees apprised of new requirements and threats.

- **DIRECT ENERGY PARTNERS Policies**: DIRECT ENERGY PARTNERS will act in accordance with its existing policies and procedures governing the handling of Personal Data including, but not limited to, DIRECT ENERGY PARTNERS's Privacy Policy and Terms of Use (as amended from time to time).

132372906v1